SYMANITRON

Инновационные
промышленные сети

Руководство по настройке коммутаторов серий SEWM9A-D, SEWM9G-D, SEWM18G-D

Оглавление

Введение

Данный документ содержит информацию о возможностях программного обеспечения коммутаторов серий SEWM9A-D, SEWM9G-D, SEWM18G-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 • Модели • Возможности программного обеспечения
2. Способы подключения к устройству	• Подключение через консольный порт • Подключение с использованием Telnet • Подключение через Web-интерфейс
3. Управление устройством	• Перезагрузка • Вход в систему и выход из системы
4. Статус устройства	• Основная информация • Статус портов • Статистика по портам
5. Основные настройки	• IP адрес • Информация об устройстве • Настройка портов • Изменение пароля • Обновление программного обеспечения
6. LLDP	Настройка протокола LLDP
7. ARP	Настройка протокола ARP
8. QoS	Настройка услуги QoS
9. Port Trunk	Настройка транковых портов
10. MAC Aging Time	Настройка MAC адресов
11. Скорость портов (Port Rate)	Настройка скорости портов
12. Кольцевое резервирование	• Настройка протокола Sy2-Ring • Настройка протоколов RSTP/STP • Настройка протокола Sy2-RP
13. Многоадресная передача (Multicast)	• GMRP • Многоадресная рассылка статических FDB (Static FDB Multicast) • IMGP Snooping
14. Диагностика	• Зеркалирование портов (Port Mirroring) • Проверка соединений (Link Check) • Виртуальный тестер кабелей
15. SNTP	Настройка протокола SNTP
16. Безопасность (Security)	• SSH • Dot1x

	• Безопасность порта (Port Security) • Настройка AAA • Настройка TACACS+ • Настройка SSL
17. VLAN	Настройка VLAN PVLAN GVRP
18. RMON	Настройка протокола RMON
19. 19. Одноадресная рассылка (Unicast)	Настройка услуги одноадресной рассылки
20. Сообщения о тревогах и запись информации в системный журнал	• Аварийная сигнализация (Alarm) • Ведение системного журнала
21. SNMP	• Протокол SNMP v2 (версия 2) • Протокол SNMP v3 (версия 3)
22. DHCP	• Настройка сервера DHCP • DHCP Snooping • Настройка Option82

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*

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 серий SEWM9A-D, SEWM9G-D, SEWM18G-D предназначены для установки на DIN-рейку и могут использоваться в различных областях промышленности: системах передачи данных в энергетике, на транспорте, в горнодобывающей промышленности, ветроэнергетике. Данная серия коммутаторов имеет консольный порт в формате Mini USB, поддерживает стандарты IEC52439-6 и VCT. Кнопка «Reset» позволяет сбросить настройки устройств в состояние «заводские установки» в одно касание. Это высокопроизводительная серия коммутаторов может обеспечить потребности сетей передачи данных для многих отраслей промышленности.

1.2. Функциональные возможности ПО

Программное обеспечение коммутаторы серий SEWM9A-D, SEWM9G-D, SEWM18G-D поддерживает множество различных функций:

- Протоколы кольцевого резервирования: RSTP/STP, Sy2-Ring, IEC62439-6;
- Протоколы мультиадресной рассылки (Multicast): IMGP Snooping, GMRP, Static;
- Функции коммутации: VLAN, PVLAN, GVRP, QoS, ARP;
- Управление пропускной способностью: транковые порты (Port Trunk), лимитирование скорости портов;
- Протокол синхронизации времени: SNMP;
- Безопасность: IEEE802.1X, TACACS+, SSH, SSL, Безопасный порт; AAA;
- Управление устройством: обновление через FTP/TFTP, передача файлов посредством FTP/TFTP, ведение системного журнала;
- Диагностика устройства: зеркалирование портов (port mirroring), LLDP, VCT, проверка статуса соединения;
- Система тревожных оповещений: ошибка порта (port alarm), ошибка питания (power alarm), ошибка кольца (ring alarm);
- Сетевой доступ к устройству и управление: CLI, Telnet, Web, NMS Symanitron, SNMP.
- ……

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, он имеет возможность, используя различные команды, получать информацию о состоянии устройства и выполнять настройки коммутатора:

Подсказка	Тип отображения	Функция	Команда
SWITCH>	Режим Просмотр	• Показать текущие пользовательские команды • Показать IP адрес • Показать версию ПО	Введите «**Enable**» для входа в режим Управления
SWITCH #	Режим Управление	• Показать информацию о конфигурации коммутатора • Загрузить/выгрузить конфигурационный файл • Загрузить/выгрузить файл системного журнала • Вернуться к заводским настройкам • Записать текущую конфигурацию • Обновить ПО • Перезагрузить коммутатор	Введите «**Configure terminal**» для переключения из режима Управления в режим Настройки
SWITCH (config) #	Режим Настройка	• Настроить все функциональные возможности коммутатора	Введите «**exit**» для возврате в режим Просмотра

Когда выполняется настройка коммутатора посредством сервиса 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, <H:H:H:H:H:H> означает MAC адрес, word<1,31> означает диапазон строк. Также символы ↑ и ↓ могут использоваться для просмотра последних 10 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 соединение по последовательному

порту, например HTT3.3. В примере ниже показано, как использовать консольный порт и HyperTerminal для доступа к коммутатору.

1. Установите драйвер для интерфейса MiniUSB на ваш ПК. Драйвер называется «Mini USB driver.exe».
2. Подключите USB кабель к ПК и консольному интерфейсу устройства (кабель должен быть оснащён разъёмом miniUSB с одной стороны и USB с другой).
3. Запустите HyperTerminal (или другой эмулятор терминала вроде Putty), он поможет вам подключиться к устройству для его настройки.

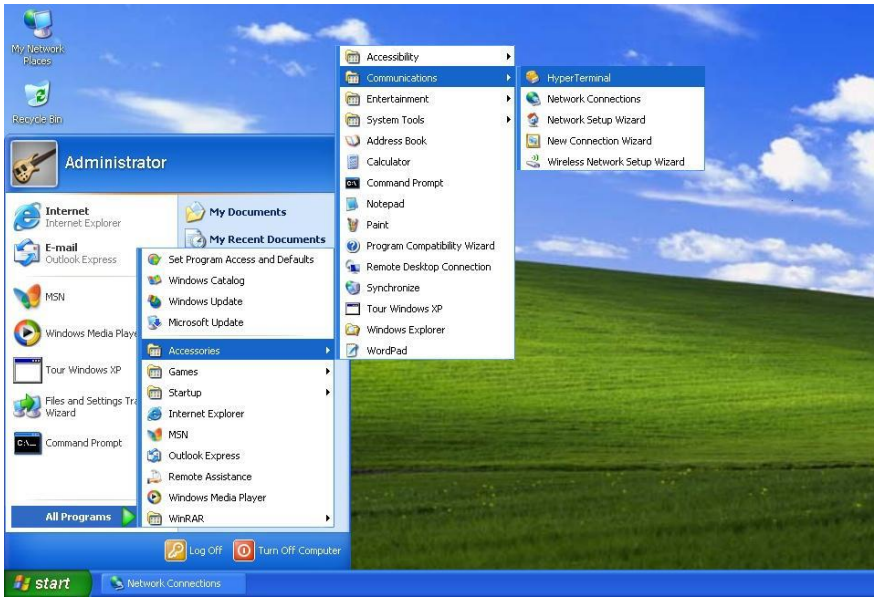


Рис. 1. Запуск HyperTerminal

4. Создайте новое подключение, например, с именем «Switch» (см. рис. 2).

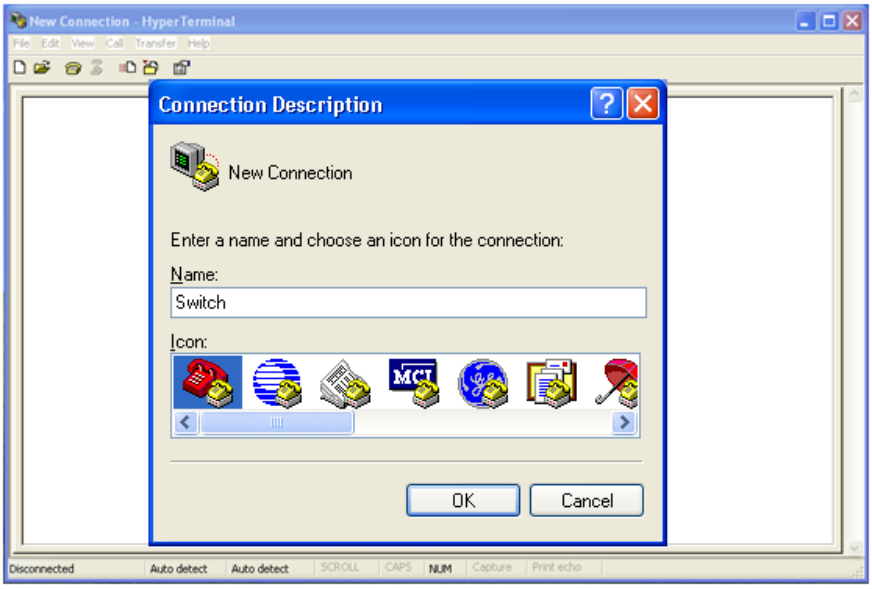


Рис. 2. Создание нового подключения

5. Выберите COM порт для подключения.

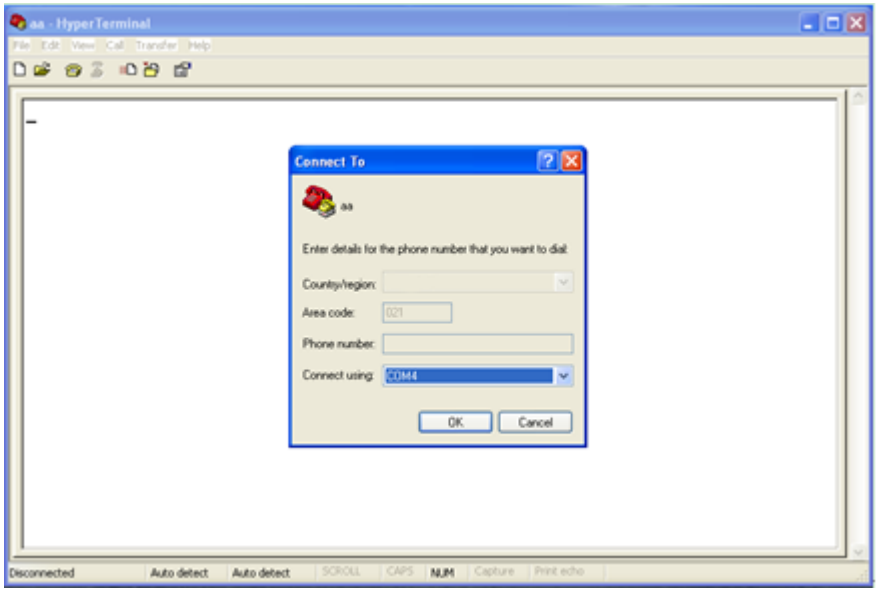


Рис. 3. Выбор COM порта для подключения

6. Настройте параметры COM порта (Бит в секунду (Baud rate): 115200, Биты данных (Data bits): 8, Чётность (Parity): None, Стоповые биты (Stop bits): 1, Контроль потока (Flow control): None.

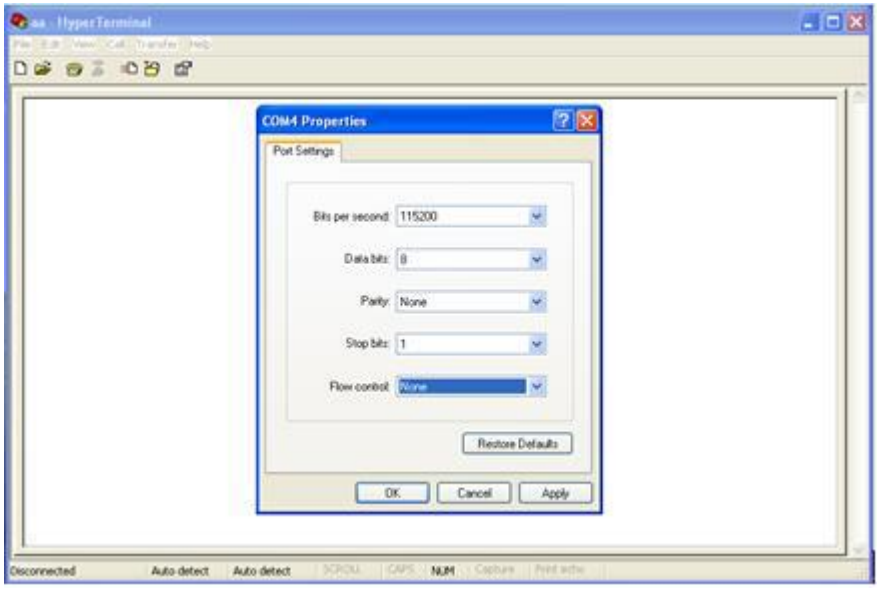


Рис. 4. Настройка параметров COM порта

7. Нажмите <OK> для входа в командную строку CLI. Введите пароль «admin» и нажмите <Enter>.

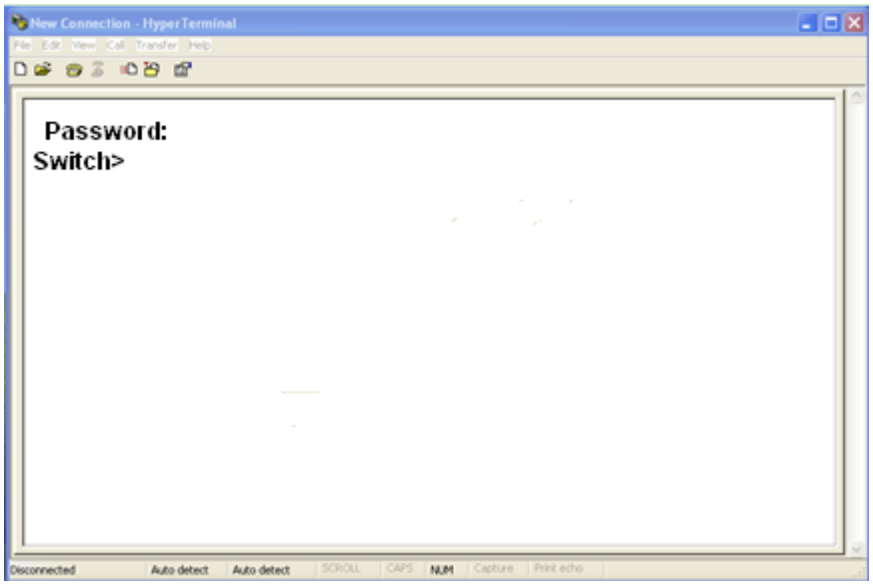


Рис. 5. Экран CLI

2.3. Подключение к коммутатору посредством Telnet

1. Подключите любой RJ45 порт коммутатора к Ethernet порту ПК.
2. Откройте <Выполнить> на ПК, там введите “telnet IP-адрес”, по умолчанию IP-адрес - 192.168.0.2.

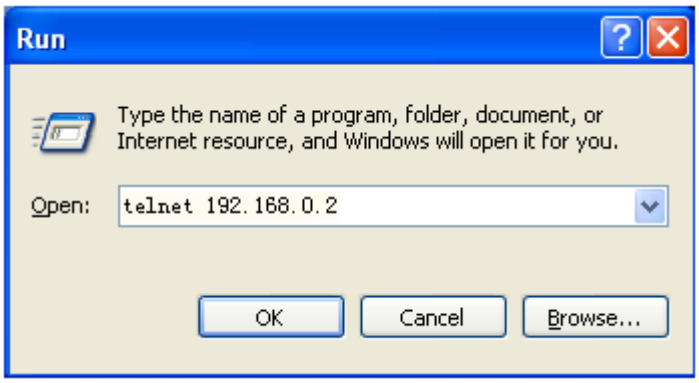


Рис. 6. Доступ через Telnet

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

3. Нажмите “OK”, откроется интерфейс терминала Telnet. Введите имя пользователя «admim» и пароль «123». Нажмите <Enter> для подключения к коммутатору.

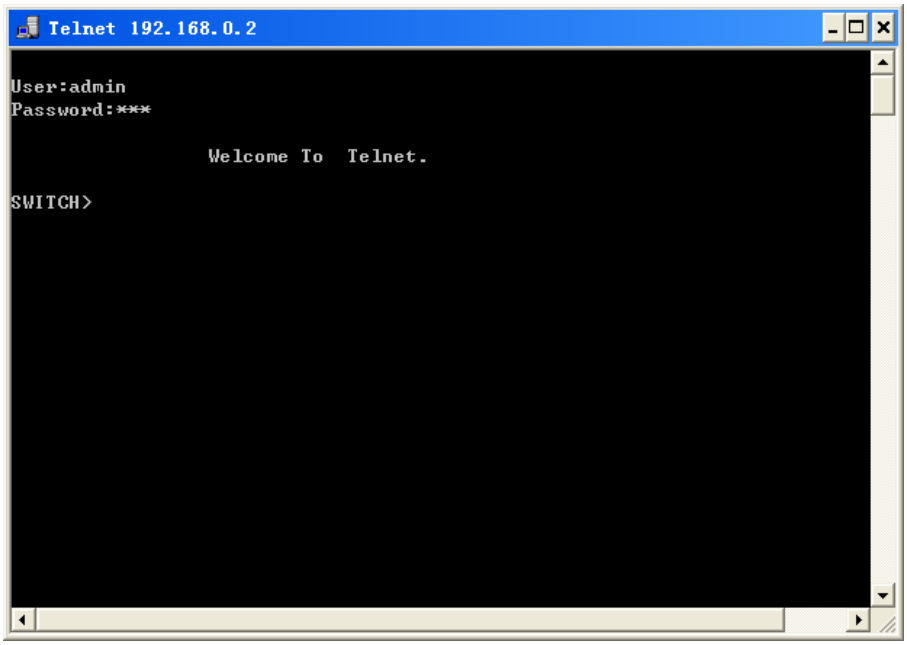


Рис. 7. Интерфейс терминала Telnet

2.4. Доступ через WEB-интерфейс

Для подключения через Web-интерфейс по умолчанию используется протокол HTTP. Если для подключения будет использоваться протокол HTTPS, пожалуйста, изучите раздел «SSL» настоящего руководства.

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**

Затем нажмите кнопку «Sign in».

При использовании Internet Explorer, рекомендуется использовать версию не ниже 8.0.

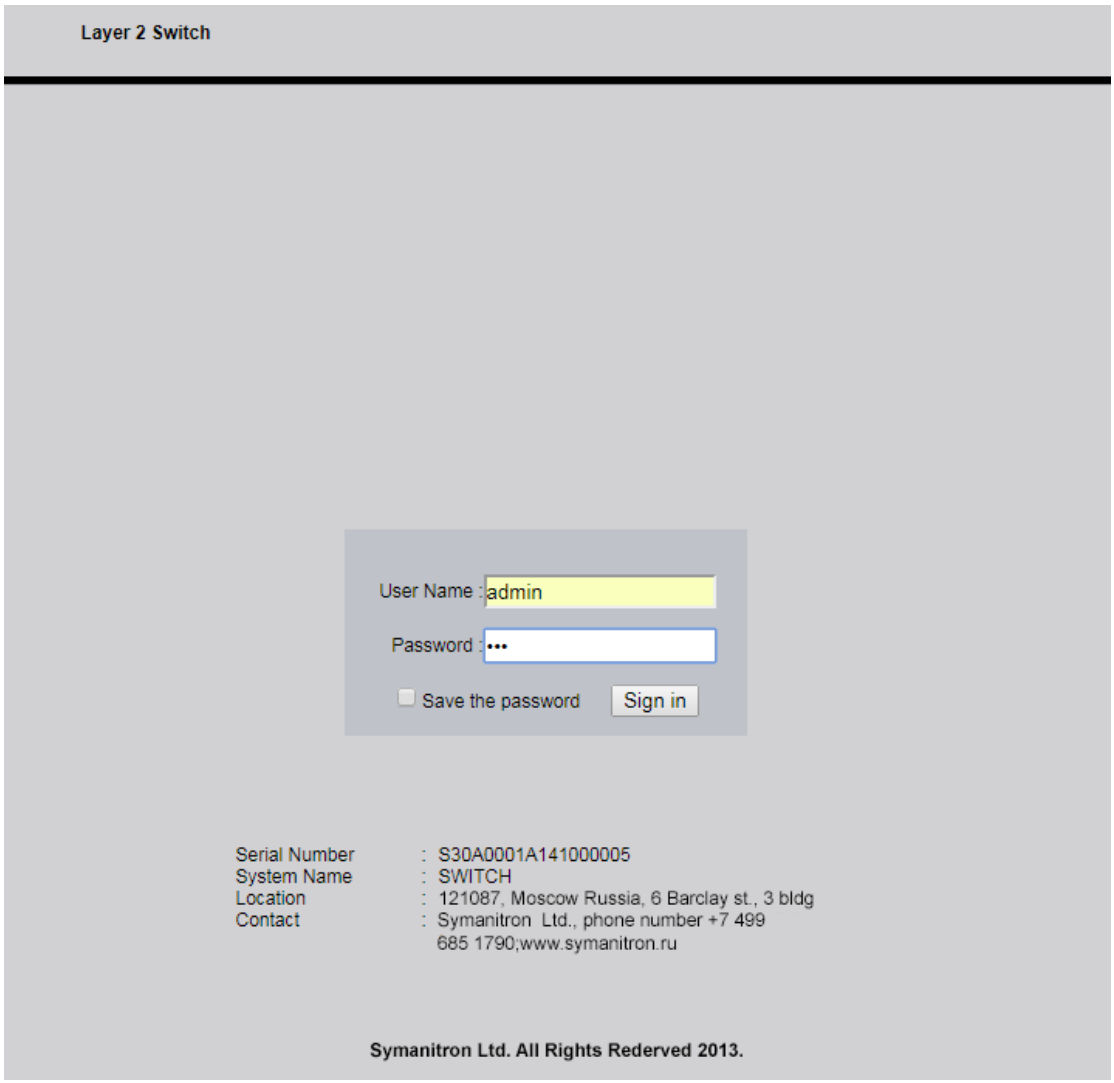


Рис. 8. Авторизация через WEB-интерфейс

3. После подключения к Web-интерфейсу коммутатора вы увидите навигационное дерево:

Рис. 9. Страница WEB-интерфейса

У вас есть возможность сворачивать или разворачивать меню, нажимая на кнопки <Expand> или <Collapse>, которые находятся сверху навигационного дерева. Вы можете выполнить соответствующие операции, нажав [Save Settings] или [Load Default] в верхней части меню.

После того как вы изменили заводские установки и записали новые параметры, необходимо перезагрузить устройство для того, чтобы новые параметры вступили в силу.

3. Управление устройством

Нажмите [Device Management]→[Reboot]/[Logout]. Вы сможете перезагрузить устройство или выйти из Web-интерфейса. Перед перезагрузкой устройство сообщит вам, что необходимо сохранить текущие настройки. Если настройки были сохранены ранее, коммутатор автоматически загрузит их после рестарта. Если настройки не сохранялись, коммутатор по умолчанию восстановит после рестарта заводские настройки.

4. Статус устройства

4.1. Основная информация о коммутаторе

Основная информация о коммутаторе включает имя устройства, MAC-адрес, модель, версию программного обеспечения, версию BootROM, тип устройства, дату выпуска прошивки и среду выполнения (рис.10).

Basic Info

Item	Information
MAC Address	48-BE-2D-00-2B-B6
SN	S3V1SA180700005
IP Address	192.168.0.2
Subnet Mask	255.255.255.0
GateWay	192.168.0.1
System Name	SWITCH
Device Model	SEWM9A-D-1SFX-7TX-40-1310-SC-24E
Software Version	R0011.P01 (2017-9-7 11:48)
BootRom Version	V2.1.19 (2016-7-9 16:7)

Рис. 10. Основная информация о коммутаторе

4.2. Статус порта

Интерфейс статуса порта выводит на экран номер порта, тип порта, статус администратора, статус соединения, скорость, тип способа связи и тип управления потоком (рис.11).

Port Status

Port	Type	Administration Status	Link	Speed	Duplex	Flow Control
1	FE	Enable	Down	---	---	---
2	FE	Enable	Up	100	Full-duplex	Off
3	FE	Enable	Up	100	Full-duplex	Off
4	FE	Enable	Up	100	Half-duplex	Off
5	FE	Enable	Up	100	Full-duplex	Off
6	FE	Disable	---	---	---	---
7	FX	Enable	Down	---	---	---
8	FX	Enable	Down	---	---	---
9	FX	Enable	Down	---	---	---

Рис. 11. Статус портов

Номер порта (Port)

Отображает номер порта, который указан на передней панели коммутатора.

Тип порта (Type)

FE: 10/100Base-TX RJ45

FX: 100Base-FX

GE: 10/100/1000Base-TX RJ45

GX: Gigabit SFP

Статус администрирования (Administration Status)

Показывает текущий статус администрирования порта.

Enable: порт доступен и готов передаче данных.

Disable: порт заблокирован и не имеет возможность передавать данные.

Статус соединения (Link)

Показывает текущий статус соединения на порту.

Up: порт находится в состоянии LinkUp, т.е. в состоянии соединения.

Down: порт находится в состоянии Link Down, т.е. порту соединения нет.

Скорость (Speed)

Показывает текущую скорость портов в состоянии LinkUp, т.е в состоянии соединения.

Способ связи (Duplex)

Показывает способ связи Full-duplex/Half-duplex (Дуплекс/Полудуплекс) на порту в состоянии LinkUp, т.е в состоянии соединения.

Full-duplex: порт может принимать и передавать данные одновременно.

Half-duplex: порт может только либо принимать, либо передавать данные.

Управление потоком (Flow Control)

Показывает статус режима управления потоком порта в состоянии LinkUp, т.е в состоянии соединения.

Для получения детальной информации о режимах и статусе duplex и flow control, пожалуйста, обратитесь к разделу «Port Configuration» настоящего руководства.

4.3. Статистика порта

Интерфейс статистики порта выводит на экран количество байт и пакетов, переданных и принятых на каждом порту, количество ошибок CRC, а также количество пакетов, длина которых менее 64 байт.

Port Statistics

Port	Type	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets 64 bytes
1	FE	0	0	0	0	0	0
2	FE	0	0	0	0	0	0
3	FE	4844	49	4160	60	0	0
4	FE	330727	778	78847	678	0	0
5	FE	0	0	0	0	0	0
6	FE	0	0	0	0	0	0
7	FX	0	0	0	0	0	0
8	FX	0	0	0	0	0	0

Рис. 12. Статистика портов

5. Основные настройки коммутатора

5.1. IP адрес

1. Показать IP адрес, используя консольный порт

Подключитесь к коммутатору через консольный порт и CLI. Введите команду «show interface» для проверки IP адреса:

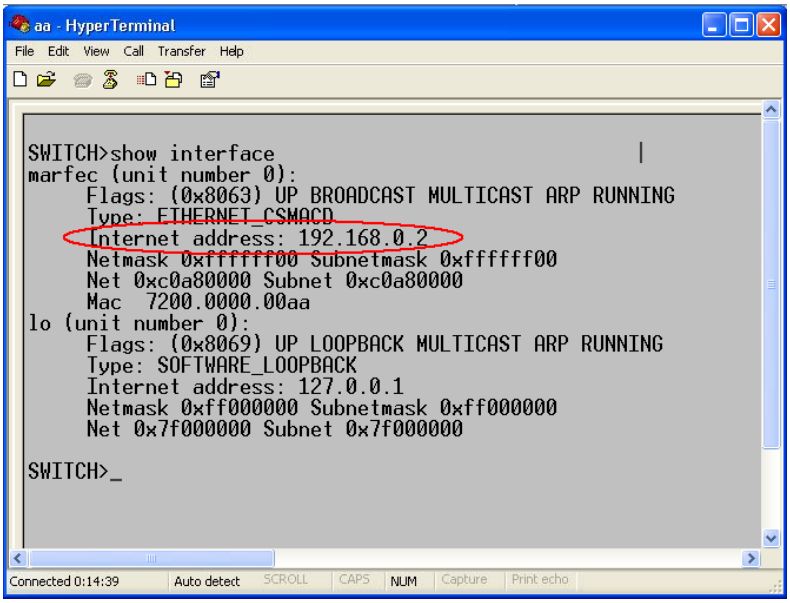


Рис. 13. Показать IP адрес

2. Настройка IP адреса

IP адрес коммутатора и адрес шлюза могут быть настроены как вручную, так и автоматически. Как показано на рис.14, если режим «Auto IP Configuration» выключен, IP адрес и адрес шлюза нужно настраивать вручную; когда режим «Auto IP Configuration» включен, коммутатор автоматически получает IP адрес посредством протокола DHCP. Соответственно в сети должен быть сервер DHCP для назначения IPадресов. Для получения подробной информации обратитесь к разделу «Настройка сервера DHCP» настоящего руководства.

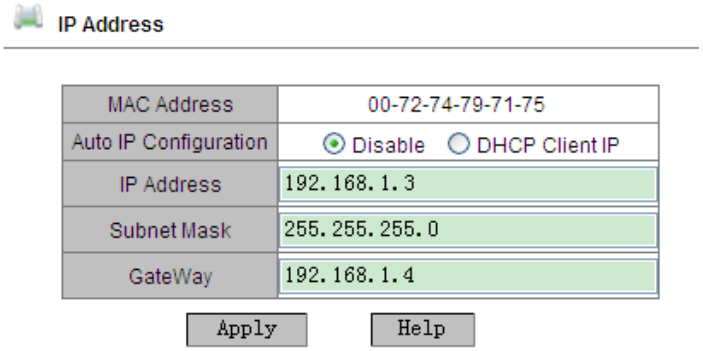


Рис. 14. Настройка IP адреса

- IP адрес и адрес шлюза должны находиться в одном сегменте сети, в противном случае изменить IP адрес будет невозможно
- Для данной серии коммутаторов изменение IP адреса вступит в действие немедленно и перезагрузка коммутатора не требуется

5.2. Информация об устройстве

Информация об устройстве включает данные об имени проекта, имени коммутатора, размещении и контактах:

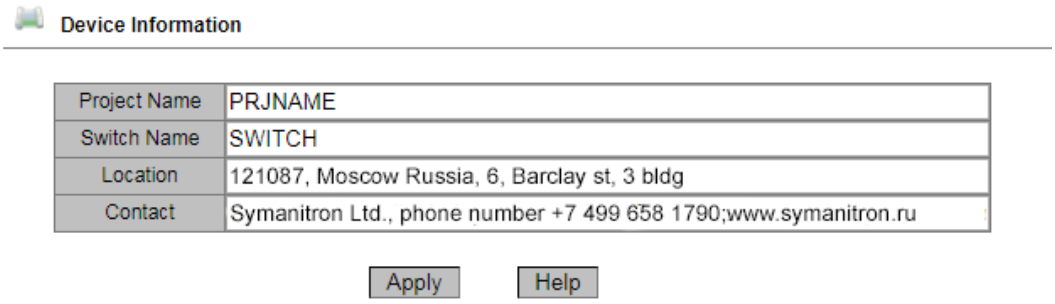


Рис. 15. Информация об устройстве

Имя проекта (Project Name)
Настраиваемый диапазон: 1~64 символов.
Имя коммутатора (Switch Name)
Настраиваемый диапазон: 1~32 символов.
Местоположение (Location)
Настраиваемый диапазон: 1~255 символов.
Контакты (Contact)
Настраиваемый диапазон: 1~32 символов.

5.3. Настройка порта

При помощи данной функции можно настроить скорость порта, статус администрирования порта, тип управления потоком и другие параметры:

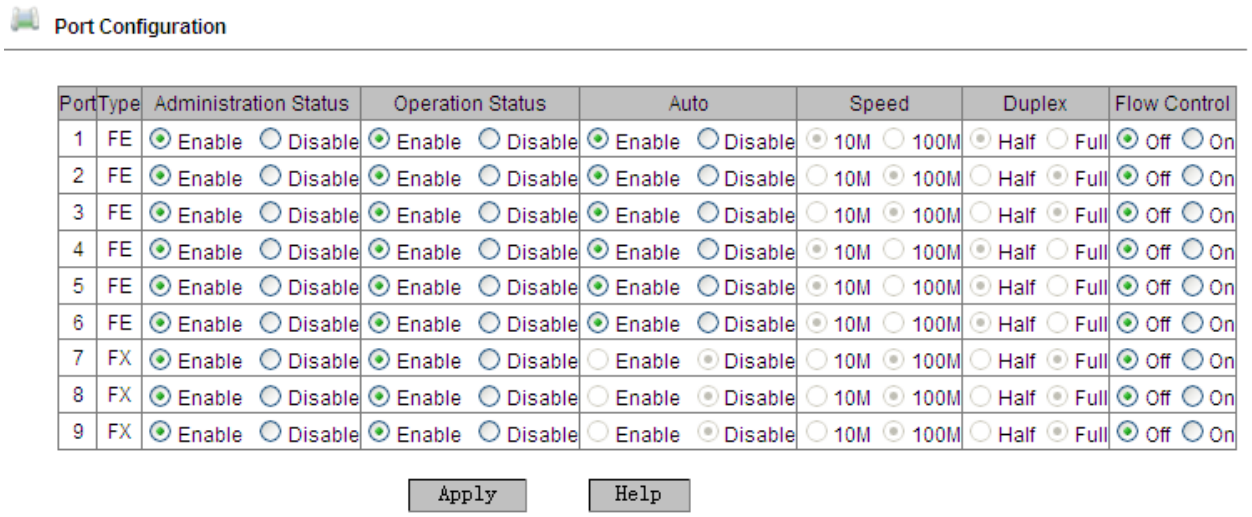


Рис. 16. Настройка порта

Статус администрирования (Administration Status)
Настраиваемые опции: Enable/Disable (Включить/Выключить).
Значение по умолчанию: Enable (Включено).
Описание: Enable (Включено) означает, что порт открыт и передача данных разрешена; Disable (Выключено) означает, что порт блокирован и передача данных запрещена.

Данная опция позволяет напрямую отключить порт и аварийные сообщения. Когда порт выключен, нельзя изменить состояние порта в режиме «Operation Status».

Статус функционирования порта (Operation Status)

Настраиваемые опции: Enable/Disable (Включить/Выключить).

Значение по умолчанию: Enable (Включено).

Описание: Настройка рабочего статуса порта. Порт отключается посредством протоколов.

Режим автосогласования (Auto)

Настраиваемые опции: Enable/Disable (Включить/Выключить).

Значение по умолчанию: Enable (Включено).

Описание: Настройка режима автосогласования (auto-negotiation) для порта. Когда режим «Auto» включен (Enable), скорость порта и режим способа связи (duplex) будут автоматически согласованы в соответствии со статусом подключения порта; когда режим «Auto» выключен (Disable), скорость порта и режим способа связи могут быть настроены вручную.

На портах 100Base-FX принудительно запрещена функция автосогласования (auto-negotiation).

Скорость порта (Speed)

Настраиваемые опции: 10M/100M/1000M

Описание: Принудительная настройка скорости порта. Когда режим «Auto» выключен (Disable), скорость порта можно настраивать вручную.

Способ связи (Duplex)

Настраиваемые опции: Half/Full (Полудуплекс/Дуплекс).

Описание: Настройка режима способа связи для порта; когда режим «Auto» выключен, настройку режимов можно производить вручную.

- Порты 10/100Base-TX могут быть настроены в режиме автосогласования (auto-negotiation) а также в режимах 10M/дуплекс, 10M/полудуплекс, 100M/дуплекс, 100M/полудуплекс.
- Порты 100Base-FX поддерживают только функцию 100M/дуплекс.
- «Медные» порты 1000M могут быть настроены в режимах автосогласования (auto-negotiation) и 1000M/дуплекс.
- Оптические порты 1000M могут быть настроены в режимах автосогласования (auto-negotiation) и 1000M/дуплекс.

Рекомендуется включить автосогласование (auto-negotiation) для каждого порта, чтобы избежать проблем подключения, вызванных несогласованной конфигурацией портов. Если требуется принудительно использовать режим speed/duplex, убедитесь, что в обоих подключенных портах установлены одинаковые настройки скорости и режима передачи (дуплекс/полудуплекс).

Flow Control

Настраиваемые опции: Off/On (Выключено/Включено).

Значение по умолчанию: Off (Выключено).

Описание: Включить/Выключить режим управления потоком для определенного порта. После того, как функция управления потоком (Flow Control) 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, необходима задержка передачи данных.

5.4. Изменение пароля

При первоначальной настройке коммутатора пользователь имеет возможность изменить пароль доступа «Администратора»:

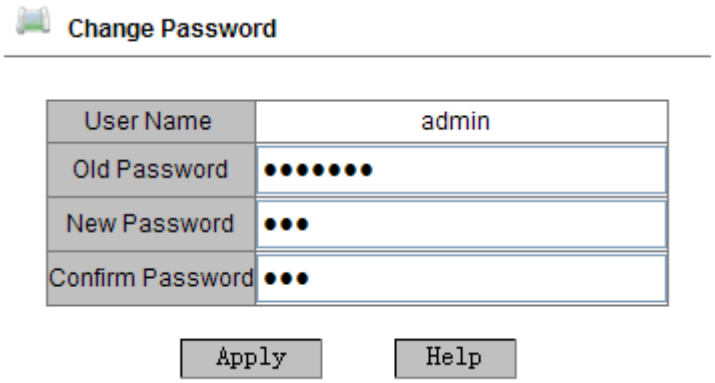


Рис. 17. Изменение пароля

5.5. Обновление программного обеспечения (ПО)

При обновлении программного обеспечения коммутатор может получить больше возможностей. Для этих серий коммутаторов обновления программного обеспечения содержат обновление версии программного обеспечения BootROM и обновление версии системного программного обеспечения. Сначала обновите версию программного обеспечения BootROM, а затем обновите версию системного программного обеспечения. Если изменения в версии BootROM нет, пользователи смогут обновить только версию системного программного обеспечения.

Для обновления системного программного обеспечения требуется наличие сервера FTP/TFTP.

5.5.1. Обновление ПО через FTP

Установите на ПК сервер FTP. В нашем примере мы покажем, как настроить сервер FTP и выполнить процедуру обновления ПО с помощью программы WFTPD.

1. Нажмите [Security]→[Users/Right], чтобы открыть раздел «Users/Right Security Dialog»; Нажмите кнопку <New User> для создания нового пользователя сервера FTP, как показано на рис. 18. Укажите имя пользователя и пароль, например, пользовательское имя «admin» и пароль «123», затем нажмите <OK>.

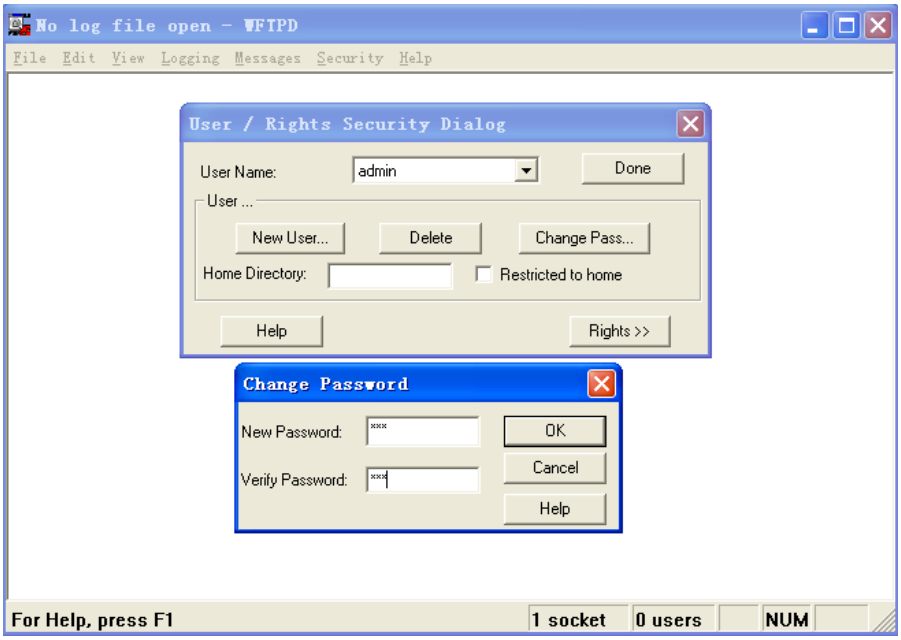


Рис. 18. Создание нового пользователя FTP

2. Укажите путь к месторасположению файла обновления в разделе «Home Directory», как показано на рис. 19 и нажмите <Done>.

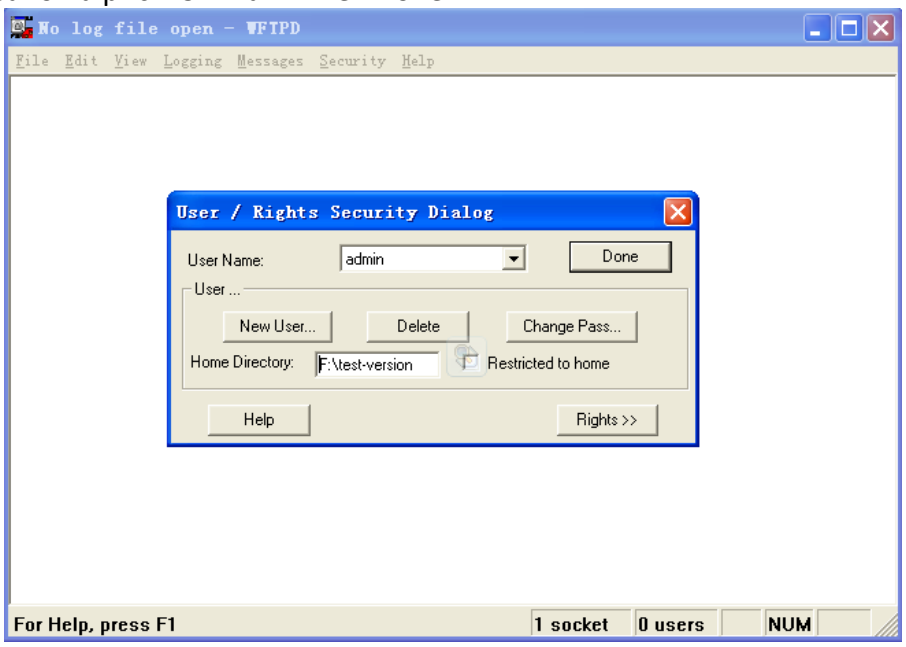


Рис. 19. Путь для записи файла

3. Для обновления ПО BootROM введите в окне управления следующую команду:

Switch#**update ftp-mode bootrom** *File_name Ftp_server_ip_address User_name Password*

Параметры команд для обновления BootROM через FTP:

Параметр	Описание
File_name	Имя версии BootROM
Ftp_server_ip_address	IP адрес сервера FTP
User_name	Создание нового пользователя FTP
Password	Создание нового пароля FTP

4. На рис.20 показана страница обновления ПО. Введите IP адрес сервера FTP, имя файла (на сервере), имя пользователя FTP и пароль. Нажмите <Apply>.

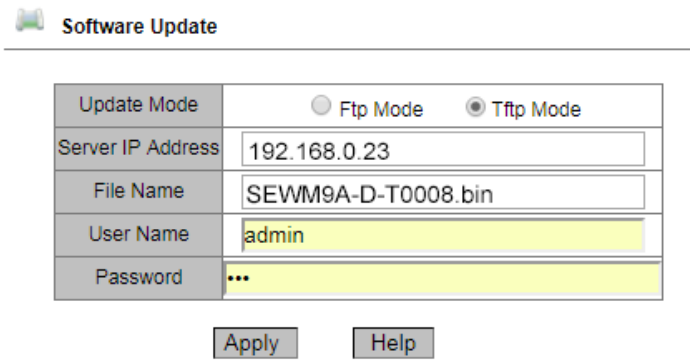


Рис. 20. Обновление ПО через FTP

Имя файла должно содержать расширение. В противном случае обновление может завершиться ошибкой.

5. Убедитесь в нормальном соединении сервера FTP и коммутатора:

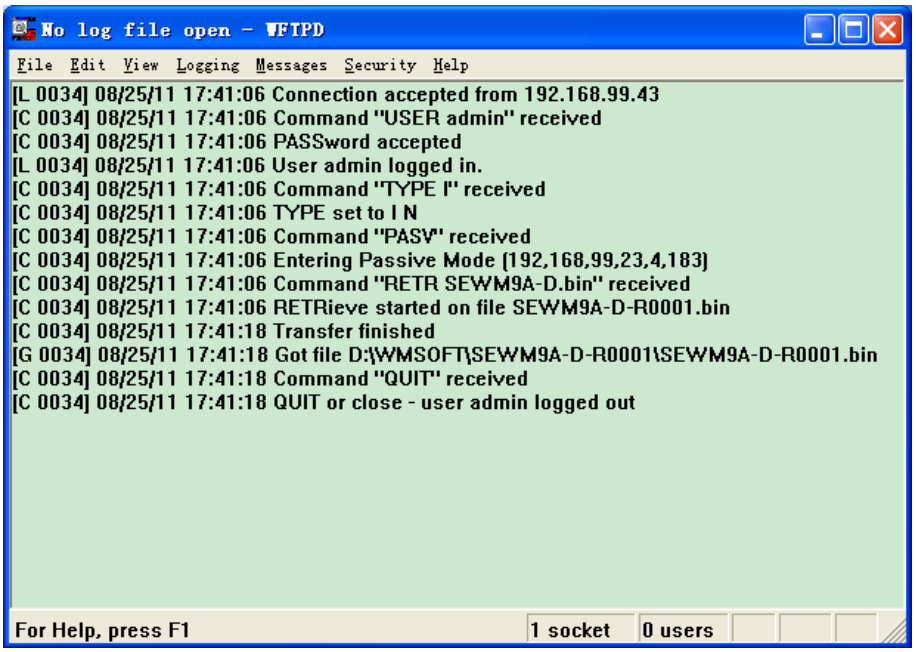


Рис. 21. Соединение коммутатора и сервера FTP

6. Дождитесь завершения обновления:

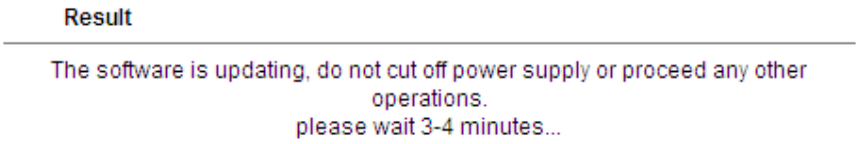


Рис. 22. Ожидание завершения обновления

7. Когда обновление будет завершено, как показано на рис.23, перезагрузите устройство. Потом зайдите в раздел «Основная информация о коммутаторе» и убедитесь в том, что обновление завершено и новая версия активна.

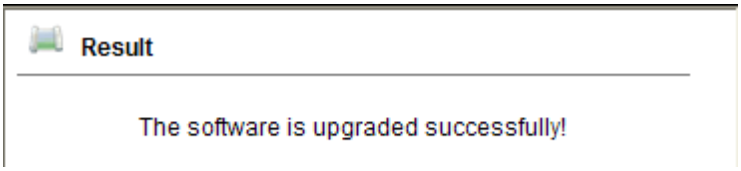


Рис. 23. Обновление через FTP завершено

- В процессе обновления ПО сервер FTP должен быть постоянно загружен.
- После завершения обновления перезагрузите устройство, чтобы активировать новую версию ПО.
- Если обновление завершено с ошибкой, не перезагружайте устройство, чтобы избежать потери файла с ПО. Есть вероятность того, коммутатор не сможет функционировать корректно.

5.5.2. Обновление ПО через TFTP

Установите на ПК сервер TFTP. В нашем примере мы покажем, как настроить сервер TFTP и выполнить процедуру обновления ПО с помощью программы WFTPD, как показано на рис. 24.

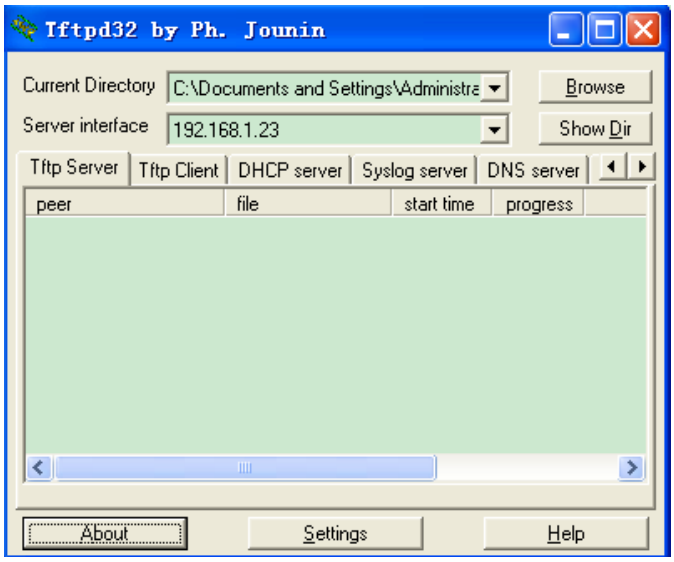


Рис. 24. Настройка сервера TFTP

1. В текущей директории выберите путь к месторасположению файла обновления на сервере; введите IP адрес сервера.
2. Для обновления ПО BootROM введите в окне управления следующую команду:

Switch#**update tftp-mode bootrom** *File_name Ftp_server_ip_address*

Параметры команд для обновления BootROM через TFTP:

Параметр	Описание
File_name	Имя версии BootROM
Ftp_server_ip_address	IP адрес сервера TFTP

3. На рис.25 показана страница обновления ПО. Введите IP адрес сервера TFTP, имя файла на сервере, нажмите <Apply> и ожидайте, пока завершится обновление.

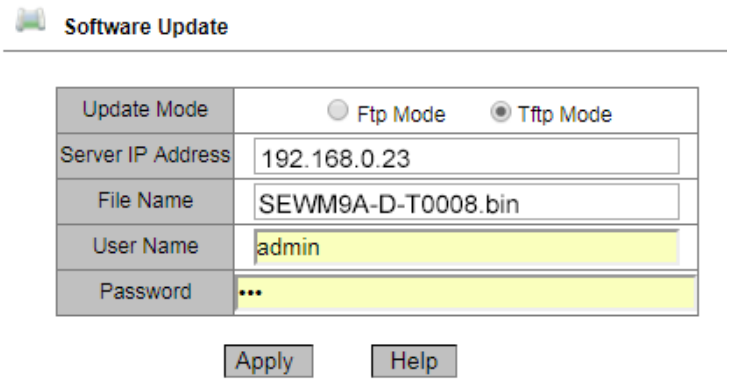


Рис. 25. Обновление ПО через TFTP

Если обновление выполняется через TFTP, нет необходимости использовать имя пользователя и пароль.

Убедитесь в нормальном соединении сервера FTP и коммутатора:

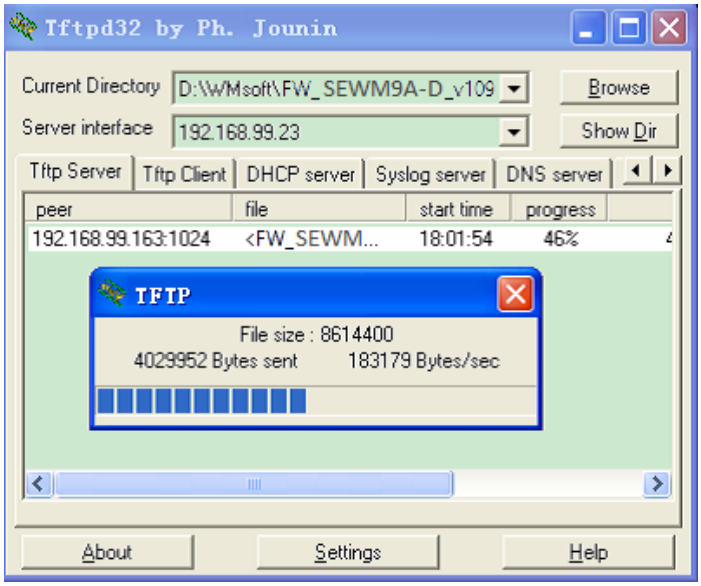


Рис. 26. Соединение коммутатора и сервера TFTP

4. Дождитесь завершения обновления:

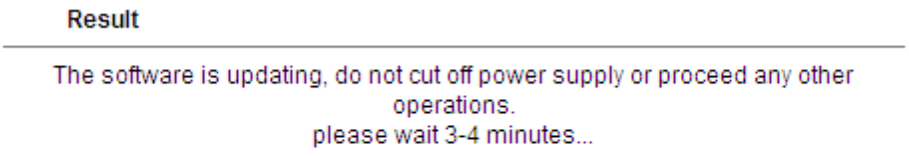


Рис. 27. Ожидание завершения обновления

5. Когда обновление будет завершено, как показано на рис.28, перезагрузите устройство. Потом зайдите в раздел «Основная информация о коммутаторе» и убедитесь в том, что обновление завершено и новая версия активна.

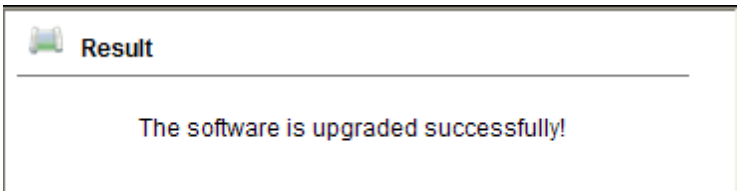


Рис. 28. Обновление через TFTP завершено

- В процессе обновления ПО сервер TFTP должен быть постоянно загружен.
- После завершения обновления перезагрузите устройство, чтобы активировать новую версию ПО.
- Если обновление завершено с ошибкой, не перезагружайте устройство, чтобы избежать потери файла с ПО. Есть вероятность того, коммутатор не сможет функционировать корректно.

5.6. Функция резервного копирования и загрузки настроек

У коммутатора имеется функция резервного копирования конфигурации. Данная функция позволяет сохранять текущие файлы с конфигурацией коммутатора на сервере. После того, как настройки коммутатора были изменены, пользователи имеют возможность загрузить файлы с исходными настройками с сервера на коммутатор с использованием протоколов FTP / TFTP.
Файлы с настройками коммутатора хранятся на сервере в форматах *.doc и *.txt. Процедура загрузки сохраненных файлов с настройками с сервера на коммутатор показана на рис. 29-32.

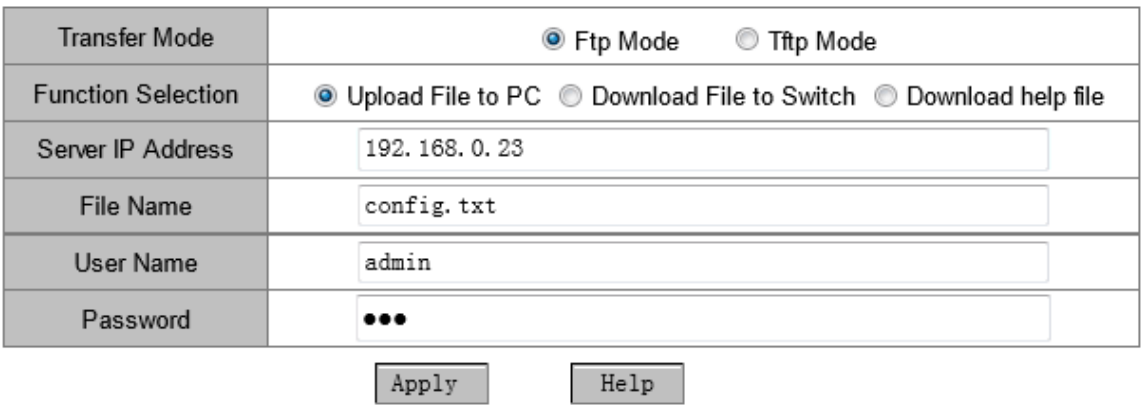


Рис. 29. Загрузка файла с настройками в режиме FTP

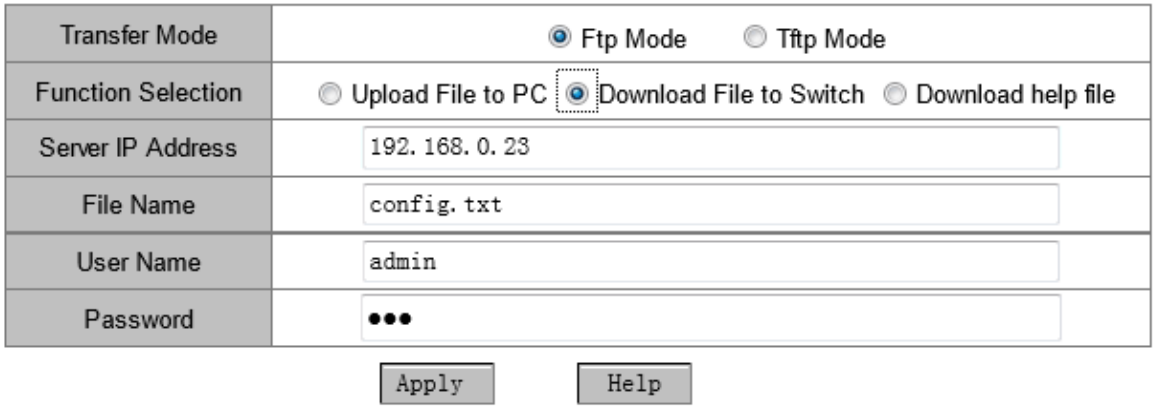


Рис. 30. Выгрузка файла с настройками в коммутатор в режиме FTP

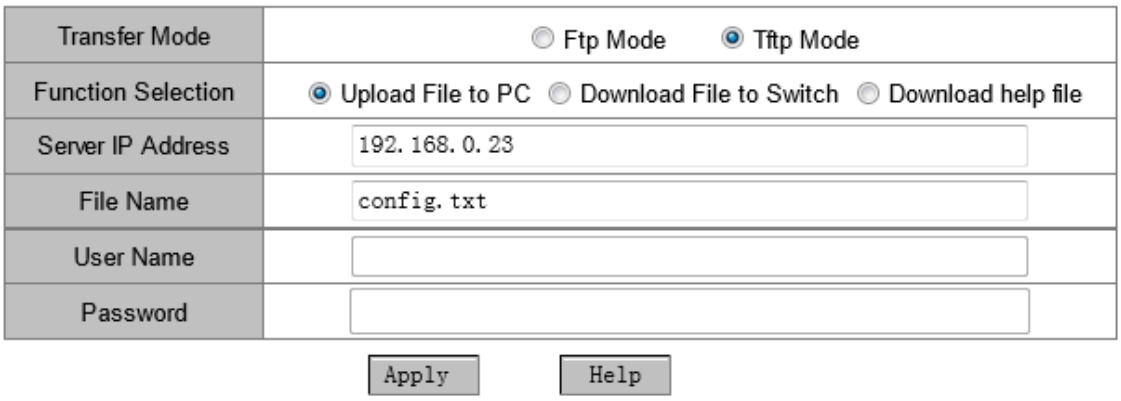


Рис. 31. Загрузка файла с настройками в режиме TFTP

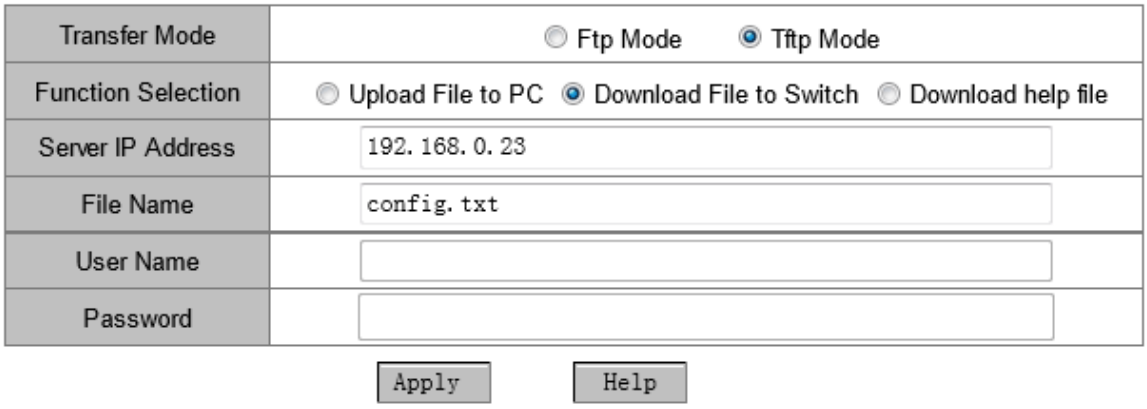


Рис. 32. Выгрузка файла с настройками в коммутатор в режиме TFTP

6. LLDP

6.1. Описание

Протокол Link Layer Discovery Protocol (LLDP) предоставляет собой стандартный метод обнаружения уровня канала (2-го уровня). Он инкапсулирует различную информацию, например, возможности устройства, адрес, идентификатор устройства и интерфейса, в

пакет Link Layer Discovery Protocol Data Unit (LLDPDU, блок данных протокола обнаружения уровня канала), и передаёт LLDPDU своим непосредственно подключённым соседям. При получении LLDPDU, соседи сохраняют эту информацию в MIB для предоставления NMS данной информации, а также информации о состоянии соединения между устройствами.

6.2. Настройка через WEB-интерфейс

1. Включите протокол LLDP:

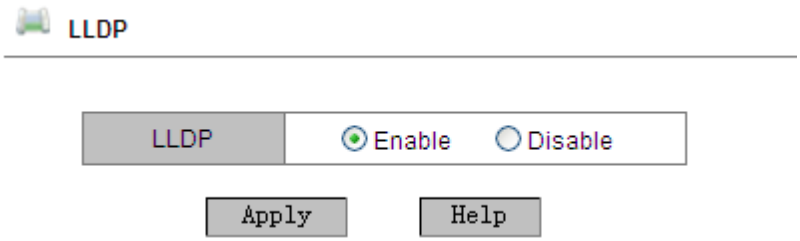


Рис. 33. Включение LLDP

Настройка LLDP
Настраиваемые опции: Enable/Disable (Включить/Выключить).
Значение по умолчанию: Enable (Включено).
Описание: Включение/Выключение протокола LLDP. Если LLDP включен, коммутатор будет передавать сообщения к соседним устройствам и, соответственно, принимать и обрабатывать сообщения LLDP от соседних устройств. Если LLDP выключен, коммутатор ни передает, ни обрабатывает сообщения LLDP.

Кроме того, если протокол LLDP включен, будет отображаться информация о соседнем устройстве, включая информацию о номере локального порта коммутатора и удаленного порта на соседнем устройстве, а также IP-адрес и MAC-адрес соседнего устройства (см. рис.34):

LLDP Information

Local Port	Remote Port	Neighbor IP	Neighbor MAC
1	1	192.168.1.4	00-72-51-73-12-88

Рис. 34. Информация LLDP

Информация о LLDP может быть показана только после того, как протокол LLDP будет включен на каждом из устройств. Т.к. данный протокол является стандартным механизмом поиска второго уровня, по умолчанию он всегда будет включен.

7. Протокол разрешения адресов (ARP)

7.1. Введение

Address Resolution Protocol (ARP) - протокол разрешения адресов, определяющий соответствие между IP адресом и MAC адресом через механизм запросов и ответов. Коммутатор может определять соответствие между IP адресом и MAC адресом других 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 серии коммутаторов поддерживает не только коммутацию на 2 уровне, но и функцию ARP, которая обеспечивает получение информации о IP адресах других устройств, находящихся в одном сегменте сети с коммутаторами, а также взаимодействия с системой управления сетью и другими управляемыми устройствами.

7.2. Описание

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.

7.3. Настройка с помощью Web-интерфейса

1. Настройте время жизни (действия, aging time) ARP:

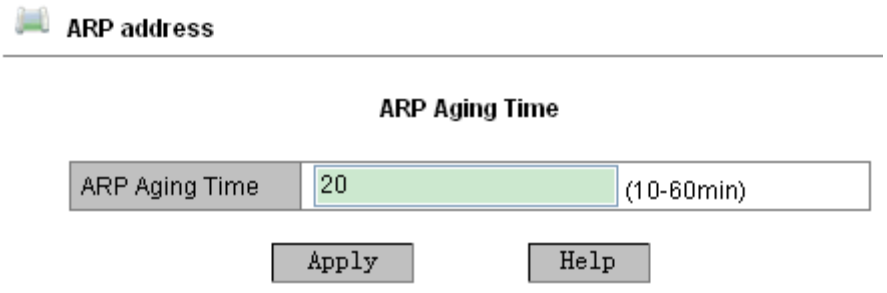


Рис. 35. Настройка времени жизни ARP

Время жизни (действия, aging time) ARP (ARP Aging Time):
Настраиваемый диапазон: 10~60 мин.
Значение по умолчанию: 20 мин.

Описание: настройка время жизни (действия, aging time) ARP. Время старта ARP начинается после добавления динамической записи ARP в таблицу адресов. Когда время закончится, эта динамическая запись будет удалена из таблицы.

2. Настройка статического адреса в записи ARP:

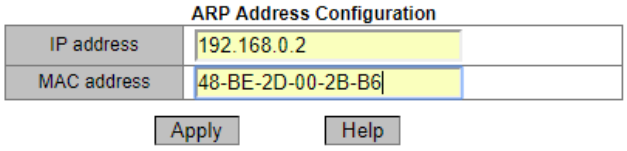


Рис. 36. Настройка статического адреса в ARP

Адрес ARP (ARP address):
Групповая настройка: {IP address, MAC address} (IP адрес, MAC адрес).
Формат: {A.B.C.D, HH-HH-HH-HH-HH-HH}. (H – шестнадцатеричный номер)
Описание: Настройка статического адреса в ARP.

- IP адрес, назначаемый для статической записи ARP, должен находиться с коммутатором в одном и том же сегменте сети.
- Когда IP адрес коммутатора назначен в статической записи ARP, система будет автоматически передавать MAC адрес коммутатора.
- Как правило, коммутатор может автоматически обнаруживать записи ARP без необходимости настройки статической записи администратором.

Отображение или удаление адреса в записи ARP:

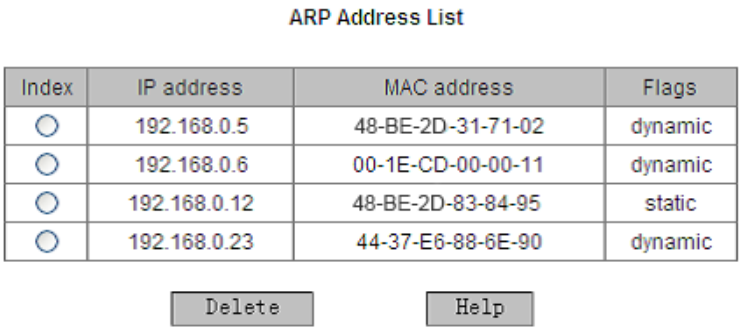


Рис. 37. Таблица адресов в ARP

Адреса ARP (ARP address):
Групповое отображение: {IP address, MAC address, Flags} (IP адрес, MAC адрес, Флаги).
Функция: отображение статических и динамических записей ARP.
Действие: Выберите статическую запись и нажмите <Delete> для удаления данной записи.

Запись динамического ARP не может быть удалена.

8. Настройка QoS

8.1. Введение

Функция QoS (Quality of Service) позволяет дифференцировать сервисы, в зависимости от разных требований в условиях ограниченной пропускной способности путём контроля трафика и управления потоком трафика в IP сетях. QoS пытается удовлетворить задачи передачи данных различных сервисов, снизить задержки в передачи данных и минимизировать эффект от задержек, в зависимости от приоритета сервиса.
Основные задачи QoS: идентификация трафика, управлением задержками передачи данных и предотвращение перегрузок в сети.
Идентификация трафика: идентификация объектов происходит в соответствии с определенными правилами. Например, объектами могут быть поля приоритетов в пакетах; приоритеты, определяемые по портам и VLAN-ам; либо другая информация о приоритетах. Идентификация трафика - основополагающая функция QoS.
Управление задержками: обязательная функция для определения важности данных. Управление задержками представляет собой комбинацию следующих техник: создание приоритетных очередей, определение последовательности передачи данных в зависимости от определённого алгоритма, что позволяет достичь приоритета передачи для самых важных сервисов.
Предотвращение перегрузок: чрезмерное количество задержек передачи данных могут повредить данным, передаваемым через сеть. Функция предотвращения перегрузок следит за использованием всех сетевых ресурсов. При обнаружении повышенного числа задержек, данная функция запускает механизм предупредительного отбрасывания пакетов и изменяет количество передаваемых данных для избавления от перегрузки сети.

8.2. Принцип работы

Каждый порт данной серии коммутаторов поддерживает 4 очереди кэширования (0, 1, 2, 3) по принципу: чем выше число - тем выше приоритет. При поступлении кадра на порт, коммутатор определяет подходящую для него очередь в зависимости от его заголовка. Коммутаторы данной серии поддерживает три режима определения соответствия очередей и приоритетов: порт, DSCP, 802.1p.

- Если для параметра Ingress Type для порта установлено значение Port, приоритет порта по умолчанию определяет очередь для сохранения сообщения. Соотношение отображения приоритета по умолчанию и очереди по умолчанию соответствует приоритету и очереди 802.1p.
- Значение DSCP зависит от части сообщения ToS/DSCP. Соотношение отображения этого приоритета и очереди может быть сконфигурировано.
- Если сообщение является тегированым, значение 802.1p зависит от приоритета тега 802.1p в сообщении. Когда сообщение является нетегированым, значение 802.1p зависит от приоритета порта по умолчанию. Можно настроить отношение отображения приоритета 802.1p и очереди.

При передаче данных, для распределения кадров по 4 приоритетным очередям порт использует режим планирования. Данные коммутаторы используют два режима постановки в очередь: WRR (Weighted Round Robin, взвешенная очередь) и приоритетные очереди SP (Strict Priority, приоритетная очередь).

- WRR распределяет данные в зависимости от взвешенного коэффициента. Размер очередей зависит от их взвешенного коэффициента. WRR отдаёт приоритет очередям с наибольшим значением коэффициента.
- Приоритетные очереди SP гарантируют, что данные с максимальным приоритетом будут передаваться в первую очередь. Как только на коммутатор поступают данные с максимальным приоритетом, устройство прекращает обработку данных с более низкими приоритетами и начинает передачу тех, что максимальным приоритетом. Только когда очередь максимального приоритета пуста, устройство переходит к передаче данных следующей по важности очереди и так далее.

8.3. Настройка через Web-интерфейс

1. Настройка QoS порта:

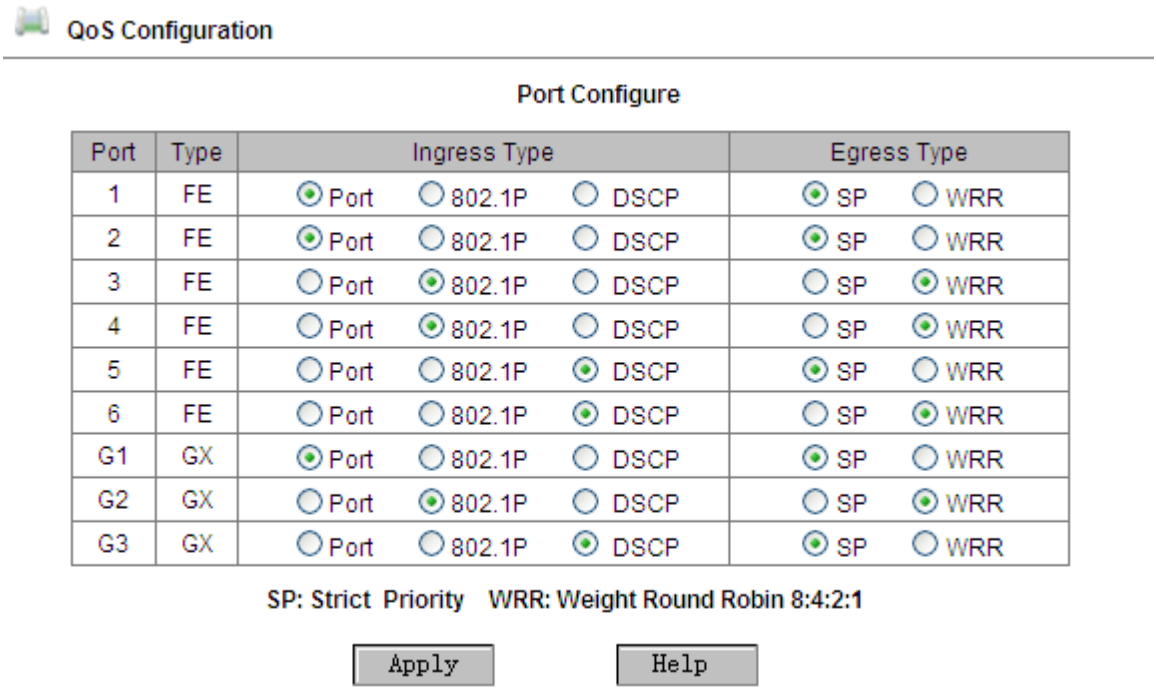


Рис. 38. Настройка порта с QoS

Настройка приоритета (Ingress Type)
Настраиваемые опции: Port/802.1p/DSCP
Значение по умолчанию: 802.1p
Описание: Настройка механизма приоритета используемого порта. Выберите только один тип механизма приоритета для каждого порта.
Настройка распределения пропускной способности (Egress Type)
Настраиваемые опции: SP / WRR
Значение по умолчанию: SP
Описание: Настройка режима распределения пропускной способности порта. SP преимущественно обрабатывает данные в очереди с высоким приоритетом; идея использования режима WRR состоит в том, что разные очереди имеют разную конфигурацию веса. В данных сериях коммутаторов порты могут принимать

фиксированное весовое соотношение: очередь 3, 2, 1, 0 соответствует весовому соотношению 8:4:2:1.

2. Настройка соотношения приоритет 802.1 p / приоритет порта к очереди.

802.1P Priority 0~7

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

Apply Help

Рис. 39. Настройка порта QoS

Приоритет 802.1P (802.1P Priority)
Групповая настройка: {Priority, Queue}
Диапазон значений: {0~7, 0~3}
Значение по умолчанию: приоритеты 0 и 1 соответствуют очереди 0; приоритеты 2 и 3 соответствуют очереди 1; приоритеты 4 и 5 соответствуют очереди 2; приоритеты 6 и 7 соответствуют очереди 3.
Описание: Настройка соотношения приоритет 802.1 p / приоритет порта к очереди.

3. Настройка соотношения приоритета DSCP к очереди

DSCP Priority 0~63

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

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

Рис. 40. Настройка соотношения приоритета DSCP к очереди

Приоритет DSCP (DSCP Priority)
Групповая настройка: {Priority, Queue}
Диапазон значений: {0~63, 0~3}
Значение по умолчанию: приоритеты 0~15 соответствует очереди 0; приоритеты 16~31 соответствуют очереди 1; приоритеты 32~47 соответствуют очереди 2; приоритеты 48~63 соответствуют очереди 3.
Описание: Настройка соотношения приоритета DSCP к очереди.

8.4. Пример типовой настройки

Как показано на рис. 41, порты 1, 2, 3, 4 пересылают сообщения в порт 5. Приоритет по умолчанию для порта 1 равен 6, а принимаемые портом 1 сообщения будут отображаться в очереди 3; принятые сообщения порта 2 с приоритетом 802.1P, равным 2, отображаются в очереди 1; принятые сообщения порта 3 с приоритетом 802.1P, равным 4, отображаются в очереди 2; принятые сообщения порта 4 с приоритетом DSCP 6 отображаются в очереди 3; порт 5 использует режим постановки в очередь WRR.

Шаги настройки коммутатора:
1. Установите в режиме Ingress Type для порта 1 значение «Port», для порта 2 и порта 3 значение «802.1P», а для порта 4 значение «DSCP»; установите в режиме Egress Type для порта 5 значение «WRR», как показано на рисунке 38.
2. Соответственно сопоставьте приоритеты 802.1P 2 и 4 с очередями 1 и 2, как показано на рисунке 39.
3. Сопоставьте DSCP приоритет 6 с очередью 3, как показано на рисунке 40.

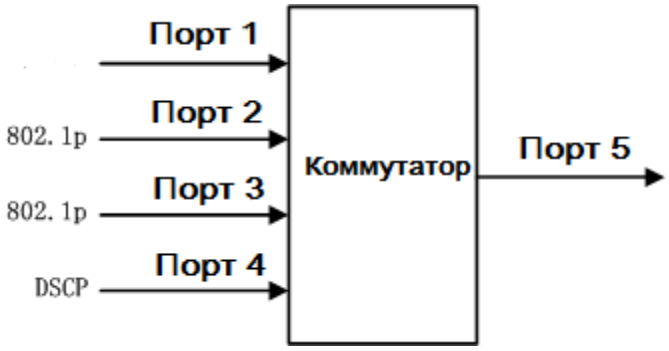


Рис. 41. Пример настройки QoS

Сообщения из порта 1 и порта 4 добавляются в очередь 3; сообщения из порта 2 добавляются в очередь 1; и сообщения из порта 3 добавляются в очередь 2. Согласно соответствующей зависимости между очередью и весом (весовое отношение очереди 1 равно 2, весовое отношение очереди 2 равно 4, весовое отношение очереди 3 равно 8), мы знаем, что отношение пропускной способности к сообщениям в очереди 1 соответствует значению 2/(2+4+8); отношение пропускной способности к сообщениям в очереди 2 соответствует значению 4/(2+4+8); отношение пропускной способности к сообщениям в очереди 3, соответствует значению 8/(2+4+8). Кроме того, все сообщения от портов 1 и 4 входят в очередь 3, поэтому они пересылаются на основе правила «First come, First go», но, конечно, общее отношение пропускной способности, выделенное для сообщений от порта 1 и порта 4, должно соответствовать значению 8/(2+4+8).

9. Транковые порты (Trunk Port)

9.1. Введение

Транковый (Trunk) порт связывает группу физических портов с одинаковой конфигурацией в один логический порт. Порты в группе не только могут использовать логический канал совместно, но также могут стать динамическим резервированием каждого канала, для повышения надежности соединения.

9.2. Реализация функции

Как показано на рис.42, три порта коммутатора А объединены (агрегированы) в Транковую группу и пропускная способность Транковой группы является общей пропускной способностью трех портов.

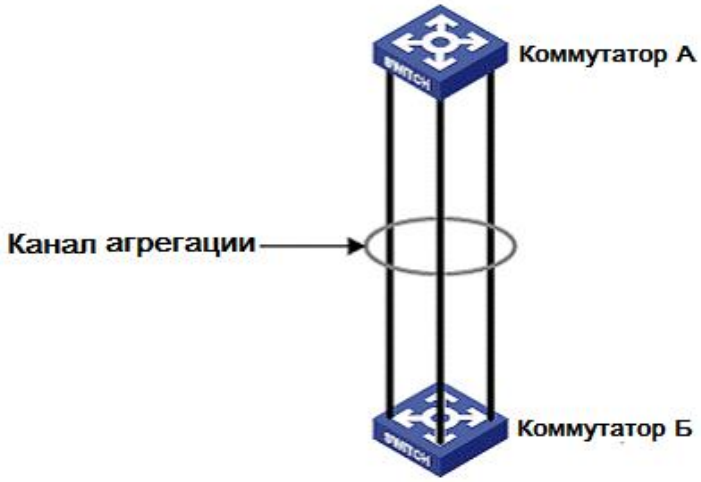


Рис. 42. Транковые порты

Когда коммутатор А передает данные для коммутатора В через агрегированный канал, транковая группа коммутатора А будет распределять потоки данных в соответствии с определенным алгоритмом, при этом только один порт будет выбран для передачи данных. Если произойдет сбой на одном из портов транковой группы, то в соответствии с алгоритмом, данные передаваемые этим портом, будут перераспределены на другой нормально работающий порт.

9.3. Описание

Режим настройки порта как транкового и следующие операции с портами и являются взаимоисключающими:

- Порт с работающим протоколом кольцевого резервирования не может быть включен в состав транковой группы. На порту, входящем в транковую группу нельзя включить протокол кольцевого резервирования, т.е. он не может быть конфигурирован как порт в составе кольца, в то же время порт с включенным протоколом кольцевого резервирования нельзя подключить к транковой группе.

- Порт с работающим протоколом многоадресной рассылки (multicast protocol) не может быть включен в состав транковой группы. На порту, входящем в транковую группу нельзя включить протокол многоадресной рассылки, соответственно порт с включенным протоколом многоадресной рассылки нельзя подключить к транковой группе.
- Порт, сконфигурированный в режиме GVRP не может быть включен в состав транковой группы. На порту, входящем в транковую группу нельзя включить режим GVRP, а порт с включенным режимом GVRP нельзя подключить к транковой группе.
- Порт, сконфигурированный в режиме статической многоадресной/одноадресной передачи (static multicast/unicast) не может быть включен в состав транковой группы. Порт, входящий в транковую группу, не может быть добавлен в статическую запись многоадресной/одноадресной рассылки, а порт, добавленный в статическую запись многоадресной/одноадресной, не может присоединиться к транковой группе.
- Порт, сконфигурированный в режиме DHCP Snooping, не может быть включен в состав транковой группы. На порту, входящему в транковую группу, нельзя включить режим DHCP Snooping, а порт сконфигурированный в режиме DHCP Snooping, нельзя включить в состав транковой группы.
- Порт, сконфигурированный в режиме зеркалирования портов, не может быть включен в состав транковой группы. На порту, входящему в транковую группу, нельзя включить режим зеркалирования портов, а порт, на котором включен режим зеркалирования портов, нельзя включить в состав транковой группы.

- Гигабитные порты данных серий коммутаторов не поддерживаю режим транковых портов.
- Порт может быть подключен только к одной транковой группе.

9.4. Настройка через WEB-интерфейс

1. Выбор режима работы транкового порта.

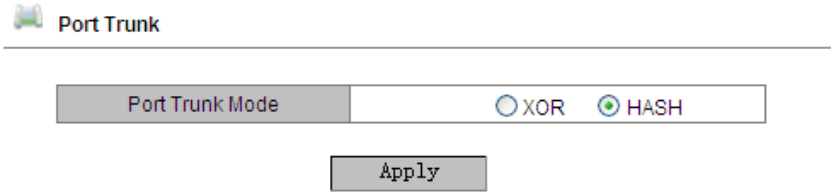


Рис. 43. Выбор режима работы транковых портов

Режим работы транкового порта (Port Trunk Mode)
Настраиваемые опции: XOR/HASH
Значение по умолчанию: HASH
Описание: Настройка порта в транковый режим (Port Trunk). Настройка порта в транковый режим определяет способ совместного использования потоков в транковой группе.

2. Настройка групп транковых портов

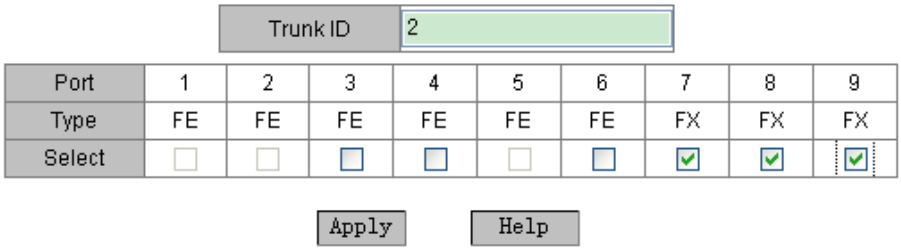


Рис. 44. Настройка групп транковых портов

Идентификатор транкового порта (Trunk ID)
Настраиваемый диапазон: 1~16
Описание: Назначение портов в транковую группу. Коммутаторы данной серии поддерживают максимум 16 транковых групп, и каждая транковая группа поддерживает максимум 4 порта.

3. Отображение списка транковых групп

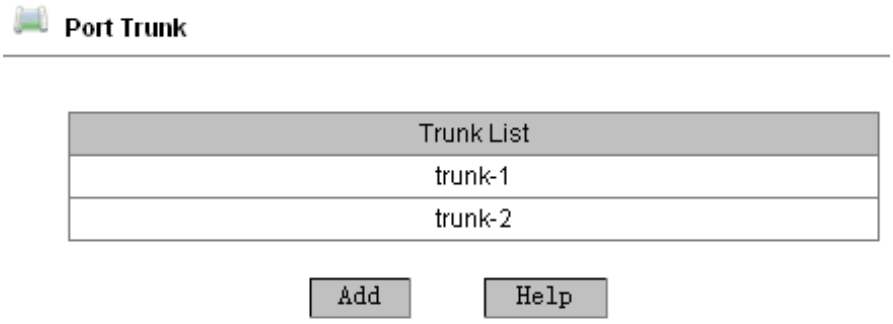


Рис. 45. Просмотр списка транковых групп

Нажмите на имя транковой группы для просмотра портов, входящих в группу, а также для изменения параметров или удаления группы.

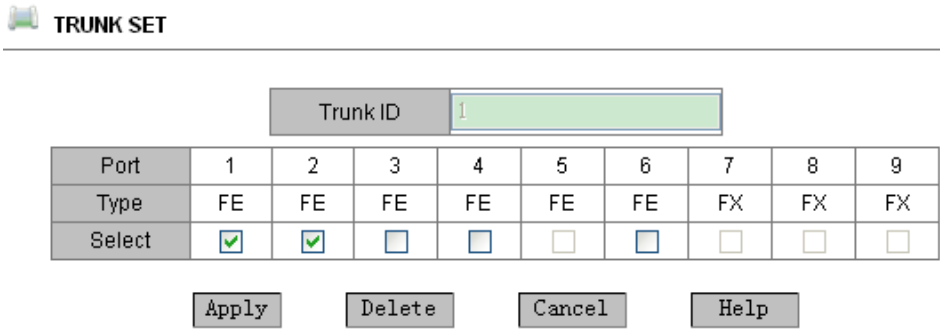


Рис. 46. Изменение параметров или удаление транковой группы

Измените список участников транковой группы (добавьте новые порты или удалите существующие). Нажмите <Apply> чтобы активировать изменения; нажмите <Delete>, чтобы удалить транковую группу.

9.5. Пример типовой настройки

Как показано на рисунке 42, три порта (порты 1, 2, 3) коммутатора A подключаются к трем портам (порты 1, 2, 3) коммутатора B для формирования транковой группы 2, чтобы реализовать разделение потоков между портами.
Настройка коммутатора:

1. Создайте транковую группу 2 в коммутаторе A и выберите порты 1, 2 и 3, чтобы назначить их участниками группы, как показано на рисунке 44.
2. Создайте транковую группу 2 в коммутаторе B и выберите порты 1, 2 и 3, чтобы назначить их участниками группы, как показано на рисунке 44.

10. Время старения MAC адреса (MAC Aging Time)

10.1. Введение

Каждый порт коммутатора имеет функцию автоматического изучения адресов. Функция предназначена для того, чтобы узнать адрес источника принимаемого кадра, включая исходный MAC-адрес и номер порта коммутатора, и сохранить его в таблице адресов. Режим времени старения (Aging Time) начинает работать после добавления динамического адреса в таблицу адресов. Если все порты коммутатора не получают кадр с этим адресом источника в течение одной или двух стадий времени старения, адрес будет удален из таблицы динамических переадресаций. Статическая таблица MAC-адресов не зависит от времени старения.

10.2. Настройка через WEB-интерфейс

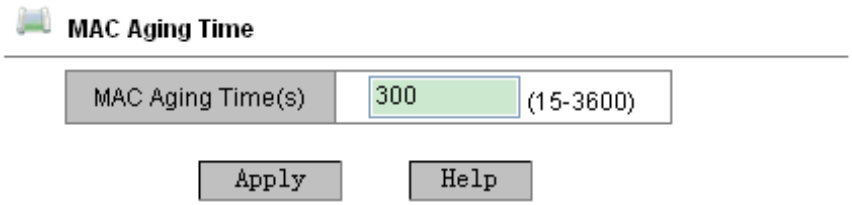


Рис. 47. Настройка времени старения MAC-адресов

Настройка времени старения (MAC Aging Time)
Диапазон значений: 15~3600 сек.
Значение по умолчанию: 300 сек.
Описание: Значение должно быть кратным 15. Пользователи могут изменить время старения в соответствии с конкретной ситуацией, чтобы эффективно использовать функцию старения MAC.

11. Скорость порта (Port Rate)

11.1. Введение

Настройка скорости порта ограничивает количество принимаемых/передаваемых сообщений и отбрасывает данные, превышающие ограничение. Порты доступа ограничивают скорость выбранных сообщений, в то время как выходные порты ограничивают скорость всех сообщений.

Ограничение скорости для пяти типов сообщений во входных портах:

- Unknown Unicast Frame (UUF): сообщение, MAC-адрес назначения которого не был изучен или не был добавлен статически;
- Unknown Multicast Frame (UMF): сообщение, MAC-адрес назначения которого не был добавлен или не был обнаружен с помощью протоколов IGMP Snooping и GMRP;
- Broadcast Frame (BF): сообщение с MAC-адресом назначения FF: FF: FF: FF: FF: FF;
- Multicast Frame (MF): сообщение, MAC-адрес назначения которого был добавлен или был обнаружен с помощью IGMP Snooping и GMRP;
- Unicast Frame (UF): одноадресное сообщение, MAC-адрес получателя которого был изучен или статически добавлен.

11.2. Реализация функции

Буфер маркеров (Token Bucket) можно рассматривать как контейнер для хранения определенного количества маркеров. Маркеры помещаются в буфер с заданной скоростью, при этом буфер имеет заданную емкость. Если количество маркеров превышает емкость буфера, то в определенный момент он будет переполнен и система остановит накопление маркеров. Каждый маркер позволяет отправлять определенное количество бит. В процессе передачи пакета количество маркеров, эквивалентное длине пакета в битах, удаляется. Если в буфере недостаточно маркеров, пакет может передаваться до тех пор, пока в буфере не будет достаточного количества маркеров или может быть сброшен.

Буфер маркеров используется при настройке скорости порта для управления потоком. Если для порта установлена скорость, перед отправкой сообщения в этом порту будут обрабатываться буфером маркеров. Если в буфере присутствует достаточное количество маркеров, сообщения будут переданы, в противном случае они будут удалены.

11.3. Настройка через WEB-интерфейс

1. Добавить настройку скорости порта

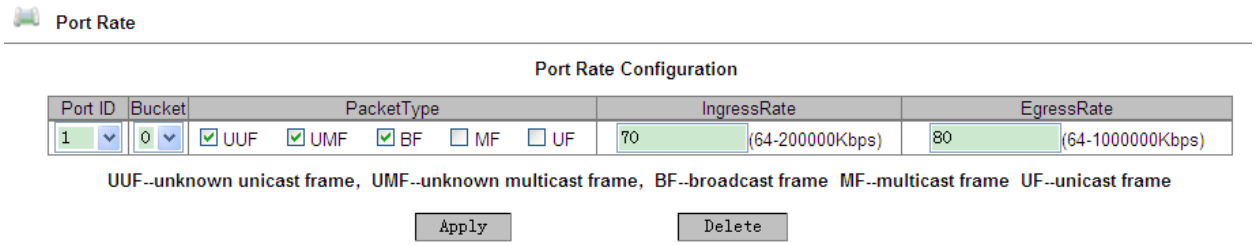


Рис. 48. Настройка скорости порта

Идентификатор порта (Port ID)
Настраиваемая опция: все порты коммутатора
Буфер (Bucket)
Настраиваемый диапазон: 0~4
Описание: настройка значений для буфера маркеров. Для каждого порта можно установить 5 разных значений маркеров.
Тип пакета (Packet Type)
Настраиваемые опции: UUF/UMF/BF/MF/UF
Описание: выбор типа пакетов, которым необходимо ограничить скорость в маркерном буфере. Одновременно можно выбрать несколько типов пакетов.
Входящий поток (Ingress Rate)
Настраиваемый диапазон: 64~200000 Кбит/с
Описание: Функция ограничения скорости входящего потока пакетов, при этом превышающие ограничение пакеты будут отброшены. Скорость входящего потока для Fast Ethernet находится в диапазоне 64~100000 Кбит/с. Скорость входящего потока порта для Gigabit Ethernet находится в диапазоне 64~200000 Кбит/с.
Исходящий поток (Egress Rate)
Настраиваемый диапазон: 64~1000000 Кбит/с
Описание: Функция ограничения скорости исходящего потока пакетов, при этом при этом выходная скорость на порту будет распределена посредством 5 буферных маркеров. Скорость исходящего потока для Fast Ethernet находится в диапазоне 64~100000 Кбит/с. Скорость исходящего потока порта для Gigabit Ethernet находится в диапазоне 64~200000 Кбит/с.

2. Удаление настройки скорости порта

Выберите метку буферного маркера для выбранного порта, как показано на рис. 48 и нажмите <Delete>, чтобы удалить конфигурацию ограничения скорости передачи пакетов в данном буфере порта.

После того, как параметр скорости входящего трафика удаляется буфера маркеров, скорость исходящего трафика порта также удаляется. Если для других буферных маркеров этого порта требуется изменить исходящую скорость, его необходимо сбросить.

3. Отображение списка настройки скорости портов.

Port ID	Bucket	PacketType	IngressRate	EgressRate
1	0	1 2 3	64Kbps	64Kbps
	1	4	66Kbps	
	2	5	68Kbps	
	3	NULL	disable	
	4	NULL	disable	
2	0	NULL	disable	disable
	1	NULL	disable	
	2	NULL	disable	
	3	NULL	disable	
	4	NULL	disable	
3	0	NULL	disable	disable
	1	NULL	disable	
	2	NULL	disable	
	3	NULL	disable	
	4	NULL	disable	

Рис. 49. Отображение списка настройки скорости портов

В колонке «Тип пакета» (PacketType) «1» означает UUF (неопознанный одноадресный кадр, Unknown unicast frame), «2» означает UMF (неопознанный многоадресный кадр, Unknown multicast frame) «3» означает BF (широковещательный кадр, Broadcast frame), «4» означает MF (многоадресный кадр, multicast frame), «5» означает UF (одноадресный кадр, Unicast frame).

11.4. Пример типовой настройки

Ограничьте скорость входящего трафика UUF, UMF и BF на порту 1 до 70 Кбит/с и установите выходную скорость порта 1 до 80 Кбит/с, соответственно они будут обработаны в буферном маркере 0. Шаги настройки: выберите порт 1, буферный маркер 0, настройте типы пакетов как UUF, UMF и BF; установите предел скорости входящего потока до 70 Кбит/с и скорость выходящего потока до 80 Кбит/с, как показано на рис. 48.

12. Резервирование

12.1. Sy2-Ring

12.1.1. Введение

Sy2-Ring и Sy2-Ring+ - проприетарные протоколы резервирования компании Symanitron. Они позволяют сети восстанавливаться менее чем за 50мс при сбое связи, обеспечивая надёжное и стабильное соединение.
Sy2-Ring бывают двух типов: кольцо, определяемое на портах (Sy2-Port-Ring), и кольцо, определяемое по VLAN (Sy2-VLAN-Ring):

- Sy2-Port-Ring: определяет порт, через который необходимо передавать или блокировать пакеты данных.

- Sy2-VLAN-Ring: определяет через который необходимо передавать или блокировать пакеты данных по определённому VLAN. Это позволяет настраивать несколько колец на одном порту, относящихся к разным VLAN.

Sy2-Port-Ring и Sy2-VLAN-Ring нельзя использовать одновременно.

12.1.2. Концепция

Концептуально протоколы работают следующим образом:

- 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 находится в режиме пересылки пакетов.
- Ведомый порт (Slave port): это порт на мастер-узле, чьё состояние меняется на рабочее позже мастер-порта. 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 режим пересылки 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 портом.
- Резервный мастер-порт (Master Backup Port): если в кольце имеется два резервных порта, резервный порт с наибольшим MAC-адресом будет резервным мастер-портом. Порт находится в состоянии пересылки пакетов.
- Резервный ведомый порт (Slave Backup Port): если в кольце два резервных порта, резервный порт с наименьшим MAC адресом будет резервным ведомым портом. Он находится в режиме отбрасывания пакетов.
- Режим перенаправления пакетов: если порт находится в режиме пересылки пакетов, он может передавать и получать данные.
- Режим отбрасывания: если порт находится в режиме отбрасывания пакетов, он может только принимать данные, но не может их передавать.

12.1.3. Реализация

1. Реализация протокола Sy2-Ring

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

Если кольцо замкнуто, мастер-порт на мастер-узле находится в режиме пересылки пакетов, а резервный порт в режиме отбрасывания пакетов; все кольцевые порты запасных узлов находятся в состоянии пересылки пакетов.

Кольцо может быть разомкнуто в следующих случаях:

- Мастер-порт мастер-узла вышел из строя. Ведомый порт мастер-узла и все кольцевые порты ведомых узлов в этом случае переходят в режим пересылки пакетов.
- Ведомый порт мастер-узла вышел из строя. Мастер-порт на мастер-узле и все кольцевые порты ведомых узлов переходят в режим пересылки пакетов.

- Другие порты вышли из строя или неисправно соединение между ними. Оба порта мастер-узла и все кольцевые порты ведомых узлов переходят в режим пересылки пакетов.

Настройки Sy2-Ring должны соответствовать следующим условиям:

- Все коммутаторы одного кольца должны иметь одинаковый номер домена.
- Каждое кольцо может иметь только один мастер-узел, но множество ведомых узлов.
- Только два порта каждого коммутатора могут быть в кольце.
- Для двух объединенных колец резервные порты могут быть настроены только в одном кольце.
- В одном кольце можно настроить максимум два резервных порта.
- На коммутаторе может быть только один резервный порт для одного кольца.
- Sy2-Port-Ring и Sy2-VLAN-Ring не могут настроены в одном коммутаторе одновременно.

Как показано на рисунке ниже, рабочие процессы коммутаторов A, B, C и D будут следующими:

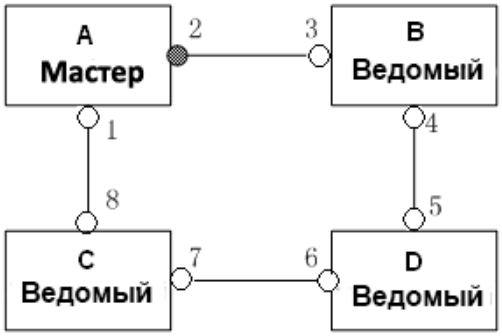


Рис. 50. Топология Sy2-Ring

1. Настройте коммутатор A как мастер-узел, а другие коммутаторы как ведомые узлы.
2. Порт 1 будет первым портом мастер-узла, у которого состояние связи изменяется на «включено» и он находится в состоянии пересылки. Порт 2 в данном случае находится в состоянии блокировки. Кольцевые порты ведомого узла находятся в состоянии пересылки.
3. В случае обрыва связи между коммутаторами C и D, статус порта 2 коммутатора A будет изменен и будет находиться в состоянии пересылки, а порты 6 и 7 коммутаторов C и D будут находиться в состоянии блокировки (см. рис. 51).

Изменение статуса соединения влияет на роли и статус портов в кольце.

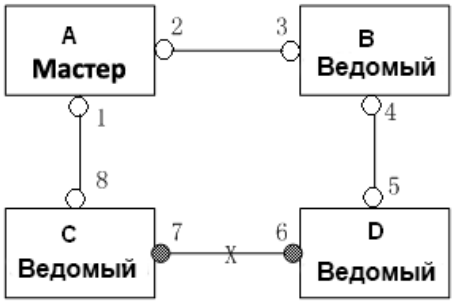


Рис. 51. Восстановление Sy2-Ring

2. Реализация протокола Sy2-Ring+

Протокол Sy2-Ring+ обеспечивает резервирование для двух колец Sy2-Ring. По одному резервному порту настроено на коммутаторе C и коммутаторе D соответственно. Какой порт будет резервным мастер-портом, зависит от MAC-адресов двух портов. Если резервный мастер-порт выходит из строя, его место займёт один из резервных ведомых портов, предотвращая возникновение колец и обеспечивая резервную связь между кольцами.

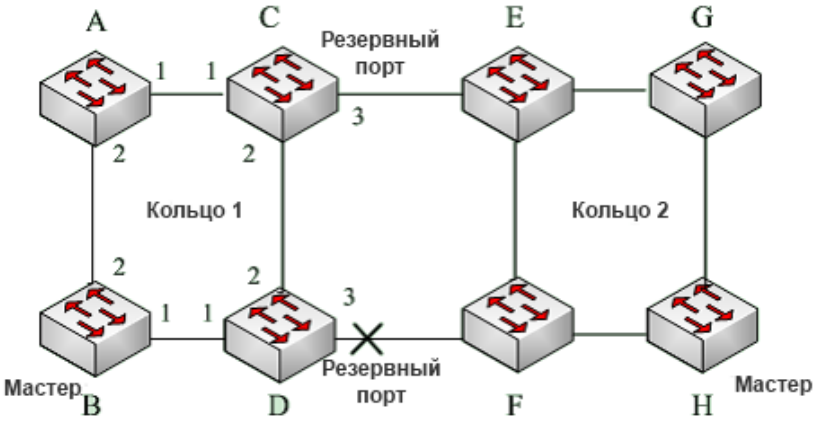


Рис. 52. Топология Sy2-Ring+

Изменение статуса соединения влияет на статус резервных портов.

3. Реализация протокола Sy2-VLAN-Ring

Протокол Sy2-VLAN-Ring дает возможность данным разных VLAN быть переданными различными путями. Каждый путь пересылки для VLAN формируется посредством Sy2-VLAN-Ring. Разные Sy2-VLAN-Ring могут иметь разные мастер-узлы. На рис. 53 показана конфигурация двух Sy2-VLAN-Ring.

Линии связи кольца DT-VLAN-Ring10: AB-BC-CD-DE-EA.

Линии связи кольца DT-VLAN-Ring20: FB-BC-CD-DE-EF.

Два кольца соприкасаются связями BC, CD, DE. Коммутаторы C и D используют одни и те же порты в двух кольцах, но при этом использую разные логические связи, которые основаны на VLAN.

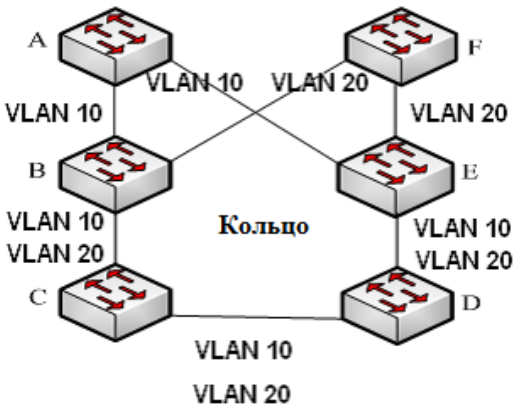


Рис. 53. Sy2-VLAN-Ring

12.1.4. Настройка режима резервирования

1. Настройка режима резервирования

Select Redundancy Mode	SY2-RING-PORT SY2-RING-VLAN
Check Loop Status	Enable Disable

Apply Help

Рис. 54. Настройка режима резервирования

Настройка режима резервирования (Select Redundancy Mode)
Настраиваемые значения: Sy2-PORT/Sy2-VLAN
Значение по умолчанию: Sy2-PORT
Описание: Включение протокола кольцевого резервирования Sy2-Ring.
Проверка статуса петли (Check Loop Status)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение и выключение определения статуса кольца. После включения определения статуса кольца коммутатор автоматически определяет статус кольца. Когда не кольцевой порт принимает пакеты Sy-Ring, порт будет заблокирован. Поэтому используйте эту функцию с осторожностью.

2. Создание и настройка кольца Sy-Ring.

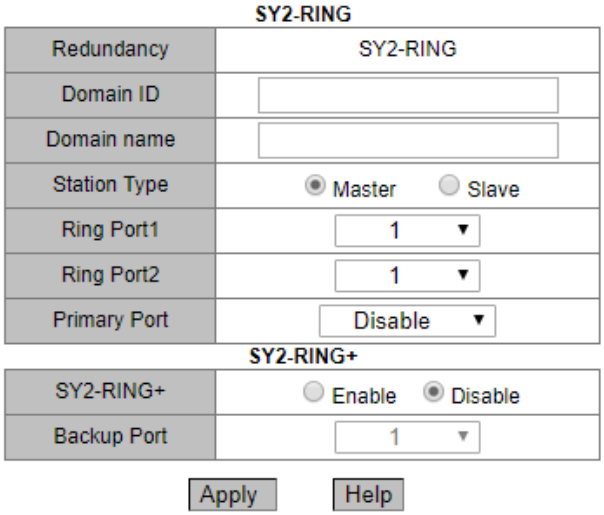


Рис. 55. Настройка Sy-Ring

Резервирование (Redundancy)
Принудительное значение: Sy2-Ring
Идентификатор домена (Domain ID)
Диапазон значений: 1~32
Описание: Идентификатор домена используется для разграничения колец. Один коммутатор поддерживает до 16 колец, определяемых по портам и до 8 колец, определяемых по VLAN.
Доменное имя (Domain name)
Диапазон значений: 1~31 символов
Описание: Назначение доменного имени.
Тип узла (Station Type)
Настраиваемые значения: Master/Slave (Мастер/Ведомый)
По умолчанию: Master (Мастер)
Описание: Выбор роли коммутатора в кольце.
Кольцевой порт 1/Кольцевой порт 2 (Ring Port1/Ring Port2)
Варианты: all switch ports (все порты коммутатора)
Описание: Выбор двух кольцевых портов.

Настройка порта в статусе транкового и в статусе кольцевого являются взаимоисключающими. Порты, добавленные в транковую группу, не могут быть настроены как кольцевые порты, а кольцевые порты не могут быть добавлены в транковую группу.

Sy2-Ring+
Настраиваемые значения: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключен)
Описание: Включение/выключение протокола Sy2-Ring+.

Резервный Порт (Backup Port)
Варианты: all switch ports (все порты коммутатора)
Описание: Настройка одного порта в качестве резервного. Вы можете настроить резервный порт только после включения функции Sy2-Ring+.

После того, как настройка завершена, кольца созданы, вы можете посмотреть информацию о Sy2-Ring:

SY2-RING List

Domain ID	Station Type	Ring Port(1,2)	Primary Port	SY2-RING+ Status	Backup Port	Change times	Ring State
a-1	master	1,2	1	Enable	3	1	RING-CLOSE
b-2	slave	4,5	Disable	Enable	6	0	----

Add Help

Рис. 56. Список Sy-Ring

3. Просмотр и модификация настроек Sy-Ring

Включите режим изменения настроек Sy-Ring, как показано на рис. 56. Вы сможете просматривать или изменять настройки кольца:

SY2-RINGConfiguration

Redundancy	SY2-RING
Domain ID	1
Domain Name	1-1
Station Type	master
Ring Port1	1
Ring Port2	2
Primary Port	Disable
SY2-RING+	Disable
Backup Port	---

Apply Delete Cancel Help

Рис. 57. Просмотр и модификация настроек Sy-Ring

После завершения изменений нажмите <Apply>, чтобы изменения вступили в силу. Вы можете удалить настройки Sy-Ring, нажав на кнопку <Delete>.
4. Просмотр статуса Sy-Ring и портов:

SY2-RING State List

Redundancy	SY2-RING
Ring Port 1	forwarding
Ring Port 2	blocking
Ring State	RING-OPEN
Clean Change times	CLEAN

Redundancy	SY2-RING+
Equipment IP	192.168.0.2
Equipment MAC	48-BE-2D-00-2B-B6
Backup Port Status	blocking

Рис. 58. Просмотр статуса Sy-Ring

12.1.5. Пример типовой настройки

Как показано на рисунке 52, коммутаторы A, B, C, D формируют кольцо 1; коммутаторы E, F, G, H формируют кольцо 2; связи CE и DF являются резервными для колец 1 и 2.
Настройка коммутатора A:

1. Домен: 1; Имя домена: Ring; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring: Disable; Резервный порт: none, как показано на рис. 55

Настройка коммутатора B:

2. Домен: 1; Имя домена: Ring; Тип узла: Master; Кольцевые порты: 1 и 2; Sy-Ring: Disable; Резервный порт: none, как показано на рис. 55

Настройка коммутаторов C и D:

3. Домен: 1; Имя домена: Ring; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring: Enable; Резервный порт: 3, как показано на рис. 55

Настройка коммутаторов E и F:

4. Домен: 2; Имя домена: Ring; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring: Enable; Резервный порт: 3, как показано на рис. 55

Настройка коммутатора G:

5. Домен: 2; Имя домена: Ring; Тип узла: Slave; Кольцевые порты: 1 и 2; Sy-Ring: Disable; Резервный порт: none, как показано на рис. 55

Настройка коммутатора H:

6. Домен: 2; Имя домена: Ring; Тип узла: Master; Кольцевые порты: 1 и 2; Sy-Ring: Disable; Резервный порт: none, как показано на рис. 55

12.2. STP/RSTP

12.2.1. Описание

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. 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 порт/порт назначения выходит из строя, его альтернативный порт/резервный порт немедленно переходит в состояние пересылки.

12.2.2. Базовая концепция

- Корневой мост: является “корнем дерева”. Сеть может иметь только один корневой мост. Какой из коммутаторов будет корневым зависит от сетевой топологии и данная ситуация может измениться при изменении топологии сети. Для определения сетевой целостности, корневой коммутатор периодически отправляет BPDU другим узлам, которые пересылают их дальше, чтобы гарантировать стабильность топологии.
- Корневой порт: 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 корневых портов нет.
- Мост назначения: устройство, которое отвечает за пересылку конфигурации BPDU другим устройствам/локальным сетям
- Порт назначения: порт на мосту назначения, который отвечает за пересылку конфигурации BPDU другому устройству или локальной сети. Все порты в корневом мосту являются портами назначения.
- Альтернативный порт: резервный порт корневого порта. Если корневой порт выходит из строя, альтернативный порт становится новым корневым.
- Резервный порт: резервный для порта назначения. Когда порт назначения выходит из строя, резервный порт становится новым портом назначения и передаёт данные вместо него.

12.2.3. Настройка BPDU

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

…	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 (ID) Корневого моста: приоритет корневого коммутатора (2 байта) + MAC-адрес корневого коммутатора (6 байт).
Стоимость пути: стоимость кратчайшего пути до корневого моста.
Идентификатор (ID) Моста назначения: приоритет назначенного коммутатора (2 байт) + MAC-адрес моста назначения (6 байт).
Идентификатор (ID) Порта назначения: приоритет порта + номер порта.
Возраст сообщения: как далеко BPDU может быть передан по сети.
Время старения: максимальное время хранения BPDU на устройстве. Когда возраст сообщения больше чем время старения, BPDU отбрасывается.
Hello интервал: интервал для отправки BPDU.
Задержка отправки: задержка изменения статуса (отбрасывание--обнаружение или обнаружение--пересылка).

12.2.4. Реализация

Процесс вычисления логического дерева для всех устройств следующий:

1. Начальная стадия: все устройства на всех своих портах генерируют BPDU, считая себя корневым мостом; ID корневого моста – это ID устройства; стоимость пути до корневого коммутатора равна 0; ID моста назначения – это ID устройства, порт назначения – локальный порт.
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 конфигурации BPDU, сгенерированный локальным портом, ниже, чем принятая конфигурация BPDU, устройство заменит содержимое BPDU конфигурации, сгенерированное локальным портом, содержимым принятой конфигурации BPDU.

Устройство выбирает оптимальную конфигурацию BPDU после сравнения конфигурации 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 коммутатором логического 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 порта назначения. В соответствии с конфигурацией BPDU и стоимостью пути корневого порта, конфигурация BPDU порта назначения рассчитывается для каждого порта:

- Идентификатор корневого моста заменяется идентификатором конфигурации BPDU корневого порта.
- Стоимость корневого пути заменяется на стоимость конфигурации BPDU корневого порта плюс соответствующая стоимость пути корневого порта.
- ID моста назначения заменяется ID устройства.
- ID порта назначения заменяется на ID данного порта.

6. Выбор порта назначения. 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 пакеты могут принимать и отправлять только техническую информацию RSTP, но не данные.

12.2.5. Настройка через WEB-интерфейс

1. Включите протокол STP/RSTP:

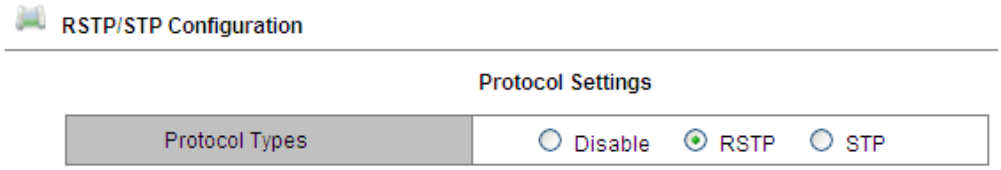


Рис. 59. Включение протокола STP/RSTP

Типы протокола (Protocol Types)
Настраиваемые опции: Disable/RSTP/STP (Выключить/RSTP/STP)
Значение по умолчанию: Выключено (Disable)
Описание: Включить или выключить протоколы RSTP или STP.

2. Настройка моста BPDU:

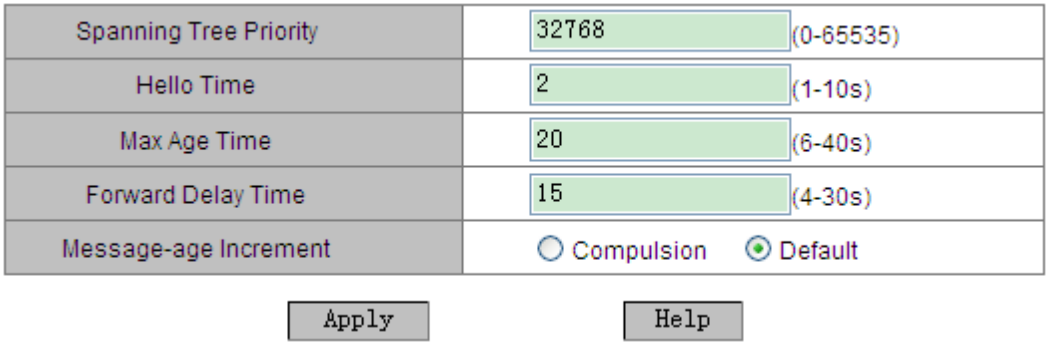


Рис. 60. Настройка моста BPDU

Приоритет STP (Spanning Tree Priority)
Настраиваемый диапазон: 0~65535 с шагом 4096.
Значение по умолчанию: 32768
Описание: Настройка приоритета сетевого моста. Приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

Интервал времени Hello (Hello Time)
Настраиваемый диапазон: 1~10 сек.
Значение по умолчанию: 2 сек.
Описание: Настройка временного интервала отправки настроек BPDU.
Максимальное время старения (Max Age Time)
Настраиваемый диапазон: 6~40 сек.
Значение по умолчанию: 20 сек.
Описание: Если значение возраста сообщения в BPDU больше указанного значения, тогда BPDU отбрасывается.
Время задержки пересылки (Forward Delay Time)
Настраиваемый диапазон: 4~30 сек.
Значение по умолчанию: 15 сек.
Описание: время изменения статуса пересылки (отбрасывание--изучение--пересылка).
Увеличение возраста сообщения (Message-age Increment)
Настраиваемые варианты: Принудительно/По умолчанию (Compulsion/Default)
Значение по умолчанию: По умолчанию (Default)
Описание: Настройка значения, которое нужно добавить в возраст сообщения, когда BPDU проходит через сетевой мост. В принудительном режиме (Compulsion) значение возраста сообщения – плюс один (plus one). В режиме «По умолчанию» (Default) значение возраста сообщения - max (максимальное время возраста / 16, 1).
Время задержки пересылки (Forward Delay Time), максимальное время старения (Max Age Time) и интервал времени Hello (Hello Time) должны удовлетворять следующим требованиям:
2 x (Время задержки пересылки – 1.0 секунда) ≥ Максимальное время старения ≥ 2 x (Время Hello + 1.0 секунда)

3. Настройка протокола RSTP, включение порта:

Port Settings

Port	Type	Protocol Status	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
1	FE	Enable / Disable	128	200000	Yes / No
2	FE	Enable / Disable	128	2000000	Yes / No
3	FE	Enable / Disable	128	2000000	Yes / No
4	FE	Enable / Disable	128	2000000	Yes / No
5	FE	Enable / Disable	128	2000000	Yes / No
6	FE	Enable / Disable	128	2000000	Yes / No
7	FX	Enable / Disable	128	200000	Yes / No
8	FX	Enable / Disable	128	200000	Yes / No
9	FX	Enable / Disable	128	200000	Yes / No

Apply Help

Рис. 61. Настройка протокола RSTP, включение порта

Статус протокола (Protocol Status)
Настраиваемые опции: Включить/Выключить (Enable/Disable)

Значение по умолчанию: Выключено (Disable)
Описание: Включение или Выключение STP/RSTP на портах.

- Порт, на котором настроена функция зеркалирования и порт с настройками кольцевых протоколов являются взаимоисключающими.
- Транковый порт и порт с настройками кольцевых протоколов являются взаимоисключающими.

Приоритет порта (Port Piority)
Настраиваемый диапазон: 0~255 с шагом 16
Значение по умолчанию: 128
Описание: Настройка приоритета порта, который определяет роль порта.
Стоимость пути (Path Cost)
Настраиваемый диапазон: 1~200000000
Значение по умолчанию: 2000000 (10M порт), 200000 (100M порт), 20000 (1000M порт)
Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от ширины полосы. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение, вручную выберите «Нет» (No) в поле «Cost Count».
Счетчик стоимости (Cost Count)
Настраиваемые варианты: Да/Нет (Yes/No)
Значение по умолчанию: Да (Yes)
Описание: если выбрано «Да», стоимость пути порта принимает значение по умолчанию; если выбрать «Нет», пользователи могут самостоятельно настроить стоимость порта.

12.2.6. Пример типовой настройки

Как показано на рисунке 62, приоритеты коммутаторов A, B, C имеют значения 0, 4096, 8192 соответственно, а стоимость пути (path cost) трех связей имеет значения 4, 5, и 10 соответственно.

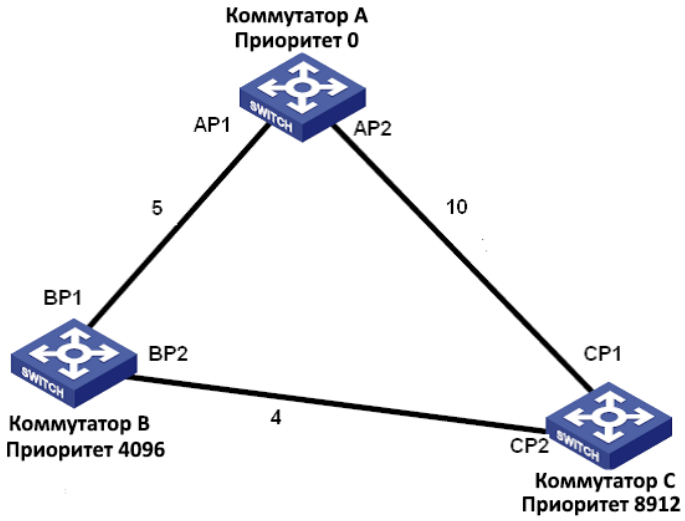


Рис. 62. Пример настройки RSTP

Настройка коммутатора A:

1. Установите значение приоритета «0», а временные параметры в значение «по умолчанию» (см. рис. 60).
2. Присвойте стоимости пути порта 1 значение 5, а стоимости пути порта 2 значение 10 (см. рис. 61).

Настройка коммутатора B:

1. Установите значение приоритета «4096» а временные параметры в значение «по умолчанию» (см. рис. 60).
2. Присвойте стоимости пути порта 1 значение 5, а стоимости пути порта 2 значение 4 (см. рис. 61).

Настройка коммутатора C:

1. Установите значение приоритета «8192» а временные параметры в значение «по умолчанию» (см. рис. 60).
2. Присвойте стоимости пути порта 1 значение 10, а стоимости пути порта 2 значение 4 (см. рис. 61).
   - Приоритет коммутатора A равен «0» и имеет наименьший ID моста, поэтому он является корневым мостом.
   - Стоимость пути от AP1 до BP1 равна 5, а стоимость пути от AP2 до BP2 равна 14, поэтому BP1 является корневым портом.
   - Стоимость пути от AP1 до CP2 равна 9, а стоимость пути от AP2 до CP1 равна 10, поэтому CP2 он является корневым портом, а BP2 – портом назначения.

12.3. Прозрачная передача STP/RSTP

12.3.1. Описание

Протокол RSTP является протоколом, стандартизированным IEEE, а Sy2-RP/Sy2-Ring - это проприетарные протоколы резервирования Симанитрон. Протоколы RSTP и Sy2-RP/Sy2-Ring не могут работать совместно. Чтобы решить эту проблему, Симанитрон разработал специальную функцию передачи RSTP/STP, которая поддерживает работу различных протоколов резервирования на коммутатор и которая позволяет прозрачно передавать сообщения протокола RSTP.

Когда на коммутаторах, у которых включены собственные протоколы резервирования, включена функция прозрачной передачи RSTP на портах, они могут принимать и пересылать сообщения протокола RSTP. Включенную на коммутаторе функцию прозрачной передачи RSTP можно рассматривать как прозрачный канал (link).

На рис. 63 коммутаторы A, B, C и D образуют кольцо Sy2-RP. После включения функции прозрачной передачи на портах коммутаторов A и B, коммутаторы E и F могут получать сообщения протокола RSTP друг от друга, обнаруживать петли и т.д.

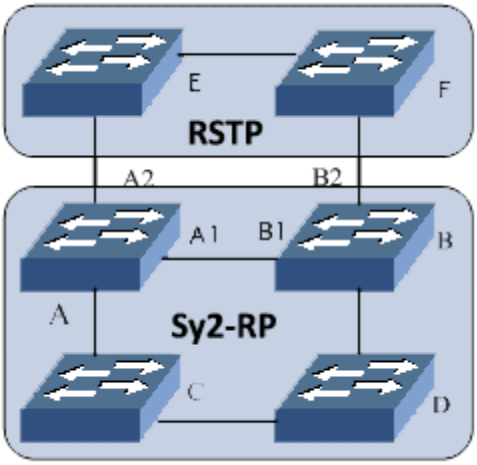


Рис. 63. Применение режима прозрачной передачи RSTP

12.3.2. Настройка через WEB-интерфейс

Настройте функцию прозрачной передачи RSTP на порту, как показано на рис. 64.

RSTP/STP Transparent Transmission

Port	Type	RSTP/STP Transparent Transmission	
1	FE	○ Enable	○ Disable
2	FE	○ Enable	○ Disable
3	FE	○ Enable	○ Disable
4	FE	○ Enable	○ Disable
5	FE	◉ Enable	○ Disable
6	FE	◉ Enable	○ Disable
7	FE	○ Enable	◉ Disable
8	FE	○ Enable	◉ Disable

Apply Help

Рис. 64. Настройка режима прозрачной передачи RSTP

Прозрачная передача RSTP/STP (RSTP/STP Transparent Transmission)
Настраиваемые опции: Выключить/Выключить (Enable/Disable)
Значение по умолчанию: Выключено (Disable)
Описание: Включить на порту функцию прозрачной передачи RSTP.

Если на порту включен протокол RSTP, функция прозрачной передачи RSTP не может быть включена.

12.3.3. Пример типовой настройки

Как показано на рисунке 63, коммутаторы A, B, C и D формируют кольцо Sy2-RP; коммутаторы E и F, формируют кольцо RSTP, в котором коммутаторы A и B формируют канал прозрачной передачи сообщений протокола RSTP от коммутатора E или коммутатора F.

- Коммутаторы A, B, C и D формируют резервное кольцо Sy2-RP, а настройка выполняется поэтапно в разделе «Sy2-RP Configuration».
- Необходимо включить протокол RSTP на соответствующих портах коммутаторов E и F (см. рис. 59 и 61).
- Необходимо включить функцию прозрачной передачи RSTP на портах A1, A2, B1, B2 у коммутаторов A и B (см. рис. 64).

12.4. Резервирование Sy2-RP

12.4.1. Описание

Symanitron разработал Sy2-RP (Symanitron Redundancy Protocol) для передачи данных в кольцевых сетях. Протокол может предотвращать широковещательные штормы в кольцевых топологиях. Если связь или узел выходят из строя, вместо них задействуется резервная связь, обеспечивающая бесперебойную передачу данных.
Протокол Sy2-RP совместим со стандартом IEC 62439-6. Один коммутатор может являться частью сразу нескольких колец Sy2-RP.

12.4.2. Концепция

- INIT: начальное состояние коммутатора.
- Root (Корневой): в кольце может быть только один корневой коммутатор. Корневой коммутатор выбирается в сети автоматически после автоматического обнаружения (auto-learning). Значение «корневой» (Root) для коммутатора не является фиксированным и может быть передано другому коммутатору при изменении топологии сети. Корневой коммутатор периодически отправляет сообщение «Announce», а другие устройства перенаправляют это сообщение для того, чтобы гарантировать стабильность сетевой топологии и работы кольца в целом. 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 "Normal" или "B-Root", в зависимости от состояния соединения и CRC деградации порта.
- B-Root: коммутатор, у которого кольцевой порт находится либо в выключенном состоянии (link-down), либо кольцевой порт неисправен (это означает, что количество сообщений CRC превышает пороговое значение). B-Root сравнивает и передаёт пакеты "Announce". Если вектор полученного пакета "Announce" меньше, чем собственный пакет "Announce", B-Root меняет свою роль на Root, в противном случае он передаёт полученный пакет и не меняет собственной роли.
- Normal (Обычный): обозначает устройство, на котором Sy2-RP включен и оба порта активны без CRC деградации. Обычные коммутаторы только передают пакеты "Announce", без проверки содержимого.

- Backup port (Резервный порт): это порты связи между кольцами Sy2-RP. Можно настроить два или более резервных портов. При этом все резервные порты должны принадлежать одному кольцу Sy2-RP. Резервный порт, у которого в первую очередь устанавливается связь, является мастером (Master) и он находится в состоянии «Forward». Другие резервные порты – это подчиненные резервные порты (Slave), которые находятся в «заблокированном» состоянии (Block).

12.4.3. Реализация

Протокол Sy2-RP определяет роли коммутатора посредством пересылки сообщений "Announce" для того, чтобы гарантировать работу резервированной сети и отсутствие в ней «петель».
Конфигурация Sy2-RP должна удовлетворять следующим условиям:

- Все коммутаторы в кольце должны иметь одинаковый идентификатор (ID) домена;
- В кольце должен быть один, и только один корневой (Root) коммутатор, но при этом может быть несколько коммутаторов B-Root или Normal;
- В каждом из коммутаторов в кольце может быть только два кольцевых порта;
- Для двух объединенных колец резервные порты можно настроить только в одном кольце;
- В кольце можно использовать несколько резервных портов;
- В каждом из коммутаторов в кольце можно настроить только один резервный порт.

На рис. 65 отображен процесс работы Sy2-RP.

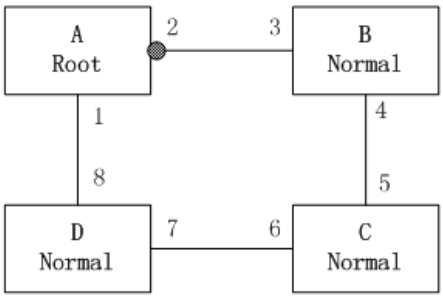


Рис. 65. Топология Sy2-RP

1. В исходном состоянии все переключатели находятся в состоянии INIT.
2. Коммутаторы в кольце сравнивают сообщение "Announce", которое пересылается между ними, а затем выбирают коммутатор «A», который должен быть корневым (Root) исходя из наиболее оптимальной конфигурации. Кольцевой порт 1 в корневом коммутаторе, который в первую очередь устанавливает связь, будет портом пересылки (Forwarding), в то же время кольцевой порт 2 будет находиться в состоянии блокировки (Block). Остальные коммутаторы будут либо B-Root, либо Normal. Два кольцевых порта в B-Root/Normal при этом находятся в состоянии пересылки (Forward).
3. Когда происходит обрыв связи CD (соединение между коммутаторами C и D), как показано на рис. 66, коммутатор A изменит свой статус от корневого (Root) до Normal, а все устройства будут ожидать назначения корневого коммутатора. В этот момент

коммутаторы C или D будут назначены новым корневым коммутатором. Если коммутатор D является корневым, коммутатор C будет назначен B-Root, а порты 6 и 7 заблокированы.

Изменение состояния связи влияет на состояние всех кольцевых портов.

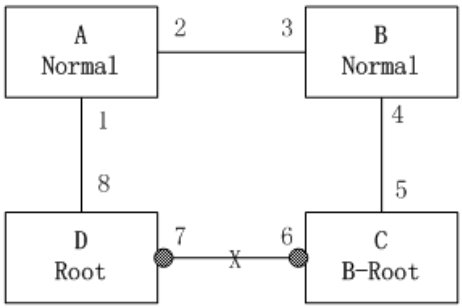


Рис. 66. Восстановление Sy2-RP

Протокол Sy2-RP может обеспечивать резервирование между двумя кольцами Sy2-RP. Как показано на рисунке 67, каждый коммутатор может настроить резервный порт. Главный резервный порт - это порт пересылки, а остальные резервные порты заблокированы. Если мастер-порт или ссылка на резервный порт не работает, система выберет подчиненный резервный порт для пересылки данных, гарантируя нормальную связь между резервными кольцами.

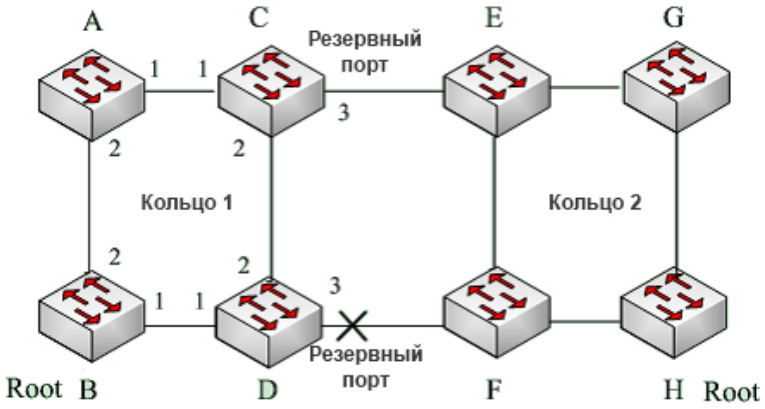


Рис. 67. Резервирование Sy2-RP

Изменение состояния связи влияет на состояние резервных портов.

12.4.4. Настройка через WEB-интерфейс

1. Настройка Sy2-RP:

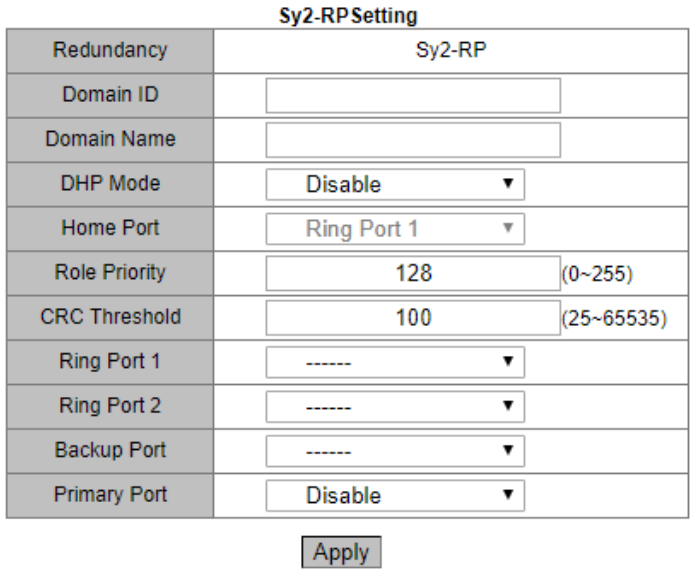


Рис. 68. Резервирование Sy2-RP

Резервирование (Redundancy)
Обязательная настройка: Sy2-RP
Идентификатор домена (Domain ID)
Настраиваемый диапазон: 1~32
Описание: Идентификатор домена используется для распознавания различных колец. Один коммутатор поддерживает не более 16 колец Sy2-RP
Имя домена (Domain Name)
Настраиваемый диапазон: 1~31 символов
Описание: Настройка имени домена.
Режим DHP (DHP Mode)
Настраиваемые опции: Disable/Normal Node/Home Node
Значение по умолчанию: Disable (Выключено)
Описание: включение/выключение режима DHP и настройка режима DHCP.
«Домашний» порт DHP (DHP Home Port)
Настраиваемые варианты: Ring Port 1/Ring Port 2/Ring Port 1-2 (Кольцевой порт 1/Кольцевой порт 2/Кольцевой порт 1-2)
Значение по умолчанию: Ring Port 1 (Кольцевой порт 1)
Описание: Если связь (link) DHP является связью одиночного узла, оба кольцевых порта могут быть сконфигурированы как Home-port.
Приоритет роли (Role Priority)
Настраиваемый диапазон: 0~255
Значение по умолчанию: 128
Описание: настройка приоритета коммутатора.
Пороговое значение CRC (CRC Threshold)
Настраиваемый диапазон: 25~65535
Значение по умолчанию: 100
Описание: настройка порогового значения CRC.
Кольцевой порт 1/Кольцевой порт 2 (Ring Port 1/Ring Port 2)
Настраиваемые опции: все порты коммутатора

Описание: выбор двух кольцевых портов.

- Одновременная настройка порта как порта зеркалирования и как кольцевого порта являются взаимоисключающими.
- Настройка порта в режиме транкового и в режиме кольцевого являются взаимоисключающими. Порт, находящийся в транковой группе, не может быть кольцевым, а кольцевой порт не может быть включен в транковую группу.

Резервный порт (Backup Port)
Настраиваемые опции: все порты коммутатора
Описание: настройка резервного порта.

Резервный порт нельзя выбрать из тех портов, которые не являются кольцевыми.

После выполненных настроек созданное кольцо будет отображаться в списке Sy2-RP, как показано на рис. 69.

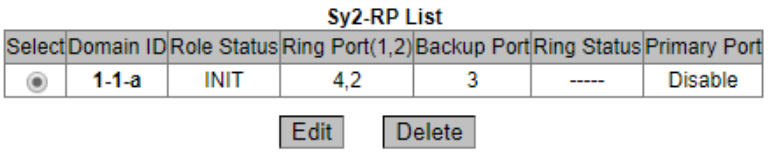


Рис. 69. Список Sy2-RP

2. Нажмите на кнопку идентификатора домена (Domain ID), чтобы отобразить детальные настройки кольца, а также изменить его настройки, как показано на рис. 70.

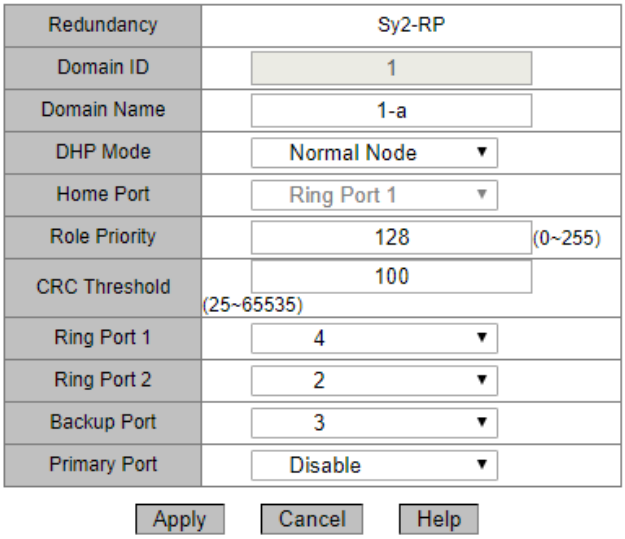


Рис. 70. Отображение и изменение настроек Sy2-RP

После выполнения настроек нажмите <Apply> для активации изменений; нажмите <Delete>, чтобы удалить настройки.

3. Отображение статуса роли коммутатора и статуса порта в кольце Sy2-RP:

Sy2-RP Status

Role Status	INIT
Ring Port 1	BLOCK
Ring Port 2	BLOCK
Backup Port	BLOCK
Ring Status	-----
IP Address	192.168.0.2
MAC Address	48-BE-2D-00-2B-B6
ROOT IP	0.0.0.0

Рис. 71. Статус Sy2-RP

12.4.5. Пример типовой настройки

Как показано на рис. 67, коммутаторы A, B, C и D формируют Кольцо 1; коммутаторы E, F, G, H формируют Кольцо 2. Связи CE и DF являются резервными линиями связи между Кольцом 1 и Кольцом 2.

- Настройка коммутаторов A и D:

ID домена: 1; Имя домена: Ring. Приоритет порта является настройкой по умолчанию. Кольцевой порт: Порт 1 и Порт 2. Как показано на рис. 68, нет необходимости настраивать резервный порт.

- Настройка коммутаторов C и D:

ID домена: 1; Имя домена: Ring. Приоритет порта является настройкой по умолчанию. Кольцевой порт: Порт 1 и Порт 2. Резервный порт: порт 3, как показано на рис. 68.

- Настройка коммутаторов E, F, G, H:

ID домена: 2; Имя домена: Ring. Приоритет порта является настройкой по умолчанию. Кольцевой порт: Порт 1 и Порт 2. Как показано на рис. 68, нет необходимости настраивать резервный порт.

13. Многоадресная передача (Multicast)

13.1. GMRP

13.1.1. Введение

Протокол GARP (Generic Attribute Registration Protocol) используется для распространения, регистрации и удаления определённой информации (VLAN, адреса мультикастовых групп) между коммутаторами в сети. Протокол GARP использует два приложения: GVRP (GARP VLAN Registration Protocol) и GMRP (GARP Multicast Registration Protocol). Более подробное

описание протокола GVRP можно почитать в соответствующем разделе данного руководства.

Благодаря механизму GARP, информация о настройках коммутатора может быть передана по всей локальной сети. Устройства, поддерживающие GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих сообщений «Join» и «Leave». При этом GARP может регистрировать или отменять информацию о настройках других членов в соответствии с их сообщениями «Join/ Leave».

GARP предусматривает три типа сообщений: «Join», «Leave» и «Leave All».

- Когда GARP устройство хочет передать свои настройки другим коммутаторам, оно отсылает сообщение «Join». Сообщения «Join» бывают двух типов: «Join Empty» и «Join In». Сообщение «Join In» отправляется для зарегистрированных настроек, в то время как «Join Empty» - для настроек, которые ещё не были зарегистрированы.
- Когда GARP устройство хочет удалить свои настройки с других коммутаторов, оно отправляет сообщение «Leave».
- После запуска GARP, он начинает отсчитывать период «Leave All». Когда период заканчивается, устройство отсылает сообщение «Leave All».

Таймеры GARP включают таймеры «Hold», «Join», «Leave» и «Leave All».

- Таймер Hold: При получении сообщения о регистрации настроек, приложение GARP не отправляет сообщение «Join» сразу, а запускает таймер «Hold». Когда таймер заканчивает отсчёт, приложение отправляет все полученные сообщения о настройках, полученные за этот период в одном «Join» сообщении, что уменьшает количество передаваемых данных по сети.
- Таймер Join: Чтобы гарантировать, что сообщения «Join» может быть надежно передано другим коммутаторам, коммутатор с включенным GARP будет ожидать временной интервал таймера «Join» после передачи первого сообщения «Join». Если в течение в ответ не получено сообщение «JoinIn», приложение снова отправляет сообщение «Join». В противном случае, сообщение «Join» не отправляется.
- Таймер Leave: Когда коммутатор с включенным GARP хочет, чтобы другие коммутаторы удалили информацию о настроках, он отсылает «Leave» сообщение. Коммутаторы, получившее это сообщение, запускают таймер «Leave». Если они не получат ни одного сообщения «Join» до истечения времени таймера, коммутаторы удаляют эту информацию о настройках.
- Таймер Leave All: При запуске GARP приложения, запускается таймер «Leave All». По его истечении, приложение отправляет сообщение «Leave All» другим коммутаторам с включенным GARP для того, чтобы они могли перерегистрировать всю свою информацию о настройках. После этого, приложение запускает таймер LeaveAll заново, чтобы начать новый цикл.

13.1.2. Протокол GMRP

GARP Multicast Registration Protocol (GMRP) - протокол регистрации многоадресной передачи, основанный на принципах GARP. Он используется для управления информацией о многоадресных группах коммутаторов. Все коммутаторы, поддерживающие GMRP, могут получать регистрационную информацию от других коммутаторов, динамически обновлять информацию о зарегистрированных

многоадресных группах, а также передавать собственную регистрационную информацию другим коммутаторам. Механизм обмена информацией гарантирует единообразие информации о многоадресных группах для всех коммутаторов сети.
Если коммутатор регистрирует или отменяет регистрацию в многоадресной группе, порт с поддержкой GMRP передаёт информацию на другие порты в том же VLAN.

13.1.3. Описание

Порт-агент: обозначает порт, на котором включены функции GMRP и агента.
Порт распространения: обозначает порт, на котором включена только функция GMRP, без функции агента.
Для GMRP необходимо наличие одного и нескольких портов-агентов. Динамически полученные многоадресные записи GMRP и информация об агенте передаётся портом распространения на порты распространения следующих устройств.
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 «Leave All».

13.1.4. Настройка через WEB-интерфейс

1. Включите протокол GMRP, как показано на рис. 72.

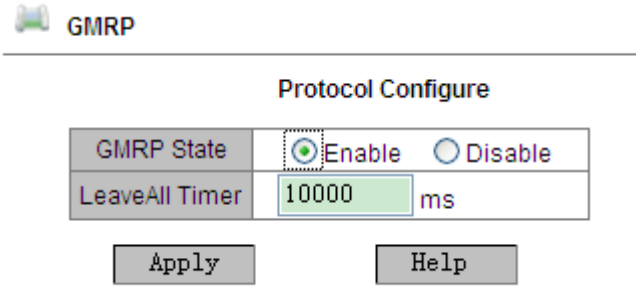


Рис. 72. Включение/Выключение GMRP

Функция GMRP (GMRP State)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение/выключение функции GMRP. Протокол не может работать одновременно с протоколом IGMP Snooping.
Таймер Leave-All (LeaveAll Timer)
Настраиваемый диапазон (мс): 100~327600
Значение по умолчанию: 10000 мс.
Описание: Настройка временного интервала для отправки сообщений «Leave All». Интервал должен быть кратен 100.

Примечание: если на разных устройствах таймеры «Leave All» истекут одновременно, они отправят множество сообщений «Leave All» одновременно. Для того чтобы избежать подобной ситуации, которая может повысить нагрузку на сеть, рабочее значение

таймеров «Leave All» должно быть случайным значением, которое больше изначального значения таймера «Leave All», но меньше чем 1,5 значения этого таймера.

2. Настройка функции GMPR для каждого порта.

Port Configure

Port	Type	GMRP Enable	Agent Enable	Hold Timer	Join Timer	Leave Timer
1	FE	(•) Enable ( ) Disable	(•) Enable ( ) Disable	100 ms	500 ms	3000 ms
2	FE	(•) Enable ( ) Disable	( ) Enable (•) Disable	100 ms	500 ms	3000 ms
3	FE	(•) Enable ( ) Disable	( ) Enable (•) Disable	100 ms	500 ms	3000 ms
4	FE	(•) Enable ( ) Disable	( ) Enable (•) Disable	100 ms	500 ms	3000 ms
5	FE	( ) Enable (•) Disable	( ) Enable ( ) Disable	100 ms	500 ms	3000 ms
6	FE	( ) Enable (•) Disable	( ) Enable ( ) Disable	100 ms	500 ms	3000 ms
7	FE	( ) Enable (•) Disable	( ) Enable ( ) Disable	100 ms	500 ms	3000 ms
8	FE	( ) Enable (•) Disable	( ) Enable ( ) Disable	100 ms	500 ms	3000 ms

Apply Help

Рис. 73. Настройка GMRP на портах

Функция GMRP на порту (GMRP Enable)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение или выключение функции GMRP на порту.
Функция агента GMRP (Agent Enable)
Варианты: Enable/Disable (Включить/Выключить)
По умолчанию: Disable (Выключено)
Описание: Включение или выключение функции агента GMRP на порту.

- Порт-агент не может распространять информацию об агенте.
- До включения функции GMRP агента нужно включить функцию GMRP на данном порту.

Таймер Hold (Hold Timer)
Настраиваемый диапазон (мс): 100~327600
Значение по умолчанию: 100 мс
Описание: Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение для всех GMRP портов.
Таймер Join (Join Timer)
Настраиваемый диапазон (мс): 100~327600
Значение по умолчанию: 500 мс
Описание: Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение для всех GMRP портов.
Таймер Leave (Leave Timer)
Настраиваемый диапазон (мс): 100~327600
Значение по умолчанию: 3000 мс

Описание: Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение для всех GMRP портов.

3. Добавление записи GMRP агента.

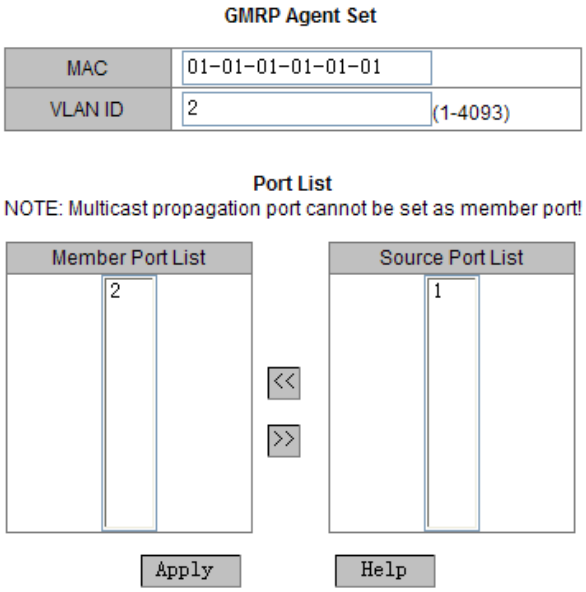


Рис. 74. Настройка записи GMRP агента

MAC адрес (MAC)
Настраиваемый формат: FF-FF-FF-FF-FF-FF (F - это шестнадцатеричное число)
Описание: Настройка MAC-адреса многоадресной группы. Наименее значимый бит первого байта равен 1.
Идентификатор VLAN (VLAN ID)
Настраиваемые опции: все созданные идентификаторы VLAN-ы
Описание: Настройка VLAN ID для GMRP агента. Информация о GMRP агенте может передаваться только через порты распространения с тем же VLAN ID, что и у порта-агента. VLAN ID агента является копией сообщения VLAN ID. Порт распространения на другой стороне может либо знать запись агента либо нет. Это зависит от того, является ли VLAN ID агента таким же, как и для портов распространения с обеих сторон.
Список портов участников (Member Port List)
Выбор портов участников для записей агента и выбор портов агента.
Список портов источников (Source Port List)
Настраиваемые опции: все порты с поддержкой GMRP агента.

4. Отображение, изменение и удаление записей GMRP агентов.

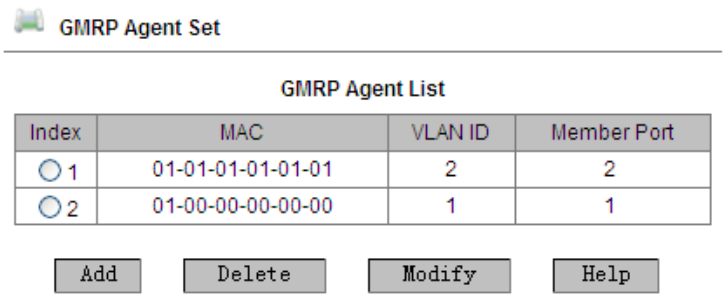


Рис. 75. Операции с GMRP агентом

На рис. 75 показаны MAC агента, VLAN ID и порты участники. Нажмите <Delete> для удаления соответствующей записи; нажмите <Modify> для изменения портов участников записи агента.

5. Проверка участников многоадресных групп агента на подключенном соседнем устройстве.

Их статус должен удовлетворять следующим условиям:

- На подключенных устройствах должна быть включена функция GMRP.
- Два порта, которые соединяют два устройства, должны быть портами распространения.

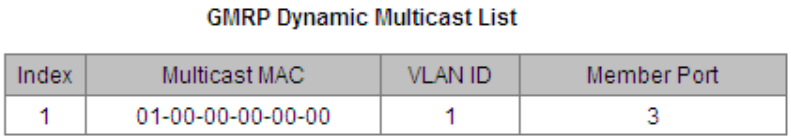


Рис. 75. Таблица многоадресных динамических GMRP

Список многоадресных динамических GMRP (GMRP Dynamic Multicast List)
Групповое отображение: {Index, Multicast MAC, VLAN ID, Member Port}
Описание: Отображение многоадресных динамических записей GMRP.

13.1.5. Пример типовой настройки

Как показано на рисунке 77, коммутаторы A и B соединены между собой портом 2 каждый. Порт 1 коммутатора A настроен как агент порт и содержит две многоадресных записи:

- MAC адрес: 01-00-00-00-00-01, VLAN: 1
- MAC адрес: 01-00-00-00-00-02, VLAN: 2

Для того, чтобы увидеть динамическую регистрацию между коммутаторами и обновление информации о многоадресной рассылке, необходимо установить различные значение VLAN для портов.

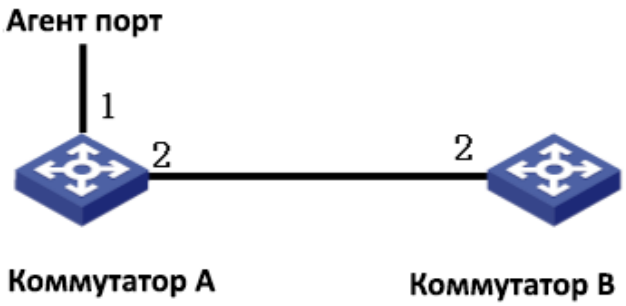


Рис. 77. Сеть GMRP

Настройка коммутатора A:

1. Включите функцию GMRP на коммутаторе A; используйте значение «По умолчанию» для таймера «Leave All» (см. рис. 72);
2. Включите функцию GMRP и функцию агента на порту 1; на порту 2 включите только функцию GMRP; все таймеры должны быть установлены в режим «По умолчанию» (см. рис. 73);
3. Настройте запись многоадресного агента. <MAC address, VLAN ID, Member port> настройте как {01 -00-00-00-00-01, 1, 1> и {01 -00-00-00-00-02, 2, 1} (см. рис. 74).

Настройка коммутатора B:

1. Включите функцию GMRP на коммутаторе B; используйте значение «По умолчанию» для таймера «Leave All» (см. рис. 72);
2. Включите функцию GMRP на порту 2; все таймеры должны быть установлены в режим «По умолчанию» (см. рис. 73);

Динамические записи многоадресной передачи GMRP в коммутаторе B показаны в таблице:

Свойства порта 2 коммутатора A	**Свойства порта 2 коммутатора B**	**Многоадресные записи коммутатора-приемника B**
Untag1	Untag1	MAC: 01-00-00-00-00-01 VLAN ID: 1 Member port: 2
Untag2	Untag2	MAC: 01-00-00-00-00-02 VLAN ID: 2 Member port: 2
Untag1	Untag2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Member port: 2

13.2. Статическая многоадресная таблица (FDB)

13.2.1. Введение

Многоадресная таблица может быть настроена статически. Запись добавляется в таблицу адресов многоадресной рассылки в виде {VLAN ID, Multicast MAC-address, Multicast member port}, а многоадресное сообщение будет перенаправлено к соответствующему порту участнику согласно записи.

13.2.2. Настройка через WEB-интерфейс

1. Включение статической многоадресной таблицы.

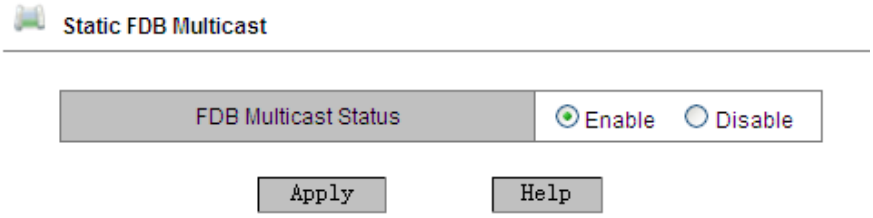


Рис. 78. Статическая многоадресная таблица FDB

Статус FDB (FDB Multicast Status)
Настраиваемые варианты: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение/Выключение статической многоадресной таблицы.

2. Добавление статической многоадресной записи

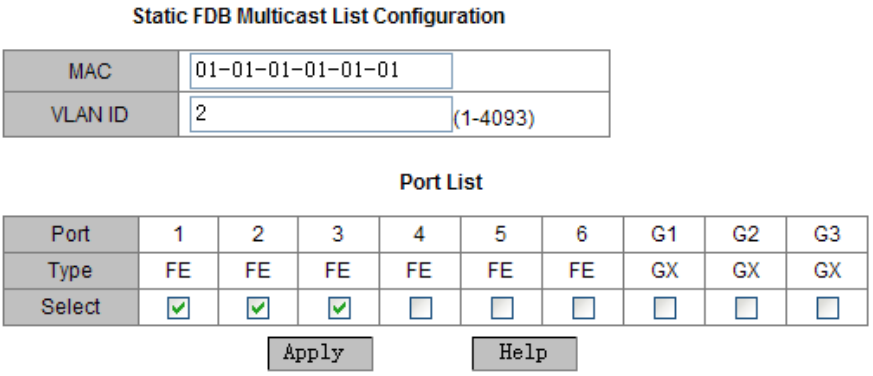


Рис. 79. Добавление записей в статическую многоадресную таблицу

MAC адрес (MAC)
Настраиваемый формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число);
Описание: Настройка группового адреса группы. Самый младший бит старшего байта равен 1.
Идентификатор VLAN (VLAN ID)
Настраиваемые опции: все созданные VLAN ID;

Описание: Установка VLAN ID для записи статической многоадресной рассылки. Только порты-члены VLAN могут пересылать это многоадресное сообщение.

Список портов (Port List)

Описание: Выбор портов участников многоадресной рассылки. Если хост, подключенный к порту, хочет получить соответствующие данные многоадресной группы, необходимо добавить статически этот порт в группу многоадресной рассылки и назначить статическим портом участником группы.

3. Просмотр, изменение и удаление статических многоадресных записей.

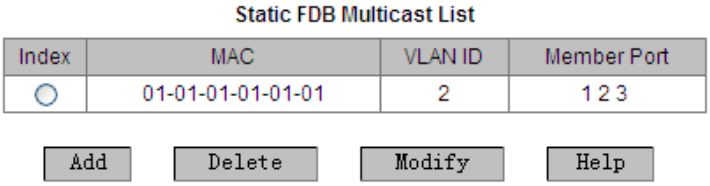


Рис. 80. Операции с записями статической многоадресной группы

В списке записей статической многоадресной рассылки отображаются MAC адрес, идентификатор (ID) VLAN и порты участники. Выберите запись, нажмите <Delete> для удаления записи; нажмите <Modify> ля изменения портов участников записи.

13.3. IMGP Snooping

13.3.1. Введение

IGMP Snooping (Internet Group Management Protocol Snooping) - многоадресный протокол второго уровня, работающий на уровне канала передачи данных. Он используется для управления и настройки многоадресных групп передачи данных. Коммутаторы с поддержкой IGMP Snooping анализируют принимаемые IGMP пакеты, устанавливают соответствие между портами и MAC-адресами многоадресной рассылки и отправляют многоадресные сообщения согласно этим соответствием.

13.3.2. Концепция

- Мастер запросов: периодически отправляет IGMP запросы для проверки и обновления информации о многоадресных группах чтобы узнать активны ли они и обеспечить поддержку групповой передачи. 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 запросы (на IGMP-коммутаторе) от мастера. При получении IGMP ответа, коммутатор инициализирует многоадресную 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.

13.3.3. Принцип работы

IGMP Snooping управляет членами многоадресных групп путём обмена пакетами между поддерживающих IGMP устройств. Данные запросы содержат следующие важные сообщения:

- Сообщение с общим запросом: Мастер запросов периодически отправляет общие запросы (с фиксированным IP адресом назначения: 224.0.0.1) для уточнения, есть ли у многоадресной группы порты участники группы. При получении запроса, устройство, не являющееся мастером запросов, ретранслирует пакет на все свои порты.
- Сообщение с конкретным запросом: Если устройство хочет покинут многоадресную группу, оно отправляет пакет "IGMP leave". После получения такого пакета, мастер запросов отправляет пакет конкретного запроса (с IP адресом назначения, соответствующим IP адресу многоадресной группы) для подтверждения того, что у коммутатора остались какие-либо порты участники данной группы.
- Сообщение с отчетом участника группы: Если устройство хочет получать определенные данные многоадресной группы, оно отправляет пакет IGMP оповещения (с IP адресом назначения, соответствующим IP адресу многоадресной группы, к которой устройство планирует присоединиться) в ответ на IGMP запрос группы.
- Пакет "IGMP leave": Если устройство хочет покинут многоадресную группу, оно отправляет пакет "IGMP leave" (с фиксированным IP адресом назначения: 224.0.0.2).

13.3.4. Настройка через WEB-интерфейс

1. Включите протокол IGMP Snooping и включите режим автоматического запроса.

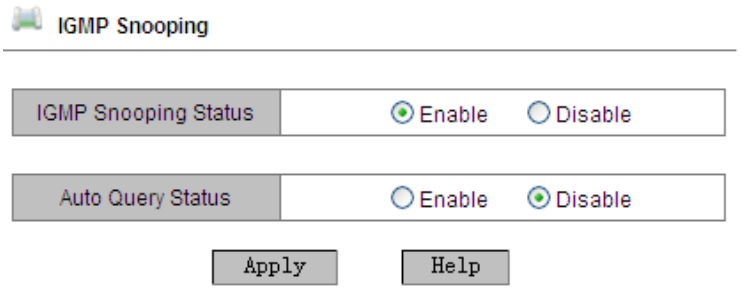


Рис. 81. Включение IMGP Snooping

Настройка IGMP Snooping (IGMP Snooping Status)
Настраиваемые опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Disable (Выключено)
Описание: Включение или выключение IGMP Snooping. IGMP Snooping и GMRP не могут быть включены одновременно.
Настройка автоматического запроса (Auto Query Status)
Настраиваемые опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Disable (Выключено)

Описание: Включение или выключение функции запросов. Если функция выключена, коммутатор не имеет возможности посылать автоматические запросы. Данную функцию можно включить только при включенном IGMP Snooping.

По крайней мере, хотя бы на одном коммутаторе должна быть включена функция автоматического запроса.

2. Отображение списка участников IGMP Snooping

IGMP Member List

MAC	VLAN ID	Member
01-00-5E-7F-FF-FE	1	6
01-00-5E-51-09-08	1	6
01-00-5E-00-01-01	1	6
01-00-5E-0A-18-03	1	6
01-00-5E-7F-FF-FA	1	4 6

Рис. 82. Отображение списка участников IGMP Snooping

Список участников IGMP (IGMP Member List)
Групповое отображение: {MAC, VLAN ID, Member} (MAC адрес, идентификатор VLAN, участник группы).
Описание: отображение таблицы адресов многоадресной рассылки FDB с включенной функцией IGMP Snooping. Идентификатор (ID) VLAN – это идентификатор участника группы.

13.3.5. Пример типовой настройки

Как показано на рисунке 83, функция IGMP Snooping включена на коммутаторах 1, 2, 3. На коммутаторах 2 и3 включена функция автоматического запроса. IP адрес коммутатора 2: 192.168.1.2; IP адрес коммутатора 3: 192.168.0.2, соответственно коммутатор 3 выбран в качестве генератора запросов.

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

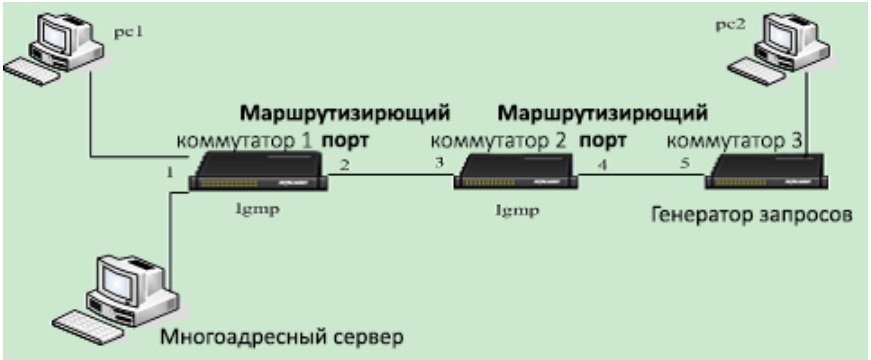


Рис. 83. Пример типовой настройки IGMP Snooping

- Т.к. коммутатор 3 является генератором запросов, он будет периодически отправлять сообщение с общим запросом, а порт 4 коммутатора 2 будет принимать это сообщение, соответственно данный порт будет выбран как маршрутизирующий порт. Далее сообщение с запросом будет перенаправлено из порта 3 коммутатора 2 в порт 2 коммутатора 1, который получив это сообщение будет назначен маршрутизирующим портом.
- Когда PC 1 подключается к многоадресной группе 225.1.1.1, он должен будет отправить сообщение с отчетом участника многоадресной группы коммутатору 1, соответственно порт 1 и маршрутизирующий порт 2 коммутатора 1 будут подключены к многоадресной группе 225.1.1.1; затем сообщение с отчетом IMGP будет перенаправлено к коммутатору 2 через маршрутизирующий порт 2, соответственно порты 3 и 4 коммутатора 2 также будут подключены к многоадресной группе 225.1.1.1; далее сообщение с отчетом IMGP будет перенаправлено к коммутатору 3 через маршрутизирующий порт 4, соответственно порт 5 коммутатора 3 также будет включен в многоадресную группу 225.1.1.1.
- Как только данные от многоадресного сервера достигнут коммутатора 1, они будут перенаправлены к PC 1посредством порта 1; т.к. маршрутизирующий порт 2 также является участником многоадресной группы, данные многоадресной передачи им также будут перенаправлены. Таким образом, когда данные достигнут порта 5 коммутатора 3 , пересылка остановится, т.к. отсутствует принимающая сторона. Но, если PC 2 также является участником 225.1.1.1, к нему также будут перенаправлены данные многоадресной рассылки.

14. Диагностика

14.1. Зеркалирование портов (Port Mirroring)

14.1.1. Введение

Port Mirroring - Зеркалирование портов. Благодаря функции зеркалирования портов, порт копирует все переданные и принятые данные одного порта (порт источника) на другой (порт назначения). Порт назначения, на который передаются данные, как правило, подключается к устройству-анализатору или RMON-монитору, для управления, мониторинга и диагностики неисправностей.

14.1.2. Описание

Коммутатор поддерживает только один порт зеркалирования, на который отправляются данные (порт назначения), но при этом нет ограничений на количество портов источника. Порты, данные которых зеркалируются, могут быть в одном VLAN или в разных. При этом, порты источника и назначения зеркалирования также могут быть в одном или в разных VLAN.
Порты источника и назначения должны быть разными портами.

- Настройка порта в режиме зеркалирования и в режиме транковой группы – взаимоисключающие. Порт источника/назначения зеркалирования не может

быть добавлен в транковую группу, в то же время порты, входящие в транковую группу нельзя настроить в режиме портов источника/назначения зеркалирования.

- Настройка порта в режиме зеркалирования и в режиме кольцевого порта - взаимоисключающие. Порт источника/назначения зеркалирования не может быть назначен кольцевым портом и на нем нельзя включать кольцевые протоколы. В то же время порт с поддержкой кольцевого протокола не может быть настроен как порт зеркалирования.
- Одновременная настройка портов в режиме зеркалирования и в режиме доверенного (Trust) порта DHCP Snooping невозможна. Порт источника/назначения зеркалирования не может быть настроен как доверенный порт, в то же время доверенный порт не может быть настроен в режиме портов источника/назначения зеркалирования.

14.1.3. Настройка через WEB-интерфейс

1. Выбор порта источника в режиме зеркалирования.

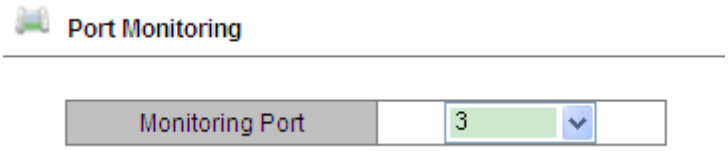


Рис. 84. Настройка порта назначения

Порт мониторинга (Port Monitoring)
Настраиваемые опции: NULL/One switch port (Нет/Один порт)
Значение по умолчанию: NULL (Нет)
Описание: Выбор порта назначения режима зеркалирования. Только один порт может быть настроен как порт назначения.

2. Выбор порта источника в режиме зеркалирования.

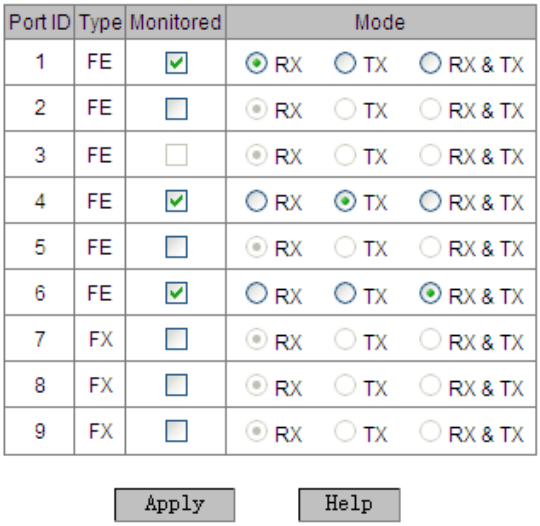


Рис. 85. Настройка порта источника

Режим (Mode)
Настраиваемые опции: RX/TX/RX&TX
Описание: Выбор данных для зеркалирования.
TX – зеркало передаваемых сообщений портом источником.
RX – зеркало принимаемых сообщений портом источником.
RX&TX – зеркало всех сообщений порта источника.

14.1.4. Пример типовой настройки

Как видно на рисунке 86, порт 2 это порт назначения режима зеркалирования, а порт 1 – порт источник. Все сообщения на порту 1 зеркалируются на порт 2.

Рис. 86. Настройка порта источника

Процесс настройки:
1. Настройте порт 2 в режим порта назначения, как показано на рис. 84.
2. Настройте порт 1 ка порт источник зеркалирования, режим порта зеркалирования установите как RX&TX, как показано на рис. 85.

14.2. Проверка связи (Link Check)

14.2.1. Введение

Проверка связи (Link Check) - это проверка того, насколько корректно порты с включенными протоколами кольцевого резервирования (STP/RSTP/Sy2-RP/Sy2-Ring) передают данные. Когда происходит аварийное переключение, режим проверки своевременно может обнаружить проблему и исправить ее.

14.2.2. Настройка через WEB-интерфейс

1. Настройка проверки связи

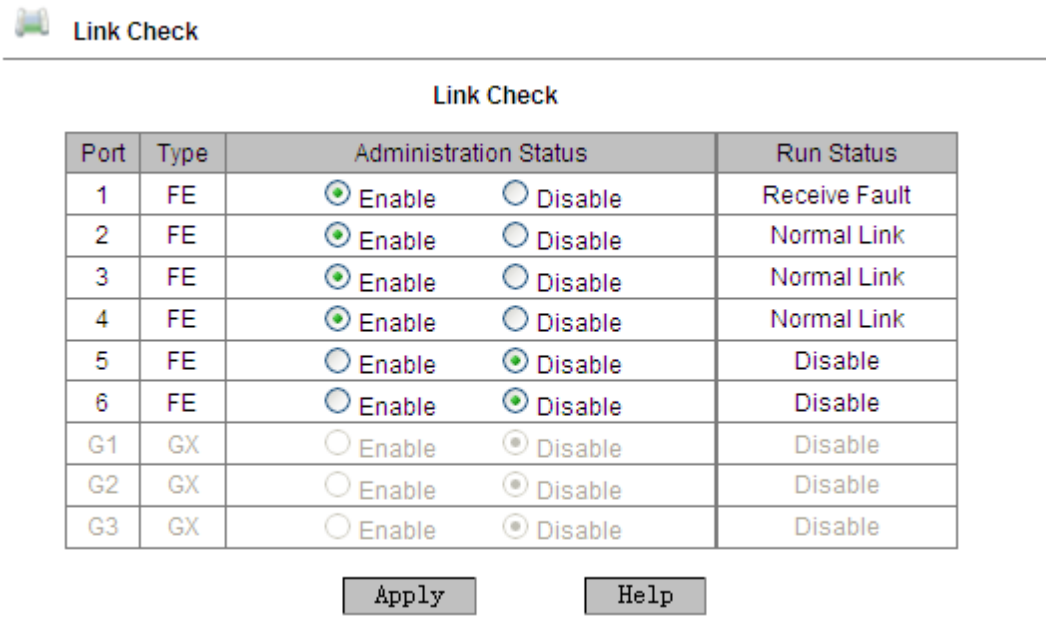


Рис. 87. Проверка связи

Режим администрирования (Administration Status)
Настраиваемые опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Enable (Включено)
Описание: Включение данной функции возможно только на портах с включенным режимом кольцевого резервирования.
Режим работы (Run Status)
Режим работы: Normal Link/Receive Fault/Disable (Нет ошибок/Прием ошибок/Выключено)
Описание: Если на кольцевом порту включена функция «Проверка связи», будет отображаться режим работы. Состояние «Normal» означает, что порт передает и принимает данные без сбоев и ошибок, в противном случае будет отображаться состояние «Receive Fault». Если на кольцевом порту не включена функция «Проверка связи», статус порта будет отображаться как «Disable».

14.3. Виртуальный тестер кабеля (Virtual Cable Tester, VCT)

14.3.1. Описание

Для определения состояния кабеля типа «витая пара» VCT использует такой метод исследования как рефлектометрия. Для обнаружения повреждения система передает в кабель импульсный сигнал и должна получить отражение этого импульсного сигнала. Когда передаваемый импульсный сигнал достигнет либо конца кабеля либо точки отказа, вся энергия импульсного или ее часть будут отражаться обратно на источник отправки сигнала, соответственно будет обнаружено повреждение кабеля. Технология VCT сначала измеряет время поступления сигнала к точке отказа, затем время возврата сигнала к исходному источнику, а потом затем вычисляет расстояние в соответствии с полученными временными результатами.

14.3.2. Реализация

Технология VCT обеспечивает проверку каналов, соединяющих медные порты Ethernet и выдает результаты тестирования линий связи. VCT может обнаруживать следующие типы повреждений кабеля:

- Short: это означает короткое замыкание, т.е. два или более проводов «закорочены» между собой.
- Open: это означает, что цепь разомкнута. Возможно в кабеле есть разорванные провода.
- Normal: это означает, что провода в кабеле исправны.
- Imped: это означает несоответствие импеданса. Поскольку импеданс кабеля Cat.5 составляет 100 Ом, чтобы избежать отражения волны и ошибки данных, импеданс терминаторов на обоих концах кабеля должен составлять 100 Ом.

14.3.3. Настройка через WEB-интерфейс

1. Проверка кабеля, длина которого известна.

Выберите кабель, длина которого известна (например, 4 м.); подсоедините один конец кабеля медному порту Ethernet 1, а другой конец кабеля не никуда подключайте; включите режим определения состояния кабеля на порту 1, как показано на рис. 88.

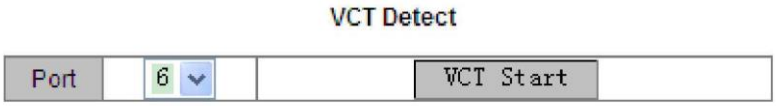


Рис. 88. Включение VCT

Порт (Port)
Настраиваемые опции: все медные порты коммутатора
Описание: Выбор порта, к которому подключен кабель и длина кабеля известна.
Метод: нажмите <VCT Start>, чтобы определить состояние кабеля, подключенного к обозначенному порту. Выполняйте проверку несколько раз, чтобы получить точный и стабильный результат теста.

2. Сравнение результатов теста с фактической ситуацией (см. рис.79).

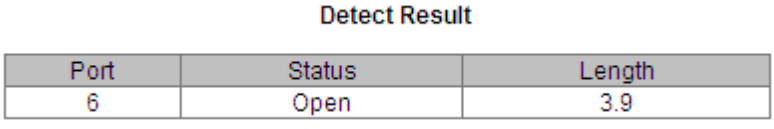


Рис. 89. Результаты теста VCT

Статус (Status)
Отображаемые опции: Open/Short/Normal/Imped

Описание: Отображение состояния кабеля, подключенного к обозначенному порту. Отображаемая информация показывает состояние кабеля: разомкнутая цепь, короткое замыкание, нормальное соединение, несоответствие импеданса.

Расстояние (Length)
Описание: Отображение расстояния от порта до точки отказа.

3. Настройка параметра «смещения» порта.

Detect Result

Port	Status	Length
6	Open	4.0(m)

Рис. 90. Настройка «смещения»

Примечание: порт во время тестирования будет в неактивном состоянии, результат «Normal» означает, что длину кабеля определить нельзя.

Смещение (Offset)
Настраиваемый диапазон (м): -10~+10
Значение по умолчанию: 0
Описание: Сравните длину кабеля с результатом теста и введите смещение. Как показано на рис. 89, длина после теста составляет 3,9 м, но фактическая длина кабеля составляет 4 м. Чтобы получить более точный результат теста, введите смещение 10 см, чтобы настроить результат теста на 4 м, как показано на рис. 91, минимизируя ошибку теста.

Detect Result

Port	Status	Length
6	Open	4.0(m)

Рис. 91. Результат теста после настройки «смещения»

Примечание: порт во время тестирования будет в неактивном состоянии, результат «Normal» означает, что длину кабеля определить нельзя.

15. SNTP

15.1. Введение

Протокол SNTP (Simple Network Time Protocol) обеспечивает синхронизацию времени между сервером и клиентом путём запросов и ответов. Если коммутатор выступает в качестве клиента, он синхронизирует своё время со временем сервера. Для одного коммутатора одновременно можно назначить до 4-х SNTP серверов, однако активным из них может быть только один.

Клиент SNTP последовательно отправляет запрос каждому серверу в виде одноадресной рассылки. Сервер, первым ответивший на запрос становится активным. Остальные серверы будут неактивны.

- Коммутатор не может служить сервером SNTP.
- Чтобы синхронизировать время по SNTP, должен быть активный SNTP-сервер.

15.2. Настройка через WEB-интерфейс

1. Включение протокола SNTP и настройка сервера SNTP.

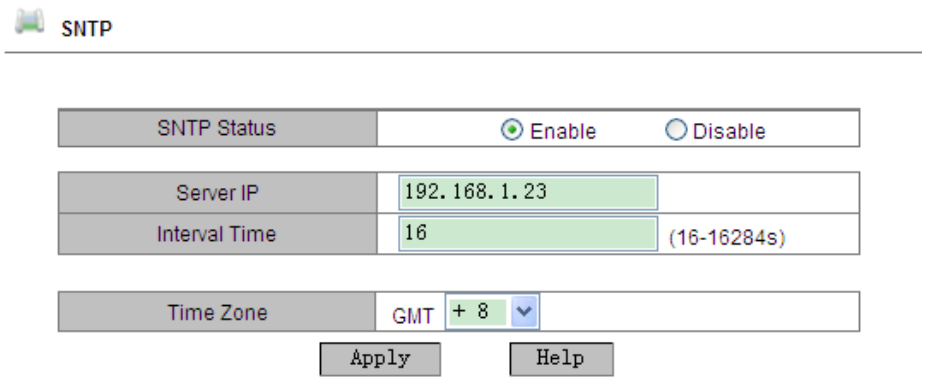


Рис. 92. Настройка SNTP

Статус SNTP (SNTP Status)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение или выключение SNTP.
Адрес сервера (Server IP)
Формат: A.B.C.D
Описание: Настройка IP адреса сервера SNTP. Клиенты будут синхронизировать своё время в соответствии с сообщениями этого сервера.
Интервал времени (Interval Time)
Настраиваемый диапазон (сек.): 16~16284
Описание: Настройка интервала для отправки запросов синхронизации на SNTP сервер.
Настройка часового пояса (Time Zone)
Варианты: 0, +1, +2, +3, +4, +5, +6, +7, +8, +9, +10, +11, +12, -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11
Значение по умолчанию: 0
Описание: Настройка часового пояса.

2. Выбор режима синхронизации времени клиент-сервер.

Last synchronization Time	2011.08.05 15:40:52
Device Time	2011.08.05 15:40:53
Update	Automatism Manual Apply

Рис. 93. Форма синхронизации

Последнее время синхронизации (**Last synchronization time)**
Отображаемый формат: yyyy.mm.dd hh.mm.ss (год.месяц.день часы.минуты.секунды)
Значение по умолчанию: 0000.00.00 00.00.00
Описание: Отображение времени полученного от сервера.
Время устройства (Device Time)
Отображаемый формат: yyyy.mm.dd hh.mm.ss (год.месяц.день часы.минуты.секунды)
Значение по умолчанию: 1
Описание: Отображение локального времени устройства.
Выбор режима синхронизации (Update)
Настраиваемые опции: Automatism/Manual (Автоматически/Вручную)
Значение по умолчанию: Automatism (Автоматически)
Описание: Выбор режима синхронизации времени клиент-сервер.

3. Отображение информации о настройках SNTP.

Number	Server IP	Server Status	Time Zone	Interval Time	Synchronization
1	192.168.1.23	active	+ 8	16	Synch
2	192.168.1.32	repose	+ 8	20	Synch

Delete

Рис. 94. Информация о настройках SNMP

Номер (Number)
Выбор номера для удаления соответствующей конфигурации сервера.По умолчанию: 1
Статус сервера (Server Status)
Отображаемые active/repose (активный/неактивный)
Сервер в активном состоянии выполняет синхронизацию времени для клиента. Существует один и только один сервер, который находится в активном состоянии, а все другие находятся в неактивном состоянии.
Синхронизация (Synchronization)
Описание: Нажмите кнопку <Synch>, если у вас установлен режим синхронизации «Manual».

16. Безопасность (Security)

16.1. SSH

16.1.1. Введение

SSH - это сетевой протокол для безопасного удаленного входа в систему. Он шифрует все передаваемые данные, чтобы предотвратить раскрытие информации. Когда данные шифруются с помощью SSH, пользователи могут использовать только режим командной строки для настройки коммутаторов.
Данная серия коммутаторов поддерживает функцию сервера SSH и дает возможность подключаться множеству клиентов SSH, которые могут авторизоваться в удаленном коммутаторе посредством протокола SSH.

16.1.2. Секретный ключ (Secret Key)

Незашифрованное сообщение называется открытым текстом, а зашифрованное сообщение называется шифрованным текстом. Шифрование или дешифрование находится под контролем секретного ключа. Секретный ключ - это специфический набор символов, который является основным параметром для контроля за преобразованием текста из открытого в шифрованный.
Для аутентификации на основе ключа используются секретные ключи. В конце каждого сообщения есть пара секретных ключей, персональный ключ и открытый ключ. Открытый ключ используется для шифрования данных, а законный владелец персонального ключа, чтобы гарантировать безопасность передаваемых данных может использовать его для их дешифрования.

16.1.3. Реализация

Чтобы осуществить безопасное SSH подключение, сервер и клиент должны пройти следующие пять этапов:

- Стадия согласования версий: в настоящее время SSH состоит из двух версий: SSH1 и SSH2. Обе стороны должны обсудить версию для использования;
- Стадия согласования ключей и алгоритмов: SSH поддерживает несколько типов алгоритмов шифрования. Обе стороны должны обсудить, какой алгоритм будет использоваться;
- Стадия аутентификации: клиент SSH отправляет на сервер запрос на аутентификацию, и сервер должен аутентифицировать клиента;
- Стадия запроса сеанса: клиент отправляет запрос на сеанс к серверу после прохождения аутентификации;
- Стадия сессии: клиент и сервер начинают связь после передачи запроса на сеанс.

16.1.4. Настройка через WEB-интерфейс

Шаги настройки сервера SSH:

1. Выключите статус SSH.
2. Нажмите <Destroy>, чтобы удалить старую пару ключей, как показано на рис. 95.

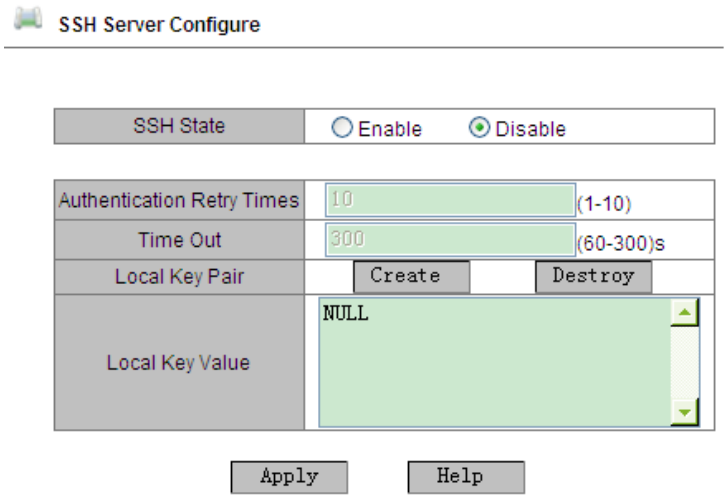


Рис. 95. Удаление старых ключей

3. Нажмите <Create>, чтобы создать новую пару ключей.

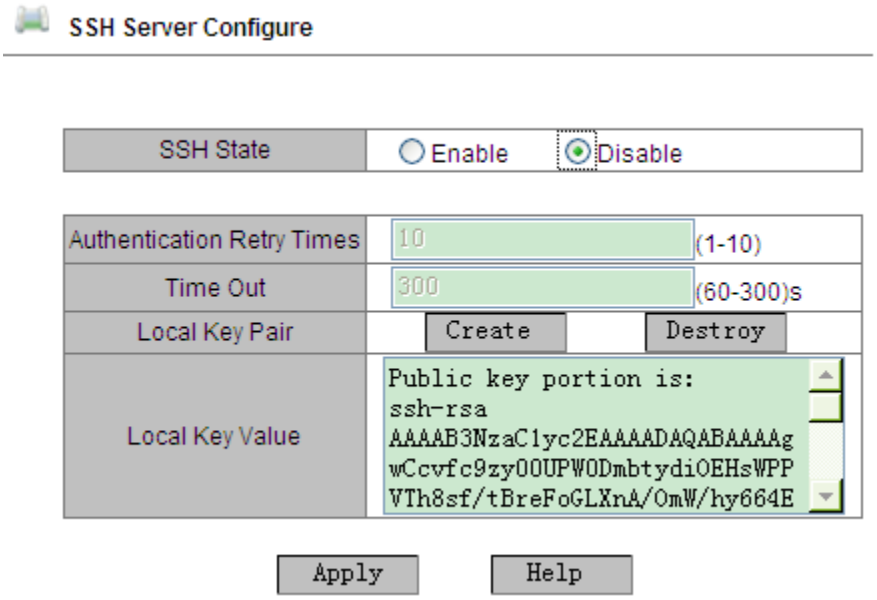


Рис. 96. Создание новой пары ключей

Режим SSH (SSH State)
Настраиваемые опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Disable (Выключено)
Описание: Включение/Выключение протокола SSH. Если протокол SSH включен, коммутатор работает как сервер SSH.
Время повторной проверки подлинности (Authentication Retry Times)
Настраиваемый диапазон: 1~10
Значение по умолчанию: 10
Описание: Настройка количества попыток авторизации в сервере SSH.

Настройка таймаута (Time Out)
Настраиваемый диапазон: 60~300
Значение по умолчанию: 300
Описание: Настройка времени, в течение которого длится клиентское соединение SSH в то время, когда нет передачи данных. После истечения данного времени соединение автоматически отключается.
Локальная пара ключей (Local Key Pair)
Настраиваемые опции: Create/Destroy (Создать/Удалить)
Описание: Создать или удалить пару локальных ключей сервера SSH. Перед включением сервера SSH необходимо создать пару локальных ключей. Необходимо удалить старую пару ключей перед созданием новой пары.
Значение локального ключа (Local Key Value)
Описание: Отображение значения локального ключа. Нажмите <Create>, чтобы автоматически сгенерировать значение ключа.

Шаги настройки сервера SSH:

1. Настройте ключ SSH, как показано на рис. 98.

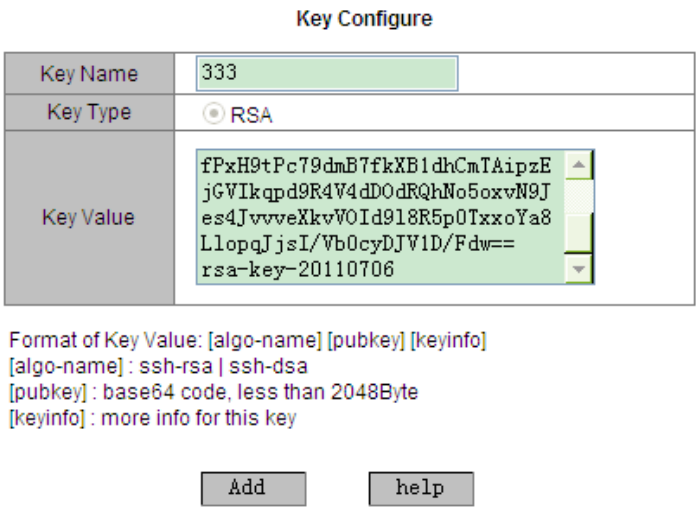


Рис. 98. Настройка ключа SSH

Имя ключа (Key Name)
Настраиваемый диапазон: 3~20 символов
Описание: Настройка имени ключа; обеспечивается поддержка максимум 3-х ключей.
Тип ключа (Key Type)
Обязательная настройка: RSA
Описание: В этой серии коммутаторов поддерживается только алгоритм RSA.
Значение ключа (Key Value)
Формат: {algorithm name, public key, key info} {имя алгоритма, открытый ключ, информация о ключе}
Название алгоритма: SSH-RSA | SSH-DSA
Открытый ключ: Основан на 64-значных кодах и его длина меньше 2048 байт.

Функции: Настройка открытого ключа соответствующего клиента. Как правило, открытый ключ генерируется программным обеспечением Puttygen и копируется вместо значения ключа сервера, персональный ключ хранится у клиента.

2. Отображение списка открытых ключей и удаление ключа.

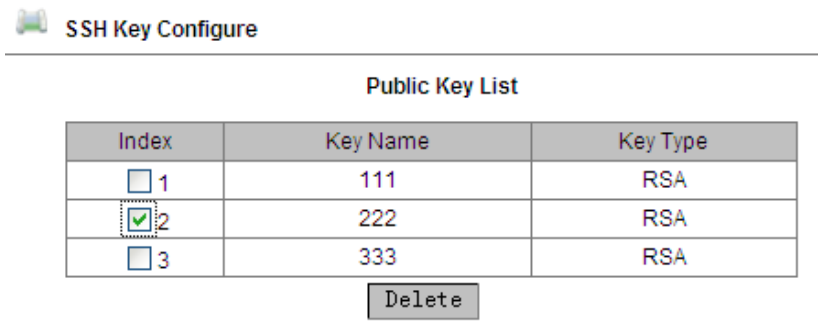


Рис. 99. Отображение списка ключей

Шаги настройки клиента SSH:

1. Настройте параметры клиента SSH, как показано на рис. 100.

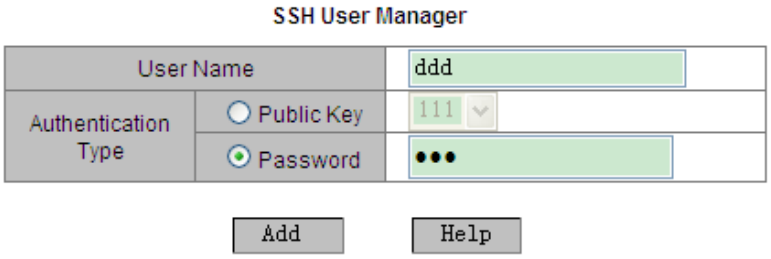


Рис. 100. Настройка клиента SSH

Имя клиента SSH (User Name)
Настраиваемый диапазон: 3~20 символов
Описание: Создание имени клиента; обеспечивается поддержка максимум 4-х клиентов.
Тип аутентификации (Authentication Type)
Настраиваемые опции: Public Key/Password (Публичный ключ/Пароль)
Значение по умолчанию: Public Key (Публичный ключ)
Описание: Настройка типа аутентификации клиента SSH. Если нужно выбрать «Public Key», выберите ключ из списка открытых ключей; если требуется выбрать «Password», необходимо ввести от 3 до 8 символов пароля для последующей авторизации.

2. Отображение списка клиентов SSH у удаление выбранных клиентов.

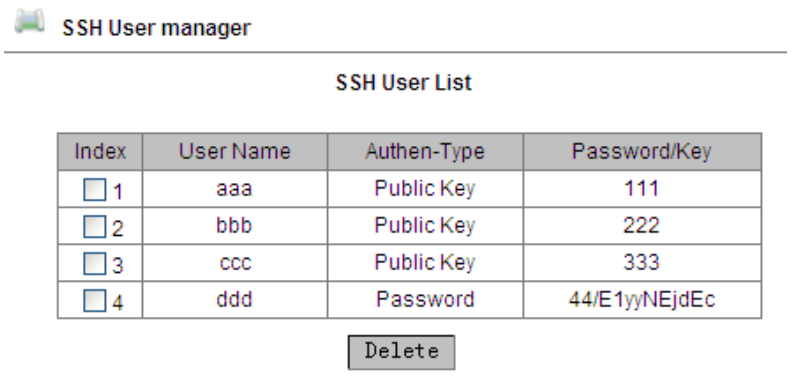


Рис. 101. Отображение списка клиентов SSH

16.1.5. Пример типовой настройки

Хост работает как клиент SSH для установления локального соединения с коммутатором, как показано на рисунке 102.

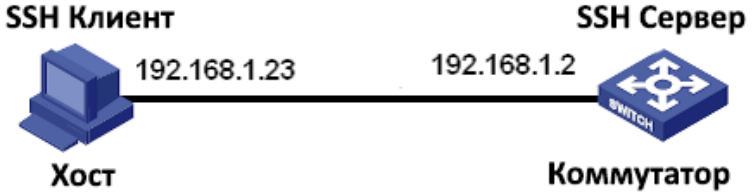


Рис. 102. Пример настройки SSH

Если клиент SSH выбирает тип аутентификации «Password», выпоните следующие действия:

1. Удалите старую пару ключей сервера, создайте новую пару ключей и запустите сервер SSH (рис. 95, 96, 97).
2. Задайте имя клиента SSH (в примере «ddd»); выберите тип аутентификации «Password», установите пароль (в примере используется пароль «444», см. рис. 100).
3. Установите соединение с сервером SSH. Сначала запустите программу PuTTY (рис. 103); введите IP-адрес сервера SSH «192. 168.1.2» в поле «Host Name».

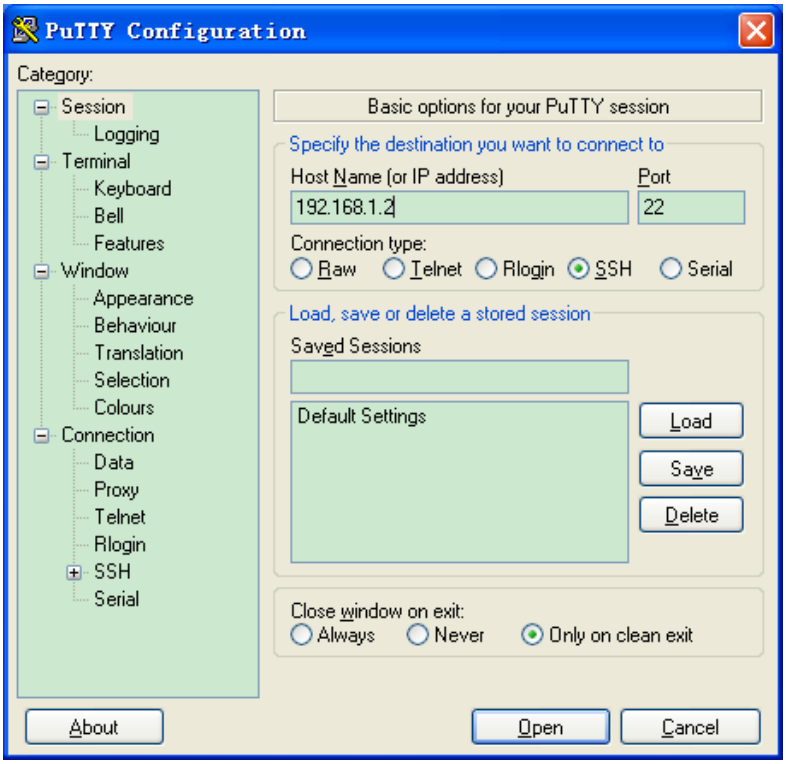


Рис. 104. Настройка клиента SSH

4. Нажмите кнопку <Open, после этого появится предупреждающее сообщение, показанное на рис. 104. Нажмите кнопку <Да>.

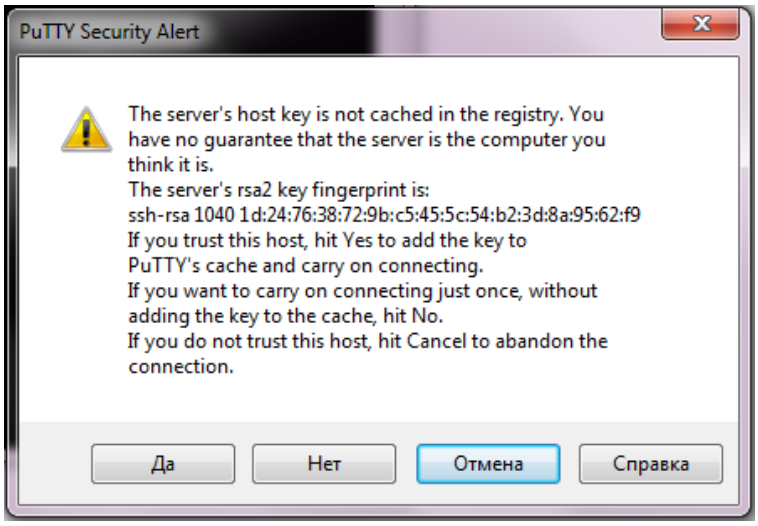


Рис. 104. Предупреждающее сообщение

5. Введите имя клиента «ddd» и пароль «444», для того чтобы войти в интерфейс настроек коммутатора (рис. 105).

Рис. 105. Экран авторизации с паролем SSH

Если клиент SSH выбирает тип аутентификации «Public Key», выпоните следующие действия:

1. Удалите старую пару ключей сервера, создайте новую пару ключей и запустите сервер SSH (рис. 95, 96, 97).
2. Выполните настройки клиента SSH (рис. 98); запустите у клиента программу PuTTYGen.exe, нажмите кнопку <Generate>, чтобы создать пару ключей клиента (рис. 106).

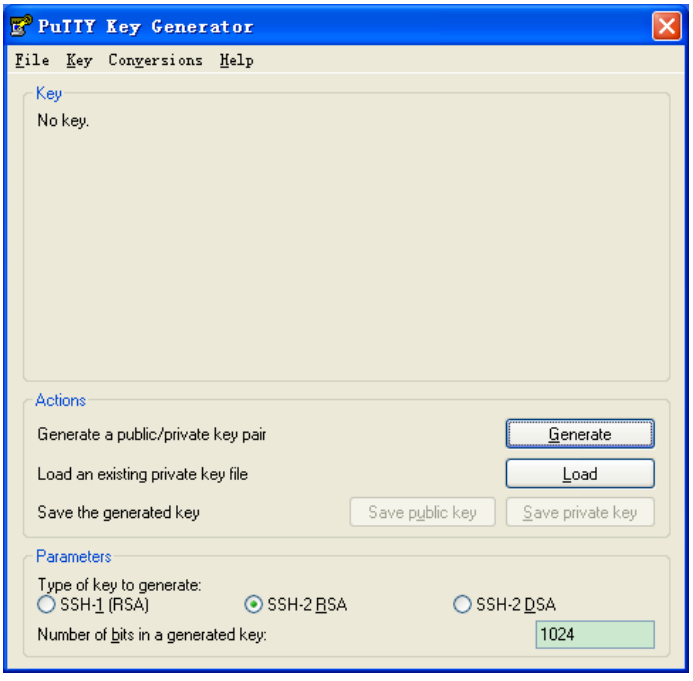


Рис. 106. Страница генерации ключа клиента

3. В процессе генерации ключа, пожалуйста, переместите указатель мыши на экран, в противном случае индикатор выполнения не покажет движения, и выполнение процесса генерации будет остановлено (рис. 107).

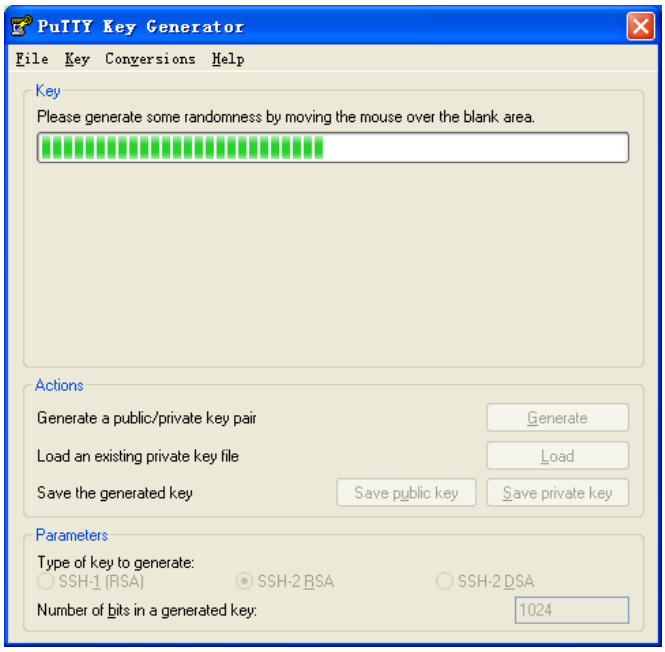


Рис. 107. Процесс генерации ключа клиента

4. Нажмите <Save private key> (рис.108), чтобы сохранить «персональный ключ» в текстовом файле, затем скопируйте «открытый ключ» в поле «Key Value» в интерфейсе настроек ключа SSH и введите имя ключа (рис. 98).

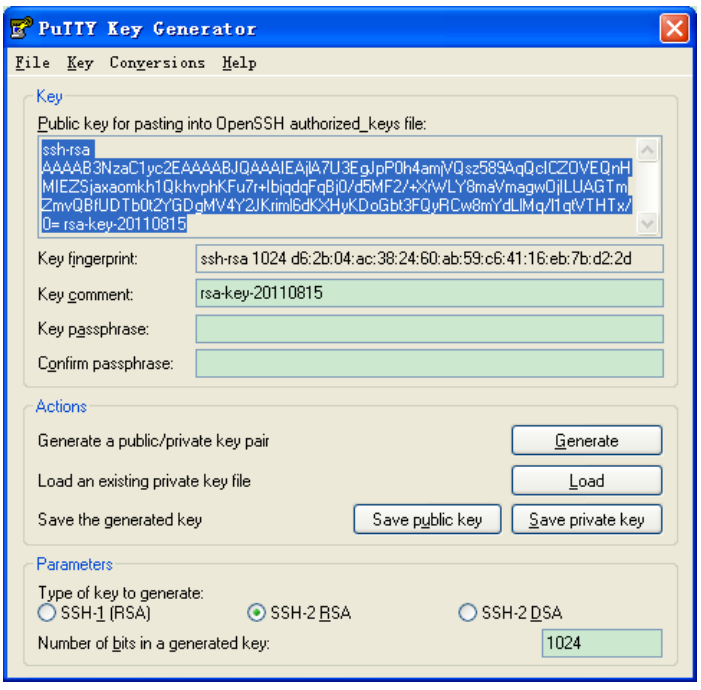


Рис. 108. Генерация значения ключа

5. Настройте имя клиента SSH (в примере используется имя «ddd») и выберите тип аутентификации «Public Key», а затем выберите соответствующее имя ключа (рис.100).
6. Установите соединение с сервером SSH. Сначала запустите программу PuTTY.exe (рис.109); введите IP-адрес сервера SSH «192.168.1.2» в поле «Host Name».

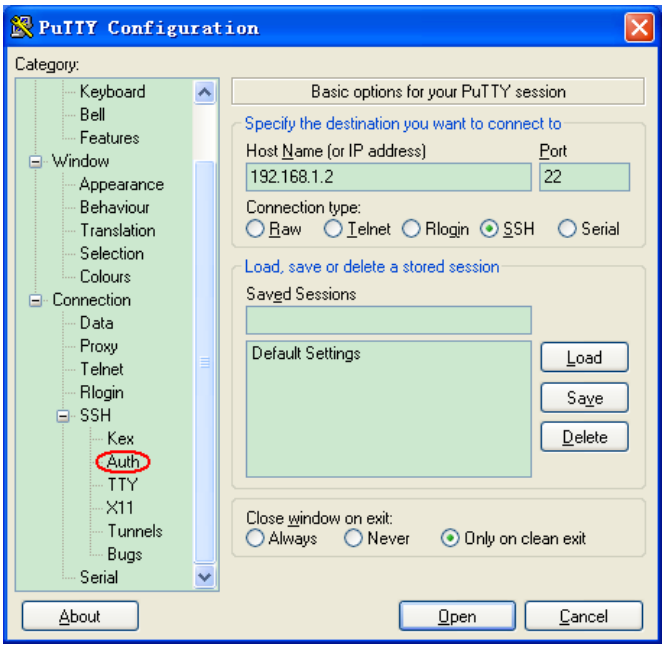


Рис. 109. Процесс генерации ключа клиента

7. Нажмите [SSH]->[Auth] (см. левую часть рис.109), соответственно на экране появится меню, отображенное на рис.110. Нажмите кнопку <Browse> и выберите файл с ключем, который был сформирован в п.4.

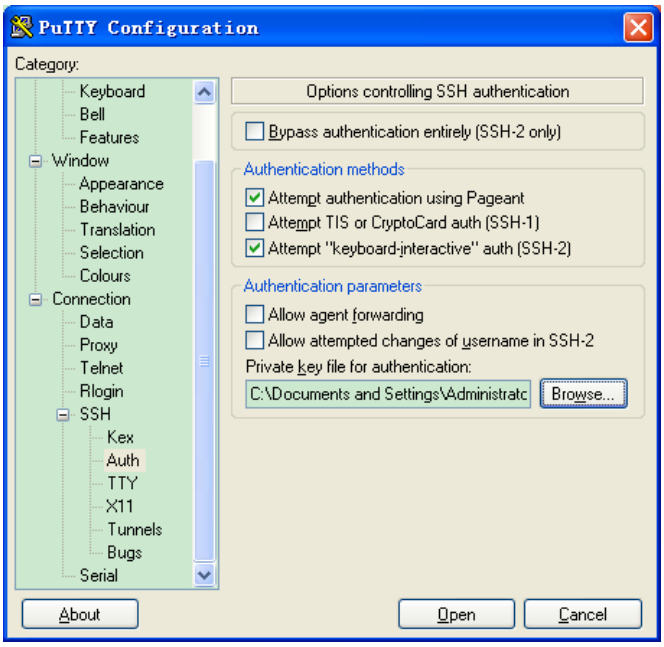


Рис. 110. Выбор файла с ключем

8. Нажмите кнопку «Open»; введите имя клиента для того чтобы войти в интерфейс настроек коммутатора (рис. 111).

Рис. 111. Экран авторизации с открытым ключем SSH

16.2. Dot1x

16.2.1. Введение

Чтобы решить проблему безопасности WLAN, комитет IEEE802LAN/WAN предложил использовать протокол 802.1X. Протокол IEEE802.1X используется в Ethernet как общий механизм контроля доступа, в основном решающий проблемы аутентификации и безопасности Ethernet. Протокол 802.1X - это своего рода протокол управления доступом к сети на основе доступа по портам. Управление доступом к сети по портам - это проверка подлинности и контроль доступа к устройствам подключенным к порту. Устройство с поддержкой 802.1X, подключенное к порту, может получить доступ к ресурсам в локальной сети только после прохождения аутентификации. Системы с поддержкой 802.1X являются типичной структурой Client/Server (Клиент/Сервер). Для работы приложений 802.1X необходимо наличие трех элементов:

Клиент: обычно это пользовательское терминальное устройство. Когда пользователи хотят подключиться к Интернету, им необходимо активировать программу клиента и ввести имя пользователя и пароль, а затем клиентская программа отправит запрос на соединение.

Аутентификатор: в Ethernet это означает коммутатор аутентификации, который в основном отвечает за передачу информации о аутентификации и результатов аутентификации, а также может включать или отключать порты в соответствии с результатами аутентификации.

Сервер аутентификации: он предоставляет услуги по аутентификации. Сервер проверяет идентификационные данные (имя пользователя и пароль), отправленные клиентом, чтобы определить, имеет ли пользователь право клиент использовать сетевые службы.

Сервер отправляет команды коммутатору «Enable/Disable» (Включить/Отключить) порт в соответствии с результатом аутентификации.

16.2.2. Настройки через WEB-интерфейс

1. Включение глобальной функции Dot1x.

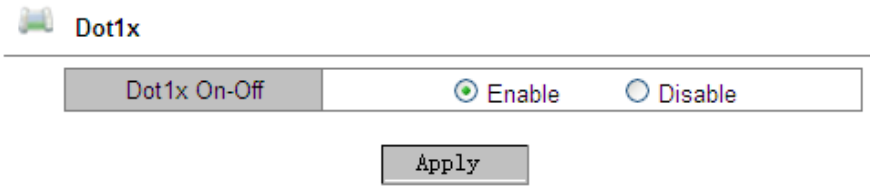


Рис. 112. Включение функции Dot1x

Включение/Выключение Dot1x (Dotlx On-Off)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение/Выключение функции безопасности Dot1x.

2. Информация о настройках Dot1x на порту.

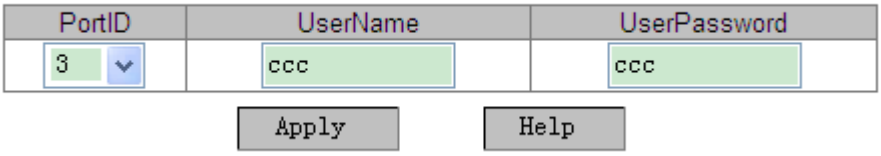


Рис. 113. Информация о Dot1x

Идентификатор порта (Port ID)
Настраиваемые опции: все порты коммутатора
Описание: Выбор порта для включения функции Dot1x.
Имя пользователя (User Name)
Настраиваемый диапазон: 1~16 символов
Описание: Настройка имени пользователя, которое будет привязано к порту.
Пароль пользователя (User Password)
Настраиваемый диапазон: 1~16 символов
Описание: Настройка пароля пользователя, который будет привязан к порту.

3. Настройка метода аутентификации и таймаута аутентификации

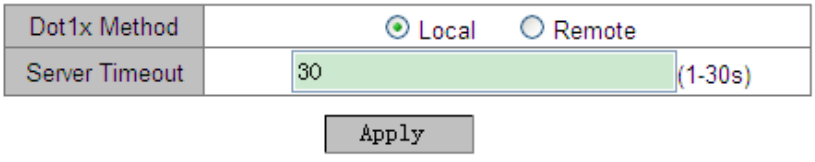


Рис. 114. Настройка метода и таймаута аутентификации

Метод Dot1x (Dotlx Method)

Настраиваемые опции: Local/Remote (Локально/Удаленно)

Значение по умолчанию: Local (Локально)

Описание: Выбор порта метода аутентификации Dot1x. Если выбрать вариант «Local», пользователю необходимо вручную добавить имя пользователя и пароль для проверки подлинности на коммутаторе. Если выбирается вариант «Remote», пользователю необходимо пройти аутентификацию сервера TACACS+ с именем пользователя и паролем, установленным на сервере TACACS+.

Настройка тайм-аута для сервера (Server Timeout)

Настраиваемый диапазон (сек.): 1~30

Значение по умолчанию: 30 сек.

Описание: Настройка тайм-аута проверки подлинности. Если пользователь не прошел аутентификацию в течение этого времени, предполагается, что аутентификация завершается с ошибкой.

4. Настройка портов с включенным режимом Dot1x.

PortID	Type	State		Mode			Reauthentication		ReauthenticationPeriod	QuietPeriod
1	FE	Enable	Disable	ForceUnauthorized	Auto	ForceAuthorized	Enable	Disable	3600	60
2	FE	Enable	Disable	ForceUnauthorized	Auto	ForceAuthorized	Enable	Disable	3600	60
3	FE	Enable	Disable	ForceUnauthorized	Auto	ForceAuthorized	Enable	Disable	3600	60
4	FE	Enable	Disable	ForceUnauthorized	Auto	ForceAuthorized	Enable	Disable	3600	60
5	FE	Enable	Disable	ForceUnauthorized	Auto	ForceAuthorized	Enable	Disable	3600	60
6	FE	Enable	Disable	ForceUnauthorized	Auto	ForceAuthorized	Enable	Disable	3600	60
7	FE	Enable	Disable	ForceUnauthorized	Auto	ForceAuthorized	Enable	Disable	3600	60
8	FE	Enable	Disable	ForceUnauthorized	Auto	ForceAuthorized	Enable	Disable	3600	60

Apply Help

Рис. 115. Настройка портов с включенным режимом Dot1x

Метод Dot1x (State)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Описание: Включение/Выключение протокола Dot1x на порту. Когда эта функция включена, пользователь может авторизоваться в системе коммутатора через этот порт только после прохождения аутентификации.

Режим (Mode)

Настраиваемые опции: ForceUnauthorized/Auto/ForceAuthorized

Значение по умолчанию: Local (Локально)

Описание: «ForceUnauthorized» означает, что порт всегда находится в состоянии отказа в несанкционированном доступе и не разрешает аутентификацию пользователя, а система аутентификации не предоставляет свою услугу пользователям, которые хотели бы получить доступ к сети через этот порт; «Auto» означает, что начальное состояние порта находится в состоянии отказа в несанкционированном доступе, а порт не позволяет пользователям получать доступ к сетевым ресурсам, но если пользователь проходит аутентификацию, порт переключается в состояние авторизации и дает возможность пользователю получить доступ к сетевым ресурсам. ForceAuthorized означает, что порт

всегда находится в состоянии авторизации и позволяет пользователю получать доступ к сетевым ресурсам без прохождения аутентификации.

Повторная аутентификация (Reauthentication)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Описание: Когда выполняется аутентификация, необходимо указать, требуется ли запрос повторной периодической аутентификации.

Период повторной аутентификации (Reauthentication Period)

Настраиваемый диапазон (сек.): 60~7200

Значение по умолчанию: 3600 сек.

Описание: Когда выполняется аутентификация, необходимо указать временной интервал, через который проходит запрос на повторную авторизацию.

Период молчания (Quiet Period)

Настраиваемый диапазон (сек.): 10~120

Значение по умолчанию: 60 сек.

Описание: когда пользователь терпит неудачу при аутентификации и переходит в режим ожидания, ему дается возможность снова отправить запрос аутентификации, когда закончится «Период молчания».

16.2.3. Пример типовой настройки

Как показано на рис. 116, клиент Dot1x подключается к порту 3 коммутатора; необходимо включить протокол Dot1x на порту 3 и выбрать режим автоматической аутентификации «Auto@; имя и пароль локального пользователя для аутентификации – «ccc», а имя и пароль для удаленной аутентификации – «ddd»; другие настройки используют значения по умолчанию.

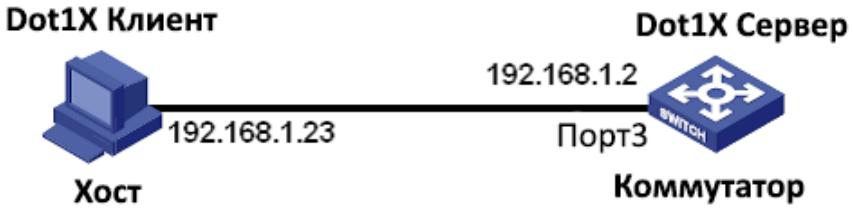


Рис. 116. Настройка портов с включенным режимом Dot1x

Настройка локальной аутентификации:

1. Включите протокол Dot1x, как показано на рис. 112.
2. Настройте имя пользователя и пароль порта как «ccc», как показано на рис. 113.
3. Выберите метод Dot1x «Local», как показано на рис. 114.
4. Включите протокол Dot1x на порту 3 и настройте режим аутентификации «Auto», как показано на рис. 115.
5. Установите клиентское программное обеспечение аутентификации 802.1X и запустите его, введите имя пользователя и пароль «ccc», чтобы выполнить аутентификацию.

Пользователь может получить доступ к коммутатору после прохождения аутентификации.

Настройка удаленной аутентификации:

1. Включите протокол Dot1x, как показано на рис. 112.
2. Настройте имя пользователя и пароль порта как «ccc», как показано на рис. 113.
3. Выберите метод Dot1x «Remote», как показано на рис. 114.
4. Включите протокол Dot1x на порту 3 и настройте режим аутентификации «Auto», как показано на рис. 115.
5. Установите клиентское программное обеспечение аутентификации 802.1X и запустите его, введите имя пользователя и пароль «ddd», чтобы выполнить аутентификацию. Пользователь может получить доступ к коммутатору после прохождения аутентификации.

16.3. Защита порта (Port Security)

16.3.1. Введение

Защита порта - это механизм безопасности на основе контроля MAC адресов для управления доступом к сети. Этот механизм обнаруживает MAC адреса источника принимаемых портом кадров для управления доступом к сети неавторизованных устройств. Основная задача функции «Безопасный порт» – дать возможность устройствам отследить разрешенные MAC адреса источников передачи определяя различные типы режима «Защита порта».

16.3.2. Настройка через WEB-интерфейс

1. Выбор порта для включения функции Port Security.

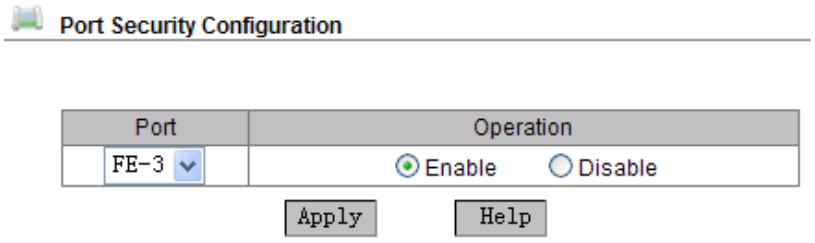


Рис. 117. Включение функции Port Security

Port (Порт)
Настраиваемые опции: все порты коммутатора
Operation (Режим работы)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Enable (Включено)
Описание: Включение/Выключение функции безопасности порта (Port Security).

2. Настройка адреса безопасного порта.

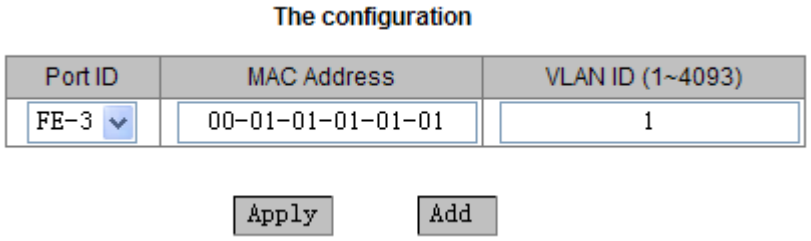


Рис. 118. Настройка адреса безопасного порта

Идентификатор порта (Port ID)
Настраиваемые опции: порты, которые поддерживают функцию Port Security.
Описание: Выбор порта для привязки к безопасному адресу.
MAC Address (MAC адрес)
Описание: Настройка MAC-адреса, который будет привязан к порту. Через данный порт могут передаваться только те сообщения, MAC адрес которых привязан к порту. Иначе сообщения будут удалены.
Идентификатор VLAN (VLAN ID)
Настраиваемые опции: Все существующие VLAN.
Описание: Настройка идентификатора VLAN для порта.

Для каждого порта данной серии коммутаторов можно настроить максимум 32 записи функции Port Security.

3. Отображение списка безопасных портов и удаление выбранных настроек безопасных портов.

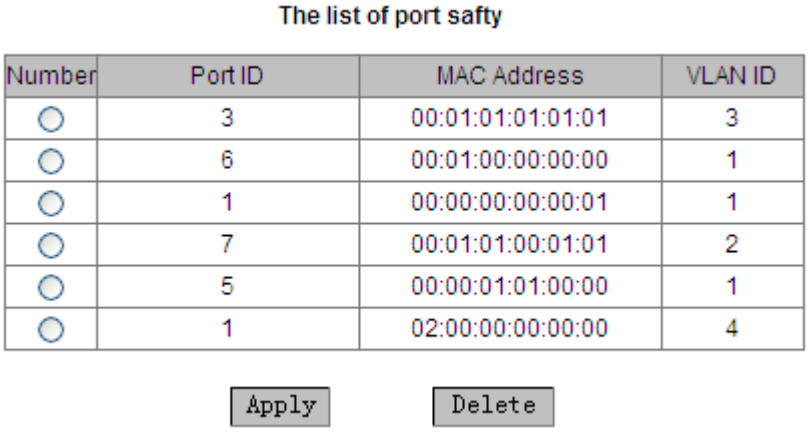


Рис. 119. Список безопасных портов

16.3.3. Пример типовой настройки

Привяжите MAC-адрес 0x000101010000 к порту 1 в VLAN 2, только тогда сообщение с MAC-адресом источника 0x000101010000 может проходить через порт 1 в VLAN 2.

Шаги настройки:

1. Включите функцию безопасного порта, как показано на рис. 117.
2. Установите для порта 1 значение MAC адреса 0x000101010000, а идентификатору VLAN присвойте значение 2, как показано на рис. 118.

16.4. Протокол AAA

16.4.1. Введение

Протокол AAA (Authentication, Authorization, Accounting / Аутентификация, Авторизация, Учет) - это механизм управления сетевой безопасностью, предоставляющий функции аутентификации, авторизации и управления учетными записями.
Аутентификация: подтверждение идентификационных данных удаленного пользователя и принятие решения о том, является ли он авторизованным пользователем.
Авторизация: предоставление разных прав различным пользователям и установка ограничений для сервисов, к которым пользователи могут получить доступ.
Управление учетной записью (Учет): запись всех действий, совершаемых пользователями при использовании сетевых ресурсов. Запись включает тип услуги, время начала услуги, информацию о потоке данных. Принято считать, что это не только метод учета, но и контроль сетевой безопасности.

16.4.2. Реализация

Во-первых, режим аутентификации обеспечивает аутентификацию пользователя. Обычно аутентификация использует имя пользователя и пароль для проверки прав доступа. Принцип аутентификации подразумевает, что каждый пользователь имеет уникальное право на получение доступа к сервисам сети. Сервер AAA последовательно сравнивает полученную информацию о правах пользователя с его записями в базе данных. Если есть соответствие, пользователь проходит аутентификацию; если нет, то сервер отправляет отказ на запрос сетевого подключения.
Затем пользователь получает права на выполнение соответствующих задач с помощью авторизации. Например, после входа в систему, пользователю необходимо ввести некоторые команды для работы с каким-то сервисом. Процесс авторизации системы определяет, имеет ли пользователь права на выполнение этих команд. Проще говоря, процесс авторизации включает в себя вид деятельности, ресурсы или услуги, доступные пользователю. Процесс авторизации происходит в процессе аутентификации. Как только пользователь пройдет аутентификацию, ему будут доступны соответствующие права доступа.
И последнее – «Учет». Данный механизм обеспечивает учет ресурсов, которые потребляются в процессе подключения пользователя. Информация включает в себя такие данные, как время соединения, переданный и принятый объем данных в процессе подключения пользователя и т.д. Процесс «Учет» выполняется на основе изучения журналов статистики и пользовательской информации, использовании ресурсов и планировании пропускной способности.

В настоящее время интерфейсом сервера сетевого подключения, координирующим работу с сервером AAA, является протокол TACACS+.

16.4.3. Настройка через WEB-интерфейс

1. Настройка порядка проверки подлинности.

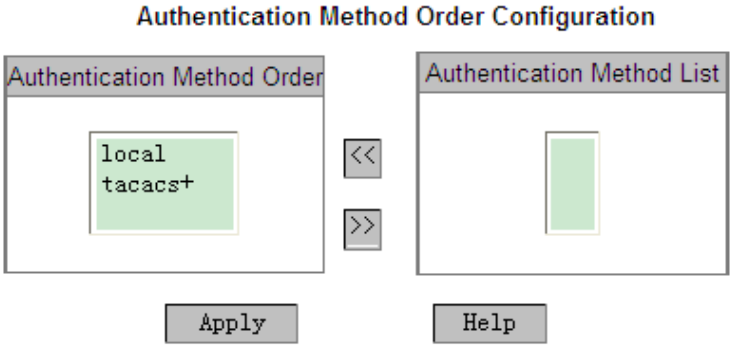


Рис. 120. Настройка метода аутентификации

Настройка порядка проверки подлинности (Authentication Method Order Configuration)
Настраиваемые опции: local/tacacs+/local, tacacs+/tacacs+, local
Значение по умолчанию: local
Описание: Выбор последовательности аутентификации.
local: выполняет локальную аутентификацию, которая использует имя пользователя и пароль, созданные на устройстве для входа в систему.
tacacs+: выполняет аутентификацию TACACS+, которая использует имя пользователя и пароль, записанные на сервере TACACS+.
local, Tacacs +: сначала выполняется локальная аутентификация, а если не удается ее пройти, выполняется аутентификация через TACACS+.
tacacs +, local: сначала выполняется аутентификация через TACACS+, а если не удается ее пройти, выполняется локальная аутентификация.

2. Настройка сервиса аутентификации TACACS+

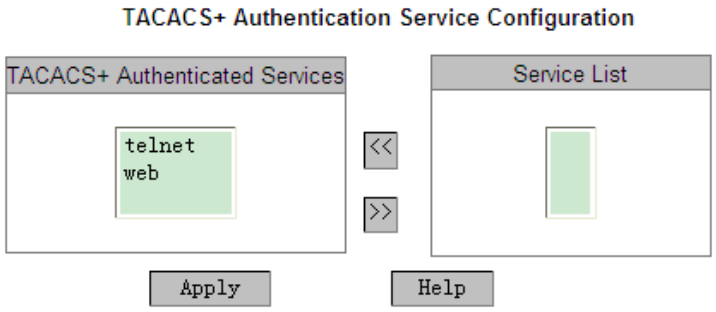


Рис. 121. Список безопасных портов

Настройка сервиса аутентификации TACACS+ (TACACS+ Authentication Service Configuration)
Настраиваемые опции: telnet/web
Описание: выбор метода аутентификации TACACS+.

16.5. Протокол TACACS+

16.5.1. Введение

TACACS+ (Terminal Access Controller Access Control System) - это своего рода приложение, основанное на протоколе TCP. Для передачи данных между NAS (Network Access Server) и сервером TACACS+ оно использует режим клиент-сервер. Клиент обслуживаются сервером NAS и он выполняет централизованное управление пользовательской информацией. Для пользователей NAS - это сервер, однако NAS для сервера TACACS+ является клиентом. Структура системы показана на рис. 122.

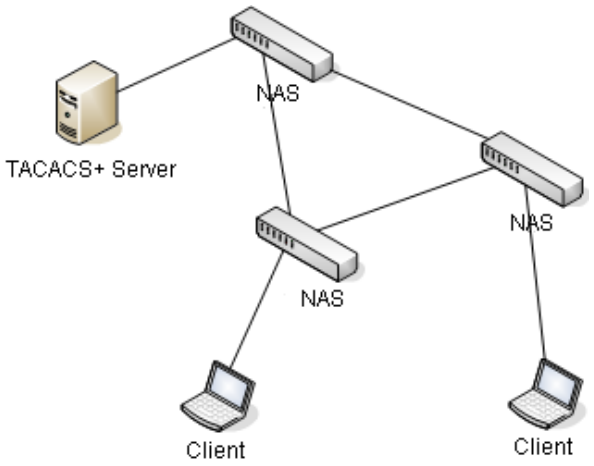


Рис. 122. Структура TACACS+

Этот протокол используется для аутентификации, авторизации и тарификации пользователя, который хотел бы получить доступ к устройству для совершения какой-либо операции. Устройство служит клиентом TACACS +, отправляя имя пользователя и пароль на сервер TACACS + для проверки. Сервер устанавливает TCP-соединение с клиентом, отвечает на запросы аутентификации и проверяет, является ли пользователь авторизованным пользователем. Пользователь сможет подключиться к устройству, чтобы выполнить операцию только после того, как он прошел проверку подлинности и был авторизован.

16.5.2. Настройка через WEB-интерфейс

1. Включение протокола TACACS+.

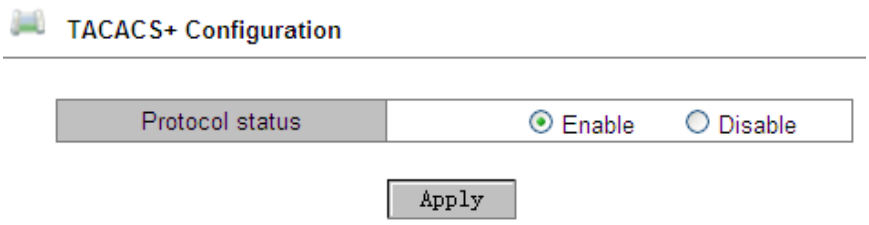


Рис. 123. Включение протокола TACACS+

Настройка протокола Tacacs+ (Protocol Status)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение/Выключение протокола TACACS+.

2. Настройка сервера TACACS+

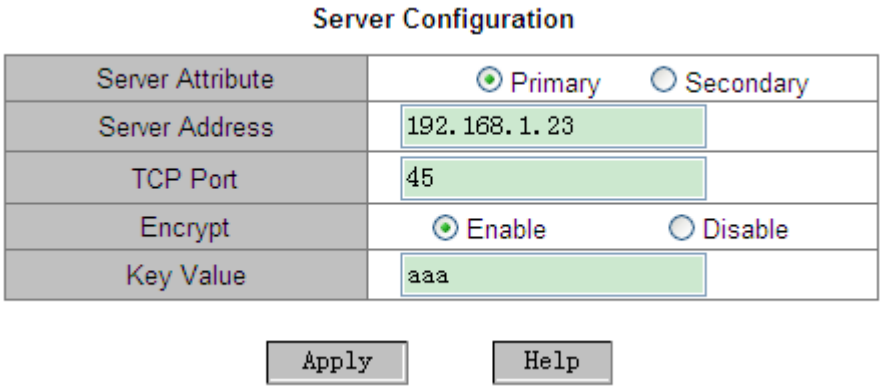


Рис. 124. Настройка сервера TACACS+

Типа сервера (Server Attribute)
Настраиваемые опции: Primary/Secondary (Первичный/Вторичный)
Значение по умолчанию: Primary (Первичный)
Описание: Выбор типа сервера.
Адрес сервера (Server Address)
Описание: Настройка IP адреса сервера.
Порт TCP (TCP Port)
Настраиваемый диапазон: 1~65535
Значение по умолчанию: 49
Описание: Настройка номера порта, который будет принимать запросы аутентификации от сервера NAS.
Шифрование (Encrypt)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение и выключение режима шифрования сообщений. Если оно включено, необходимо ввести его ключ.
Ключ шифрования (Key Value)
Настраиваемый диапазон: 1~32 символов
Описание: Настройка значения ключа шифрования. 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 клиента соответствует ключу, записанному на сервере TACACS+.

3. Отображение списка серверов.

Server List

Index	Attribute	Server Address	TCP Port	Encrypt
☐ 1	Primary	192.168.1.23	49	Enable
☐ 2	Secondary	192.168.1.32	45	Disable

Delete Modify

Рис. 125. Настройка сервера TACACS+

Отображение списка серверов TACACS +. Выбранную конфигурацию сервера можно удалить или изменить.

16.5.3. Пример типовой настройки

Сервер TACACS+, используя коммутатор, имеет возможность выполнить аутентификацию и авторизацию (см. рис. 126). IP-адрес сервера - 192.168.1.23, общий ключ для обмена сообщениями между коммутатором и сервером – «aaa».

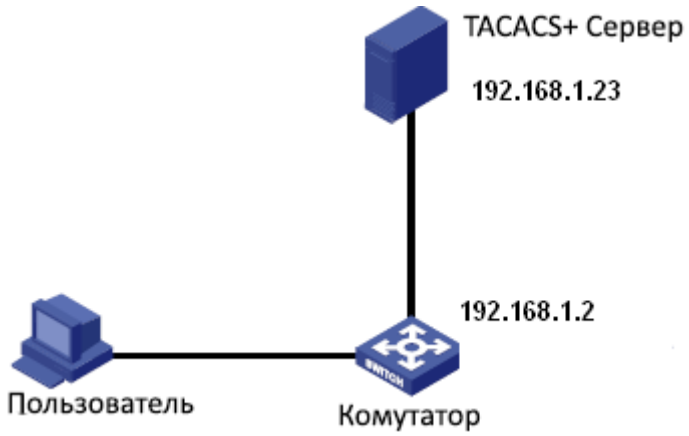


Рис. 126. Пример аутентификации TACACS+

1. Включите протокол TACACS+, как показано на рис. 123.
2. Присвойте серверу IP-адрес - 192.168.1.23, включите шифрование, установите значение ключа – «aaa», как показано на рис. 124. Для подключения к WEB-интерфейсу используется локальная аутентификация, а для входа в Telnet используется аутентификация TACACS+ (рис. 120, 121).
3. Настройте имя пользователя и пароль на сервере TACACS+ как «bbb».
4. Введите имя пользователя «admin» и пароль «123» и пройдите локальную аутентификацию для подключения к коммутатору по сети.
5. Введите имя пользователя и пароль «bbb» и пройдите аутентификацию TACACS+ для подключения к коммутатору через Telnet.

16.6. Протокол SSL

16.6.1. Введение

SSL (Secure Socket Layer) - это протокол безопасности, который обеспечивает безопасную связь на уровне протоколов приложения TCP, например, HTTPS. SSL шифрует сетевое соединение на транспортном уровне и использует симметричный алгоритм шифрования для обеспечения безопасности данных. Протокол SSL использует код аутентификации на базе секретного ключа для сохранения передаваемой и принимаемой информации. Этот протокол широко применяется в веб-браузерах, электронной почте, и т.д., используя протоколы шифрования для безопасной передачи информации по сети.
Для доступа к коммутатору с включенным протоколом SSL, пользователи должны использовать безопасное подключение с использованием https, например https://192.168.0.2.

При использовании протокола HTTPS для доступа к коммутатору убедитесь, что протокол SSL3.0 используется в настройках Интернета (откройте браузер, нажмите [Tool]->[Internet Option]->[Advanced]->[Security], отметьте «Use SSL3.0»).

16.6.2. Настройка через WEB-интерфейс

1. Включение HTTPS протокола.

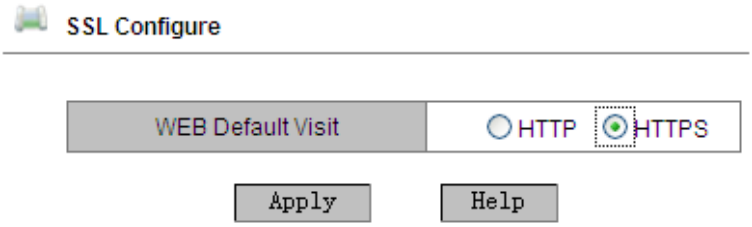


Рис. 127. Пример аутентификации TACACS+

Настройка через WEB по умолчанию (WEB Default Visit)
Настраиваемые опции: HTTP/HTTPS
Значение по умолчанию: HTTP
Описание: Выбор протокола для доступа через WEB-браузер. Если выбран протокол HTTPS, используйте https://*Ipaddress* для авторизации в WEB-интерфейсе коммутатора.

2. Авторизация в WEB-интерфейсе

Когда появится предупреждение об аутентификации, выберите «Continue browsing the website», как показано на рис. 128.

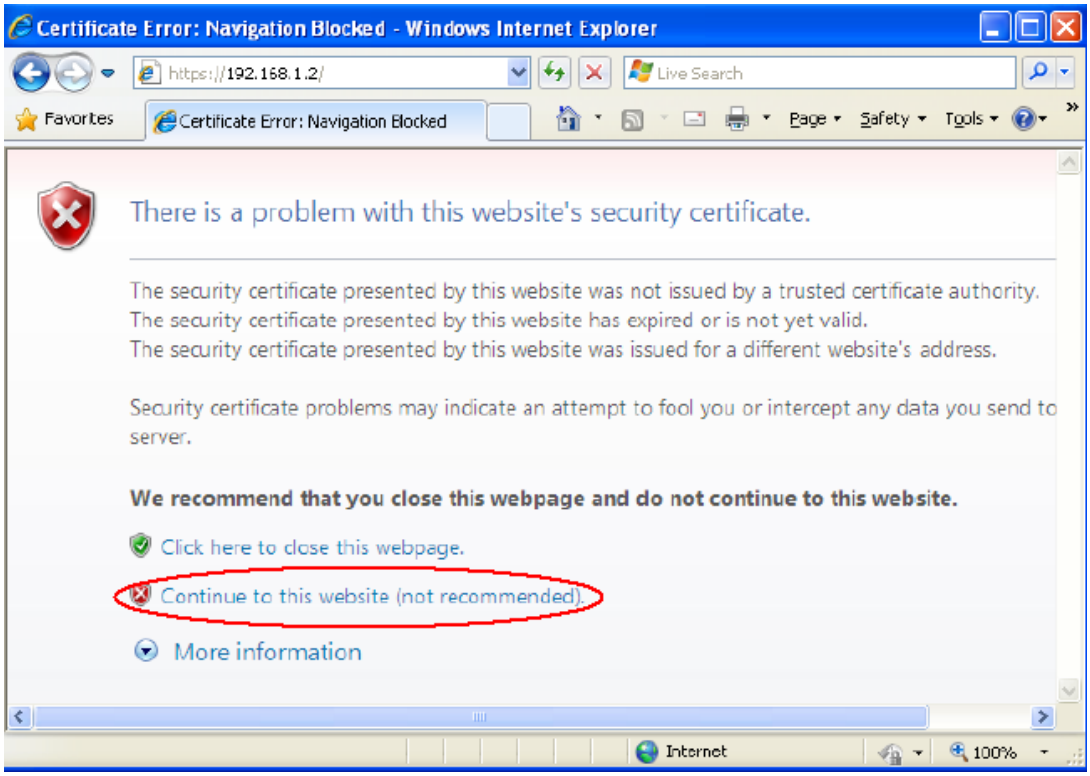


Рис. 128. Интерфейс авторизации HTTPS

Введите имя пользователя «admin» и пароль «123», чтобы успешно войти в систему через HTTPS.

17. Виртуальные локальные сети VLAN

17.1. Настройка VLAN

17.1.1. Введение

VLAN (Virtual Local Area Networks) делит LAN на несколько логических VLAN. Устройства в одной и той же VLAN могут взаимодействовать друг с другом, а устройства в разных VLAN – нет. Таким образом, широковещательные сообщения ограничены в VLAN, что повышает безопасность локальной сети.
Разделение сети на VLAN не ограничено физическим расположением устройств. Каждая VLAN рассматривается как отдельная логическая сеть. Для передачи данных между двумя разными VLAN необходим маршрутизатор, либо коммутатор 3-го уровня.

17.1.2. Принцип работы

Для того, чтобы сетевые устройства могли различать пакеты из разных VLAN, в кадры добавляются специальные идентификационные поля. На данный момент, самым распространённым протоколом для идентификации VLAN является IEEE802.1Q. Структура кадров 802.1Q показана в таблице:

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

В обычный Ethernet кадр добавляется 4-х байтный заголовок 802.1Q, который служит тегом VLAN.
Тип: 16 бит, используемые для идентификации того, что кадр содержит тег VLAN, а значение: 0x8100.
PRI: три бита, показывающие приоритет кадра 802.1p.
CFI: один бит. 0 обозначает Ethernet, а 1 - Token Ring.
VID: 12 бит, указывающие идентификатор VLAN в диапазон значений: от 1 до 4093. При этом 0, 4094 и 4095 - зарезервированные значения.

- VLAN 1 - это VLAN по умолчанию, Пользователь не может его создать или удалить вручную.
- Зарезервированные номера VLAN нужны для реализации специальных системных функций и также не могут быть созданы или удалены вручную.

Сообщение, содержащее заголовок 802.1Q, представляет собой тегированное сообщение (Tag message); если заголовка нет, то это сообщение нетегированное (Untag). Все сообщения в коммутаторе имеют тег 802.1Q.

17.1.3. VLAN на основе портов (Port-based VLAN)

Разделение на VLAN может быть либо по портам, либо по MAC адресам. Данная серия коммутаторов поддерживает разделение VLAN на основе портов. Данная функция определяет членов VLAN на основе портов коммутатора. Она добавляет порты в назначенные VLAN, а затем порты могут пересылать назначенные сообщения VLAN.
1. Тип порта
В соответствии с методами обработки тегов VLAN при передаче сообщений, порт можно разделить на два типа:

- Untag port (нетегированный порт): сообщения, отправленные с этого типа порта, не имеют тега. Как правило, этот тип порта используется для подключения к терминальному оборудованию, которое не поддерживает протокол 802.1Q. По умолчанию все порты коммутатора являются портами Untag и относятся к VLAN1.
- Tag port: все сообщения, пересылаемые с этого типа порта, несут тег VLAN. Этот тип порта обычно используется для подключения сетевых передающих устройств.

2. Идентификатор порта с VLAN (Port VLAN Identifier, PVID)
Каждый порт имеет атрибут PVID. Когда порт получает сообщение нетегированное сообщение, он добавляет тег в сообщение в соответствии с PVID.
Порт PVID - это идентификатор VLAN для нетегированного порта. По умолчанию PVID всех портов является VLAN 1.
После установки типа порта и PVID существует несколько способов настроить обработку сообщений, получаемых и передаваемых через порт (см. таблицу):

Обработка полученных пакетов		Обработка пакетов для пересылки	
Нетегированные пакеты	Тегированные пакеты	Тип порта	Обработка пакетов
Добавить теги PVID в нетегированные пакеты.	• Если идентификатор (ID) VLAN в пакете находится в списке разрешенных VLAN, принять пакет. • Если идентификатор (ID) VLAN в пакете отсутствует в списке разрешенных VLAN, отбросить пакет.	Untag	Переслать пакет после удаления тега.
		Tag	• Если входной приоритет QoS установлен на порт или как 802.1p, сохранить тег и переместить пакет. • Если входной приоритет QoS установлен для DSCP, заменить исходный тег на комбинацию очереди, отображаемой приоритетом DSCP и младшим битом входного приоритета, потом переместить пакет с новым тегом.

17.1.4. Настройка через WEB-интерфейс

1. Создайте VLAN

Выберите порты для добавления в VLAN и выполните соответствующую настройку портов.

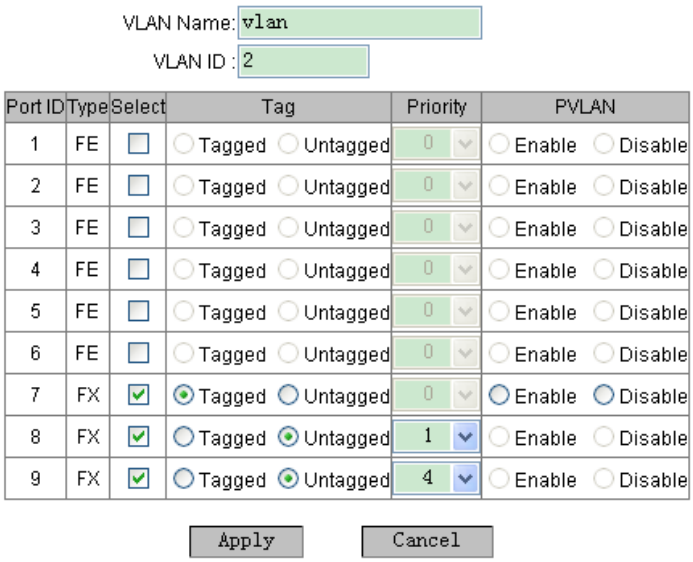


Рис. 129. Настройка VLAN

Имя VLAN (VLAN Name)

Настраиваемый диапазон: 1~31 символов.

Описание: Настройка имени VLAN.

Идентификатор VLAN (VLAN ID)

Настраиваемый диапазон: 2~4093.

Описание: Настройка идентификатора VLAN. ID VLAN используется для распознавания соответствующего VLAN. Данная серия коммутаторов поддерживает до 256 VLAN.

Настройка Тега (Tag)

Настраиваемые опции: Тегированный/Нетегированный (Tagged/Untagged).

Описание: Выбор типа порта в VLAN.

Приоритет (Priority)

Настраиваемый диапазон: 0~7.

Значение по умолчанию: 0

Описание: Настройка приоритета порта по умолчанию. При добавлении тега 802.1Q в нетегированное сообщение поле PRI является этим значением приоритета.

Настройка PVLAN (PVLAN)

Настраиваемые опции Enable/Disable (Включить/Выключить).

Значение по умолчанию: Disable (Выключено).

Описание: Включение PVLAN для тегированного порта. Более подробная информация содержится в разделе «PVLAN».

Нетегированный порт может присоединяться только к одной VLAN, а его идентификатор - это порт PVID. По умолчанию это VLAN 1, но тегированный порт может подключаться к нескольким VLAN.

2. Отображение списка VLAN

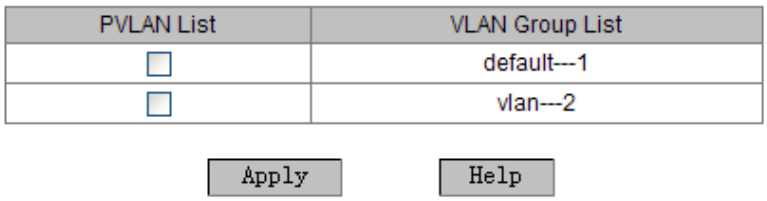


Рис. 130. Настройка VLAN

Список PVLAN (PVLAN List)

Описание: Если поставить галочку в соответствующем поле, функция PVLAN будет включена. Дополнительная информация будет представлена в разделе «PVLAN».

3. Отображение списка VLAN нетегированных портов. Соответственно, это порты PVLAN.

Port Default VLAN ID

Port ID	VLAN ID
1	2
2	1
3	2
4	1
5	1
6	1
7	1
8	1
9	1

Рис. 131. Список портов PVID

Каждый порт должен иметь атрибут Untag (нетегированный). Если атрибут не установлен, нетегированный порт по умолчанию используется в VLAN 1.

4. Изменение/Удаление VLAN

Чтобы открыть соответствующий экран, на котором можно удалить или изменить VLAN, нажмите VLAN (см. рис. 130). Нажмите <Delete>, чтобы удалить выбранную VLAN (см. рис.132).

Edit VLAN Group

VLAN Name : vlan

VLAN ID : 2

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	☐	○ tagged ○ Untagged	0	○ Enable ◉ Disable
2	FE	☐	○ tagged ○ Untagged	0	○ Enable ◉ Disable
3	FE	☐	○ tagged ○ Untagged	0	○ Enable ◉ Disable
4	FE	☐	○ tagged ○ Untagged	0	○ Enable ◉ Disable
5	FE	☐	○ tagged ○ Untagged	0	○ Enable ◉ Disable
6	FE	☐	○ tagged ○ Untagged	0	○ Enable ◉ Disable
7	FX	☑	◉ tagged ○ Untagged	0	○ Enable ◉ Disable
8	FX	☑	○ tagged ◉ Untagged	1	○ Enable ◉ Disable
9	FX	☑	○ tagged ◉ Untagged	4	○ Enable ◉ Disable

Apply Delete Cancel

Рис. 132. Изменение/Удаление VLAN

17.1.5. Пример типовой настройки

Как показано на рис. 133, сеть разделена на 3 VLAN: VLAN 2, VLAN 100 и VLAN 200. Необходимо, чтобы устройства в одной VLAN могли взаимодействовать друг с другом, при

этом другие VLAN были изолированы. ПК не могут различать теги сообщений, поэтому порты коммутаторов A и B, подключенные к ПК, настроены как нетегированные (Untag). Сообщения VLAN 2, VLAN 100 и VLAN 200 должны передаваться между коммутатором A и коммутатором B, поэтому порты, соединяющие коммутаторы A и B, должны быть настроены как тегированные (Tag), что позволит транслировать сообщения VLAN 2, VLAN 100 и VLAN 200. В таблице показана конфигурация устройств:

VLAN	Настройка
VLAN2	Настройте порты 1 и 2 на коммутаторах A и B как нетегированные порты (Untag ports), а порт 7 как тегированный порт (Tag port)
VLAN100	Настройте порты 3 и 4 на коммутаторах A и B как нетегированные порты (Untag ports), а порт 7 как тегированный порт (Tag port)
VLAN200	Настройте порты 5 и 6 на коммутаторах A и B как нетегированные порты (Untag ports), а порт 7 как тегированный порт (Tag port)

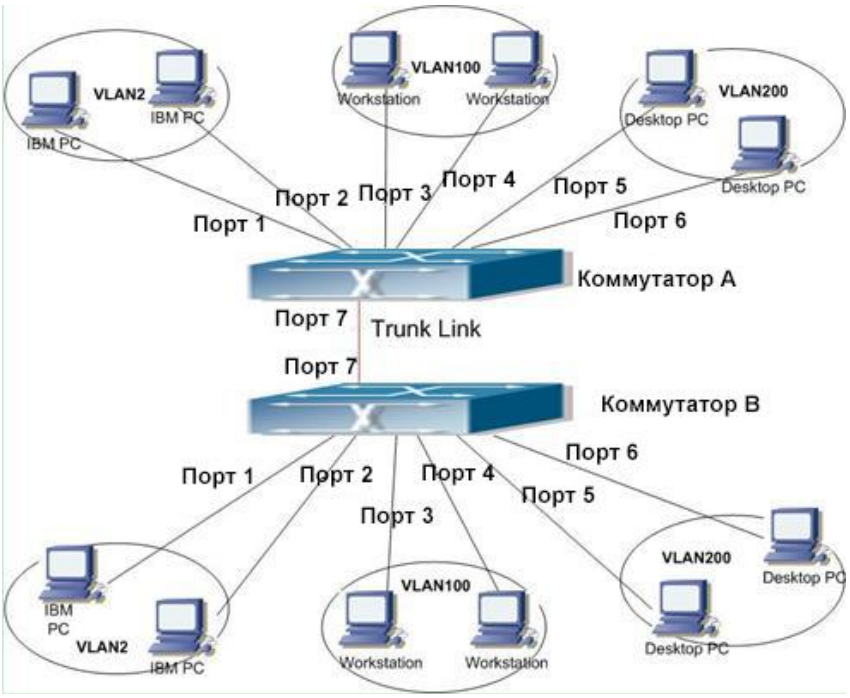


Рис. 133. Настройка VLAN

Настройте коммутаторы A и B, как показано ниже:

1. Создайте VLAN 2, добавьте в VLAN 2 порты 1 и 2 как нетегированные (Untag); добавьте порт 7 в VLAN 2 как тегированный (Tag) порт (см. рис. 129).
2. Создайте VLAN 100, добавьте в VLAN 100 порты 3 и 4 как нетегированные (Untag); добавьте порт 7 в VLAN 100 как тегированный (Tag) порт (см. рис. 129).

3. Создайте VLAN 200, добавьте в VLAN 200 порты 5 и 6 как нетегированные (Untag); добавьте порт 7 в VLAN 200 как тегированный (Tag) порт (см. рис. 129).

17.2. Изолированная VLAN (Private VLAN, PVLAN)

17.2.1. Введение

Для реализации комплексной функции изоляции трафика порта, обеспечения безопасности сети и изоляции широковещательного домена PVLAN 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.

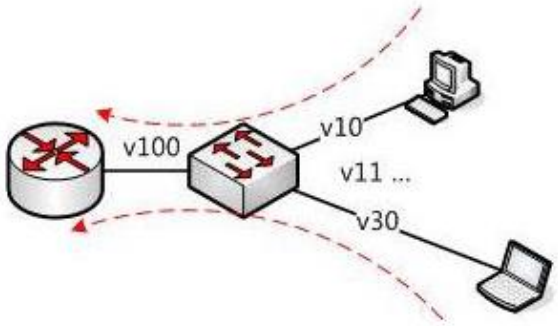


Рис. 134. Схема PVLAN

Как показано на рис. 134, 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.

Когда тегированный порт с включенной функцией PVLAN пересылает фрейм с тегом VLAN, тег VLAN будет удален.

17.2.2. Настройка через WEB- интерфейс

1. Включение на порту функции PVLAN.

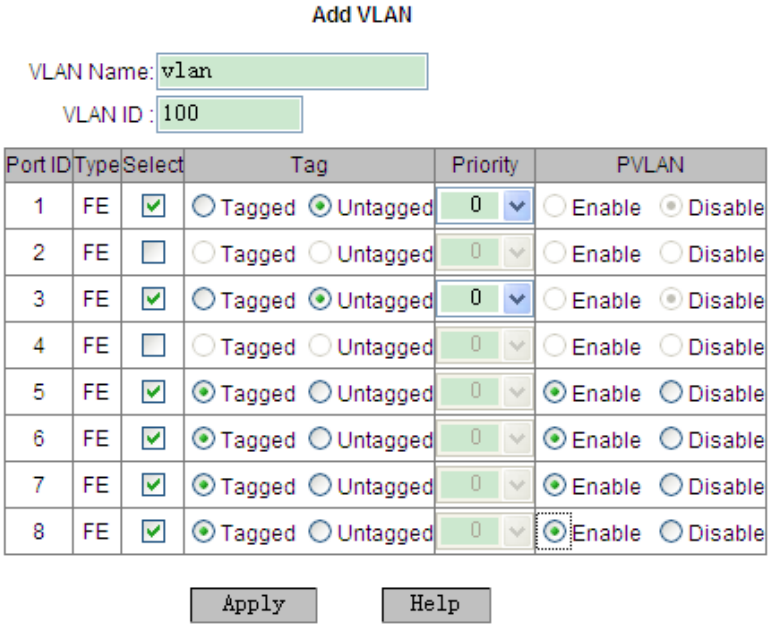


Рис. 135. Включение функции PVLAN

В интерфейсе настроек VLAN тегированные порты могут включать функцию PVLAN.
Если VLAN является общим доменом, магистральный порт должен быть настроен как нетегированный, а оконечный порт должен быть настроен как тегированный.
Если VLAN является изолированным доменом, оконечный порт должен быть настроен как нетегированный, а магистральный порт должен быть настроен как тегированный.

2. Выбор участников VLAN для включение в PVLAN.

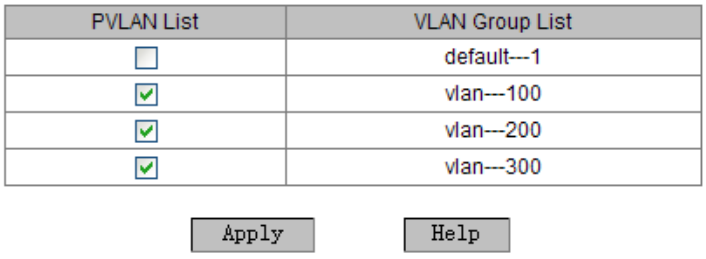


Рис. 136. Настройка участников PVLAN

Список PVLAN (PVLAN list)
Настраиваемые опции: Установить «флажок» или нет.
Значение по умолчанию: «Флажок» не установлен.
Описание: Выбор участников VLAN для PVLAN.

17.2.3. Пример типовой настройки

На рис. 137 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.

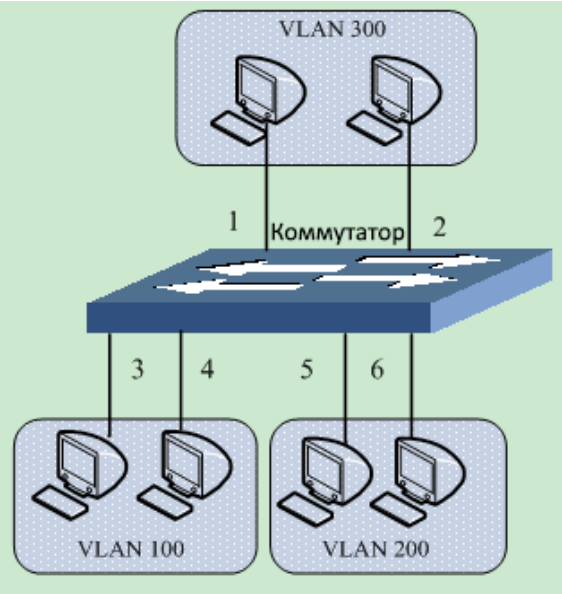


Рис. 137. Пример конфигурации PVLAN

Настройка коммутатора:

1. Настройте VLAN 300 как открытый домен (см. рис. 135).

Порты 1 и 2 должны быть настроены как нетегированные и назначены в открытый домен VLAN 300;

Порты 3 и 4 должны быть настроены как тегированные и назначены в открытый домен VLAN 300, функция PVLAN должна быть включена;

Порты 5 и 6 должны быть настроены как тегированные и назначены в открытый домен VLAN 300, функция PVLAN должна быть включена.

2. Настройте VLAN 100 как изолированный домен (см. рис. 135).

Порты 1 и 2 должны быть настроены как тегированные и назначены в изолированный домен VLAN 100, функция PVLAN должна быть включена;

Порты 3 и 4 должны быть настроены как нетегированные и назначены в изолированный домен VLAN 100.

3. Настройте VLAN 200 как изолированный домен (см. рис. 135).

Порты 1 и 2 должны быть настроены как тегированные и назначены в изолированный домен VLAN 200, функция PVLAN должна быть включена;

Порты 5 и 6 должны быть настроены как нетегированные и назначены в изолированный домен VLAN 200.

4. Настройте VLAN 300, VLAN 100 и VLAN 200 как участников PVLAN (см. рис. 136).

17.3. Протокол GVRP

17.3.1. Введение

Протокол GVRP (GARP VLAN Registration Protocol) является приложением протокола GARP (Generic Attribute Registration Protocol). Он основан на рабочем механизме GARP и управляет динамической регистрацией VLAN на устройстве и обеспечивает распространение информации на другие устройства.

Устройство с включенным протоколом GVRP может получать информацию о регистрации VLAN от других устройств и динамически обновлять локальную информацию о регистрации VLAN, а устройство может распространять локальную информацию о регистрации VLAN к другим устройствам, обеспечивая согласованность информации о VLAN на всех устройствах в одной локальной сети. Информация о регистрации VLAN, распространяемая GVRP, содержит не только локальную статическую регистрационную информацию, заданную вручную, но и динамическую регистрационную информацию от других устройств.

17.3.2. Режимы порта

На порту есть три типа режима регистрации GVRP: Обычный (Normal), Фиксированный (Fixed) и Выключено (Disable).

- Обычный (Normal): данный режим разрешает порту динамическую регистрацию или отмену регистрации настроек VLAN и обеспечивает распространение динамической и статической информации о VLAN.
- Фиксированный (Fixed): данный режим запрещает порту динамическую регистрацию или отмену динамической регистрации настроек VLAN, но при этом разрешает порту статическую регистрацию или отмену статической регистрации информации о VLAN.
- Выключено (Disable): данный режим запрещает порту динамическую или статическую регистрацию или отмену статической или динамической регистрации настроек VLAN, при этом порт не может распространять информацию о VLAN.

Настройки порт в режиме GVRP и режиме транкового порта (Port Trunk) являются взаимоисключающими. Порт с поддержкой GVRP не может присоединиться к транковой группе, а на порту, соединяющем транковую группу, нельзя включить GVRP.

17.3.3. Настройка через WEB-интерфейс

1. Включите протокол GVRP и настройте соответствующие таймеры.

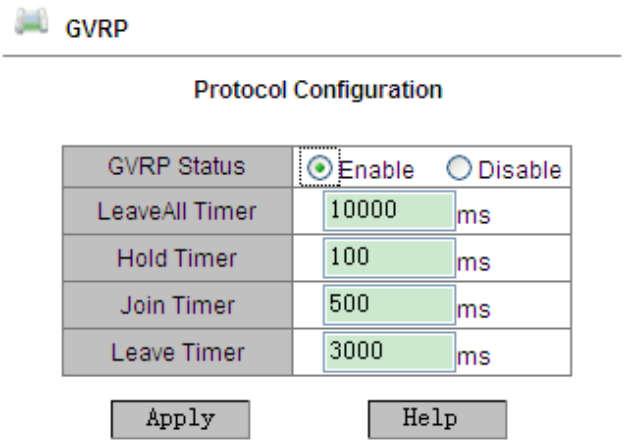


Рис. 138. Настройка протокола GVRP

Статус GVRP (GVRP Status)
Настраиваемые опции: Enable/Disable (Включено/Выключено)
Значение по умолчанию: Disable (Выключено)
Описание: Включение/Выключение протокола GVRP
Таймер LeaveAll (LeaveAll Timer)
Настраиваемый диапазон (мс): 100~327600
Значение по умолчанию: 10000 мс
Описание: Настройка интервала времени отправки всех исходящих сообщений. Значение должно быть кратно 100. Если установить тайм-аут таймера LeaveAll для разных устройств одинаковым, устройства будут отправлять сообщение LeaveAll одновременно, что увеличит количество сообщений. Чтобы этого избежать, фактическое время работы таймера LeaveAll должно быть случайным значением и должно быть длиннее времени одного таймера LeaveAll , но менее 1,5 таймера LeaveAll.
Таймер Hold (Hold Timer)
Настраиваемый диапазон (мс): 100~327600
Значение по умолчанию: 100 мс
Описание: Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение таймера для всех GVRP портов.
Таймер Join (Join Timer)
Настраиваемый диапазон (мс): 100~327600
Значение по умолчанию: 500 мс
Описание: Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение таймера для всех GVRP портов.
Таймер Leave (Leave Timer)
Настраиваемый диапазон (мс): 100~327600
Значение по умолчанию: 3000 мс
Описание: Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение таймера для всех GVRP портов.

2. Настройка порта.

Port Setting

Port	Type	GVRP Mode
1	FE	○ Disable ◉ Normal ○ Fixed
2	FE	○ Disable ◉ Normal ○ Fixed
3	FE	○ Disable ○ Normal ◉ Fixed
4	FE	○ Disable ○ Normal ◉ Fixed
5	FE	◉ Disable ○ Normal ○ Fixed
6	FE	◉ Disable ○ Normal ○ Fixed
7	FE	◉ Disable ○ Normal ○ Fixed
8	FE	◉ Disable ○ Normal ○ Fixed

Apply

Рис. 139. Настройка порта GVRP

Режим GVRP (GVRP Mode)
Настраиваемые опции: Disable/Normal/Fixed (Выключено/Обычный/Фиксированный)
Значение по умолчанию: Disable (Выключено)
Описание: Настройки режима GVRP на порту.

- Порт в режиме «Normal» может быть настроен только как нетегированный (Untagged) и существует в VLAN по умолчанию (VLAN 1).
- Невозможно выполнить любую операцию VLAN на порту в режиме «Normal».

3. Отображение статических и динамических настроек зарегистрированных VLAN.

VLAN Summary

Index	VLAN ID	VLAN Name	Untag Port	Tag Port	GVRP Aware Port
1	1	default	1,2,3,4,5,6, 7,8		
2	2	vlan			3

Рис. 140. Информация о VLAN

17.3.4. Пример типовой настройки

Как показано на рис. 141, коммутаторы A и B подключены через порт 2. Порт 1 коммутатора A установлен в Фиксированный (Fixed) режим, чтобы получать информацию о статической регистра рации VLAN; порт 2 настроен в обычный (Normal) режим и распространяет информацию о VLAN порта 1. Порт 2 коммутатора B настроен в обычный (Normal) режим и регистрирует информацию о VLAN коммутатора A. Таким образом, порт 2 коммутатора B может регистрировать такую же информацию о VLAN как и порт 1 коммутатора A.

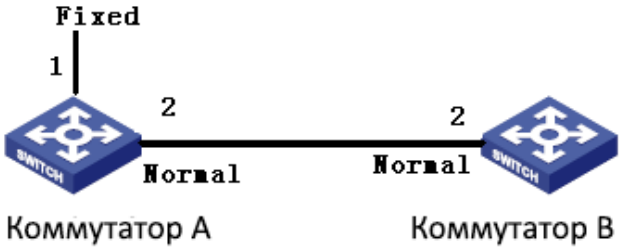


Рис. 141. Пример настройки GVRP

Настройте коммутатор следующим образом:
1. Включите протокол GVRP на коммутаторах A и B (см. рис. 138).
2. Настройте порт 1 коммутатора A в фиксированный (Fixed) режим, а порт 2 в Обычный (Normal) режим; настройте порт 2 коммутатора B в Обычный (Normal) режим (см. рис. 139).
3. Порт 2 коммутатора B может регистрировать такую же информацию о VLAN, как и порт 1 коммутатора A.

18. Протокол RMON (Remote Network Monitoring)

18.1. Введение

Протокол RMON (Remote Network Monitoring) основан на архитектуре SNMP и позволяет сетевым устройствам управления более интенсивно контролировать устройства. реализация протокола RMON основана на модели клиент/сервер и включает NMS (Network Management Station, Станция управления сетью), по сути являющейся сервером и специального Агента (Agent), который является клиентом. NMS управляет Агентом, который выполняет сбор статистики всех видов информации о трафике на порту.

Основные функции RMON – сбор статистики и сигнализация о тревогах. Функция сбора статистики предполагает, что агент может периодически выполнять сбор статистики всех видов информации о трафике на порте, например, получение информации о количестве сообщений, полученных в конкретном сегменте сети в течение конкретного периода времени. Функция сигнализации о тревогах обеспечивает выполнение агентом функций контроля за значениями указанных переменных MIB (Management Information Base) файлов. Когда значение достигает определенного порога (например, количество сообщений превышает указанное значение), агент может автоматически записывать события тревоги в журнал RMON или отправлять специальные Trap-сообщение на устройство управления.

18.2. Группы RMON (RMON Group)

Протокол RMON (стандарт RFC2819) подразделяется на несколько групп, которые включают: группу статистики (Statistics Group), группу истории (History Group), группу событий (Event Group) и группу тревог (Alarm Group) открытых MIB. Каждая группа поддерживает максимум 32 записи.

- Группа статистики (Statistics Group)

Наличие данной группы подразумевает, что система может вести сбор статистики всех видов информации о трафике на порту. Статистическая информация содержит много разной информации: количество коллизий в сети, сообщения об ошибках CRC, информацию о сообщениях со слишком маленьким или слишком большим размерами данных, информацию о широковещательных и многоадресных сообщениях, количество полученных байт, количество принятых сообщений и т.д. После успешного создания записи статистики по указанному интерфейсу, данная группа подсчитывает количество сообщений на текущем интерфейсе, а результатом является непрерывное накопление значений статистики.

- Группа истории (History Group)

Система периодически просматривает выборку всех видов информации о трафике на порту и сохраняет значения выборки в таблице записей истории, следовательно устройство управления может просматривать эту информацию в любое время. Группа истории учитывает значения статистики всех видов данных в интервале выборки сообщений, полученных портом в каждом цикле приема/передачи информации, причем периодичность данных циклов можно настраивать.

- Группа событий (Event group)

Группа событий используется для определения индексов событий и методов обработки событий. События, обработанные в группе событий, используются в элементе конфигурации группы тревог. Действие события начинается, когда контролируемое устройство достигает состояния тревоги.

Существует несколько способов обработки событий:

Журнал (Log): ведение журнала события и связанной с ним информации;

Прерывание (Trap): отправка Trap-сообщения в NMS и дальнейшее информирование о событии;

Log-Trap: запись и отправка Trap-сообщения;

Нет (None): не выполнять никаких действий

- Группа тревожной сигнализации (Alarm Group)

Функция управления тревожной сигнализацией протокола RMON обеспечивает контроль за определенными тревогами. После того, как пользователь обнаружит записи тревоги, система будет получать значения контролируемых переменных сигнала тревоги за определенный период. Когда значение переменной сигнала тревоги больше или равно пороговому значению, пользователь будет информирован о важной тревоге. Когда значение переменной тревоги ниже порогового значения, пользователь будет информирован о второстепенной тревоге. Тревоги будут обрабатываться в соответствии с определением конкретного события.

Если выборочное значение переменной аварийного сигнала превышает пороговое значение несколько раз в одном и том же направлении, инициирование события о тревоге возможно только первый раз. Это означает, что увеличение количества тревог и уменьшение количества тревог чередуются.

18.3. Настройка через WEB-интерфейс

1. Настройка информации о статистике.

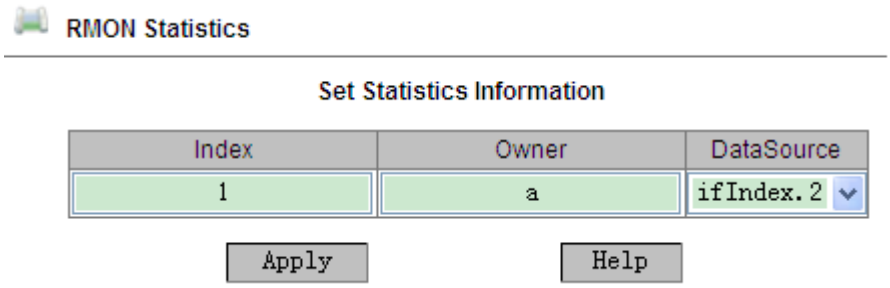


Рис. 142. Настройка статистики RMON

Индекс (Index)

Настраиваемый диапазон: 1~65535

Описание: Настройка индекса записи информации о статистике.

Владелец (Owner)

Настраиваемый диапазон: 1~32 символов

Описание: Настройка имени владельца записей информации о статистике.
Источник данных (Data Source)
Настраиваемые опции: ifIndex.portid
Описание: Выбор порта для сбора статистики.

2. Настройка таблицы истории.

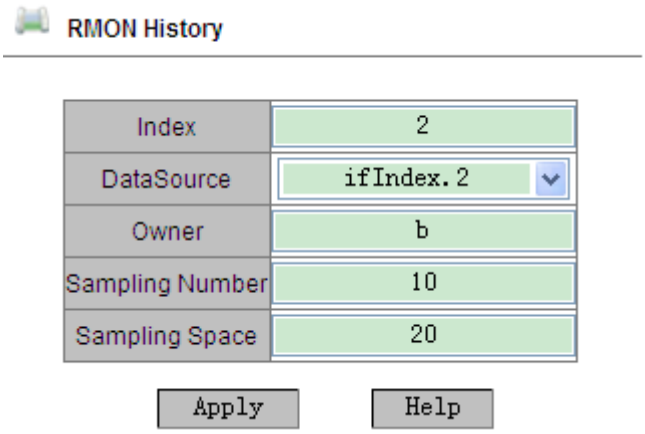


Рис. 143. Настройка истории RMON

Индекс (Index)
Настраиваемый диапазон: 1~65535
Описание: Настройка индекса записи управления историей.
Источник данных (Data Source)
Настраиваемые опции: ifIndex.portid
Описание: Выбор порта для отбора записей управления историей.
Владелец (Owner)
Настраиваемый диапазон: 1~32 символов
Описание: Настройка имени владельца записей управления историей.
Номер выборки (Sampling Number)
Настраиваемый диапазон: 1~65535
Описание: Настройка номера выборки записей управления историей.
Интервал выборки (Sampling Space)
Настраиваемый диапазон (сек.): 1~3600
Описание: Настройка интервала выборки записей управления историей.

3. Настройка контроля событий.

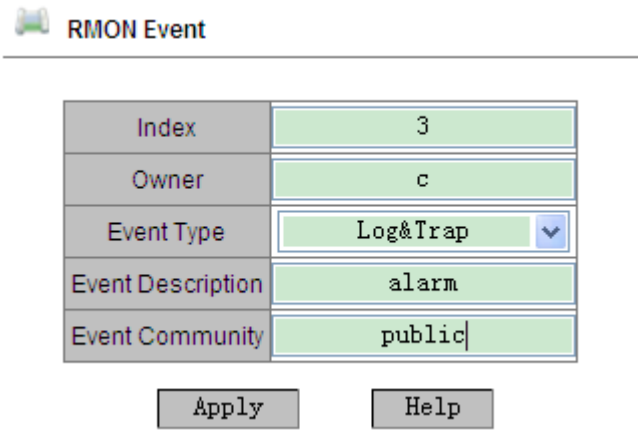


Рис. 144. Настройка контроля событий RMON

Индекс (Index)
Настраиваемый диапазон: 1~65535
Описание: Настройка индекса записи контроля событий.
Владелец (Owner)
Настраиваемый диапазон: 1~32 символов
Описание: Настройка имени владельца записей контроля событий.
Тип события (Event Type)
Настраиваемые опции: NONE/LOG/Snmp-trap/log&Trap
Значение по умолчанию: NONE
Описание: Настройка типа события при возникновении тревоги. Это метод обработки сигналов тревоги.
Значение события (Event Description)
Настраиваемый диапазон: 1~32 символов
Описание: Настройка значения события.
Имя группы событий (Event Community)
Настраиваемый диапазон: 1~32 символов
Описание: Настройка имени группы, отправляющего события Trap, которые должны соответствовать группе с наименованием SNMP.

4. Настройка контроля управления тревогами.

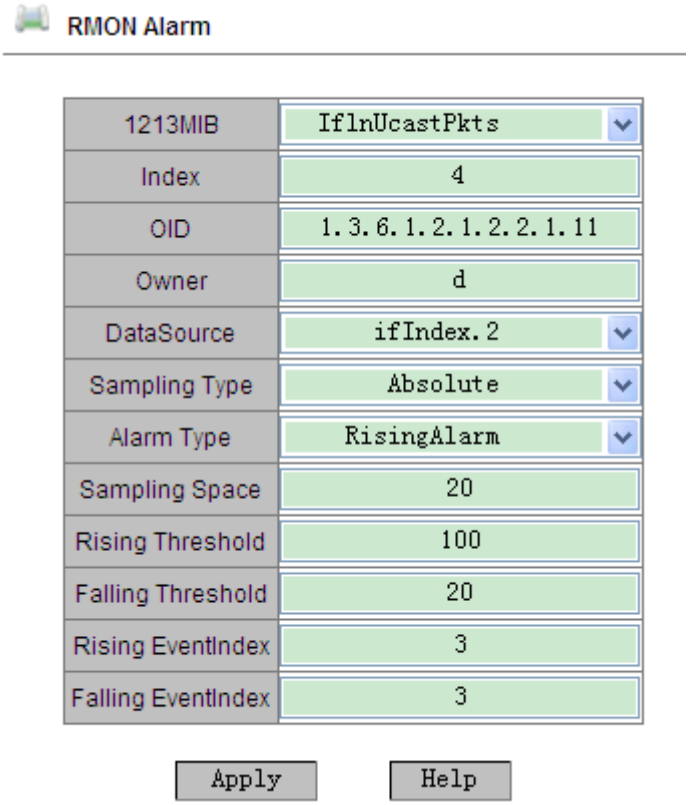


Рис. 145. Настройка контроля событий RMON

Информация MIB (MIB)
Описание: Выбор MIB информации для сбора статистики, например, количество одноадресных сообщений для входящего порта.
Индекс (Index)
Настраиваемый диапазон: 1~65535
Описание: Настройка индекса записи контроля тревог.
Идентификатор объектов (OID)
Описание: Настройка номера OID текущего узла MIB.
Владелец (Owner)
Настраиваемый диапазон: 1~32 символов
Описание: Настройка имени владельца записи контроля тревог.
Источник данных (Data Source)
Настраиваемые опции: ifIndex.portid
Описание: Выбор порта для контроля.
Тип выборки (Sampling Type)
Настраиваемые опции: Absolute/Delta
Значение по умолчанию: Absolute
Описание: Выбор метода сравнения значения выборки и порога. Absolute: прямое сравнение каждого значения выборки с порогом; Delta: текущее значение выборки минус предыдущее значение выборки, затем используется разница для сравнения с порогом.
Тип аварийной сигнализации (Alarm Type)
Настраиваемые опции: RisingAlarm/FallingAlarm/RisOrFallAlarm

Значение по умолчанию: RisingAlarm
Описание: Выбор типа тревоги.
Интервал выборки (Sampling Space)
Настраиваемый диапазон: 1~65535
Описание: Настройка периода выборки, оптимальное значение которого должно соответствовать значению интервала выборки записей управления историей.
Верхнее пороговое значение (Rising Threshold)
Настраиваемый диапазон: 1~65535
Описание: Настройка верхнего порогового значения. Когда значение выборки превышает пороговое значение, а тип сигнала тревоги установлен как RisingAlarm или RisOrFallAlarm, тревога будет активирована, кроме того активируется индекс события Rising.
Нижнее пороговое значение (Falling Threshold)
Настраиваемый диапазон: 1~65535
Описание: Настройка нижнего порогового значения. Когда значение выборки ниже порогового значения, а тип сигнала тревоги установлен как FallingAlarm или RisOrFallAlarm, тревога будет активирована, кроме того активируется индекс события Falling.
Индекс события Rising (Rising Event Index)
Настраиваемый диапазон: 0~65535
Описание: Настройка индекса события Rising. Это метод обработки возрастания тревог.
Нижнее пороговое значение (Falling Threshold)
Настраиваемый диапазон: 0~65535
Описание: Настройка индекса события Falling. Это метод обработки убывания тревог.

19. Настройка одноадресной рассылки (Unicast)

19.1. Введение

Когда коммутатор пересылает сообщение, он для подтверждения номера порта назначения ищет в таблице MAC адресов соответствующий MAC адрес, для которого предназначено данное сообщение.
MAC адреса могут быть статическими и динамическими.
Значение статического MAC адреса устанавливается пользователем, имеет наивысший приоритет (он не может быть заменен автоматически динамическим MAC адресом) и является постоянно действующими.
Динамические MAC-адреса появляются в таблице во время проверки передаваемых данных. Они считаются достоверными только в течение 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-адрес назначения, также содержащийся 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.
Данные серии коммутаторов поддерживают максимум 256 статических одноадрессных записей.

19.2. Настройка через WEB-интерфейс

1. Добавьте запись статического MAC адреса.

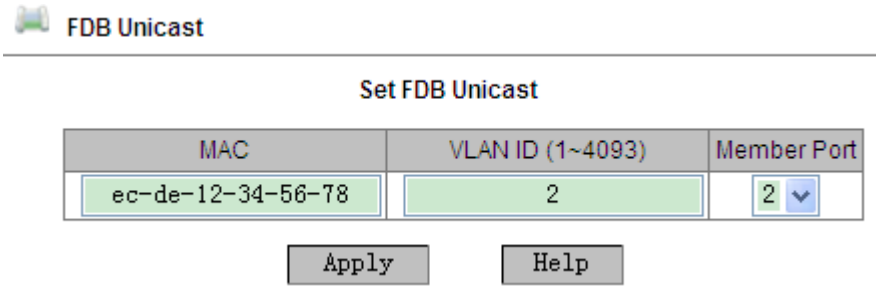


Рис. 146. Настройка статического одноадресного FDB

Настройка MAC адреса (MAC)
Настраиваемый формат: HH-HH-HH-HH-HH-HH (H - шестнадцатеричное число).
Описание: Настройка одноадресного (Unicast) MAC адреса; младший бит в старшем байте равен 0.
Настройка идентификатора VLAN (VLAN ID)
Описание: Настройка идентификатора VLAN для соответствующего порта.
Настройка порта участника (Member Port)
Настраиваемые опции: Все порты коммутатора
Описание: Выбор порта для пересылки сообщения с данным MAC адресом назначения, при этом выбранный порт должен быть участником указанной выше VLAN.

2. Отображение статических одноадресных (Unicast) MAC адресов

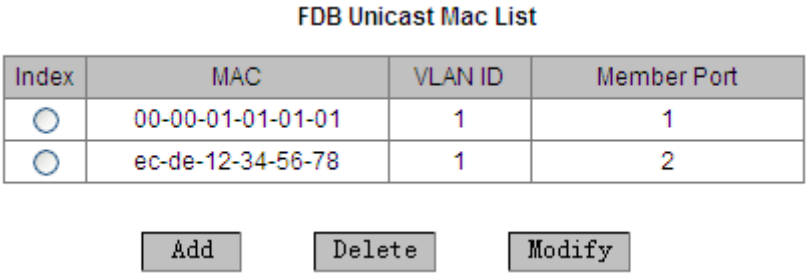
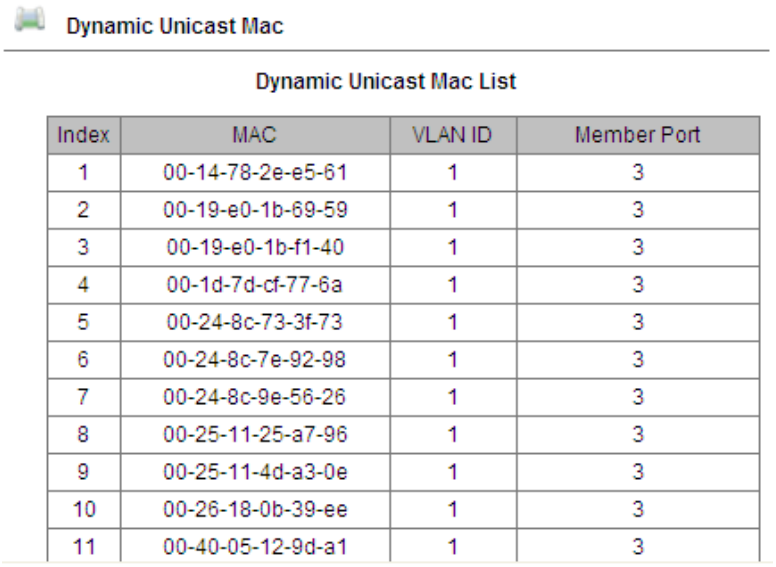


Рис. 147. Таблица статических FDB

Выберите в таблице запись для удаления или изменения параметров.

3. Отображение списка динамических одноадресных (Unicast) MAC адресов.


Dynamic Unicast Mac

Dynamic Unicast Mac List

Index	MAC	VLAN ID	Member Port
1	00-14-78-2e-e5-61	1	3
2	00-19-e0-1b-69-59	1	3
3	00-19-e0-1b-f1-40	1	3
4	00-1d-7d-cf-77-6a	1	3
5	00-24-8c-73-3f-73	1	3
6	00-24-8c-7e-92-98	1	3
7	00-24-8c-9e-56-26	1	3
8	00-25-11-25-a7-96	1	3
9	00-25-11-4d-a3-0e	1	3
10	00-26-18-0b-39-ee	1	3
11	00-40-05-12-9d-a1	1	3

Рис. 148. Таблица динамических одноадресных FDB

20. Системный журнал и аварийная сигнализация (Alarm and Syslog)

20.1. Аварийная сигнализация (Alarm)

20.1.1. Введение

Данная серия коммутаторов поддерживает три типа аварийной сигнализации. Когда срабатывает аварийная сигнализация, на передней панели коммутатора загорается соответствующий светодиод.

- Аварийная сигнализация электропитания (Power alarm): если включена данная функция, аварийная сигнализация будет срабатывать в случае проблем с одним из источников электропитания
- Аварийная сигнализация порта (Port alarm): если включена данная функция, аварийная сигнализация будет срабатывать в случае получении информации об отключении соответствующего порта (состояние Link Down).
- Аварийная сигнализация кольца (Ring alarm): если включена данная функция, аварийная сигнализация будет срабатывать в случае нарушения кольцевой топологии.

Только один «мастер» кольца протокола Sy2-Ring поддерживается функцией аварийной сигнализации кольца.

20.1.2. Настройка через WEB-интерфейс

1. Настройка аварийной сигнализации.

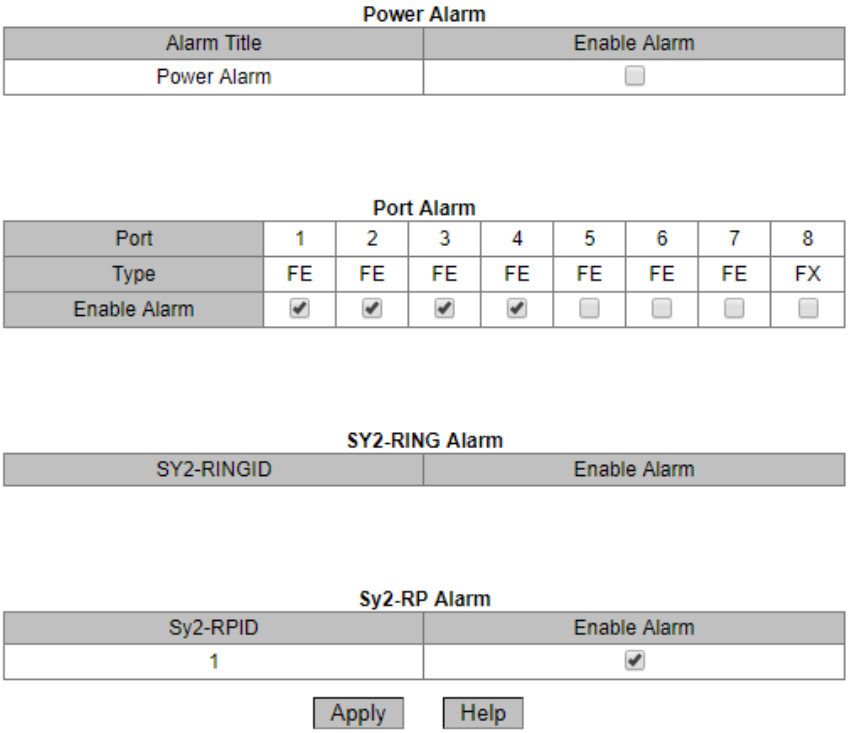


Рис. 149. Настройка аварийной сигнализации

Аварийная сигнализация электропитания (Power Alarm)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение/Выключение аварийной сигнализации по электропитанию.
Аварийная сигнализация порта (Port Alarm)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение/Выключение аварийной сигнализации порта.
Аварийная сигнализация кольца (Sy2-Ring Alarm)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Включение или Выключение функции Sy2-Ring.

2. Отображение статуса аварийной сигнализации после включения функции извещения о тревогах.

Power Alarm

Alarm Title	Alarm Status
power1	NONE
power2	WARN

Port Alarm

Port	1	2	3	4	5	6	7	8
Type	FE	FE	FE	FE	FE	FE	FE	FX
AlarmStatus	Link Up	Link Down	-	-	-	-	-	-

SY2-RING Alarm

SY2-RING ID	Alarm Status

Sy2-RP Alarm

Sy2-RP ID	Alarm Status
1	---

Рис. 150. Отображение статуса аварийной сигнализации

Статус аварийной сигнализации электропитания (Power Alarm Status)
Настраиваемые опции: NONE/WARN
Описание: После включения функции аварийной сигнализации электропитания состояние NONE отображается, если питание включено, а WARN отображается, если питание выключено.
Статус аварийной сигнализации порта (Port Alarm Status)
Настраиваемые опции: Link Up/Link Down
Описание: После того, как функция аварийной сигнализации порта активирована, состояние «Link Up» отображается, если порт функционирует в нормальном режиме, а если на порту отсутствует соединение или обнаруживается аномального соединение, тогда отображается состояние «Link Down».
Статус аварийной сигнализации кольца (Sy2-Ring Alarm Status)
Настраиваемые опции: Ring Open/Ring Close
Описание: После того, как функция аварийной сигнализации кольца включена, состояние «Ring Open» будет отображается, если кольцо находится в открытом, т.е. работоспособном, состоянии, а если в топологии кольца обнаружена коллизия, т.к. кольцо разомкнуто, отображается состояние «Ring Close».

20.2. Системный журнал (Syslog)

20.2.1. Введение

Данная функция ведёт журнал, в который записывается информация о системе, ошибки, возникающие неисправности и ошибки, а также многое другое. Системный журнал включает непосредственно сам системный журнал задач (System log), а также журнал учета экслуатации.

Системный журнал задач содержит следующую информацию:

- Список зарегистрированных задач;
- Журнал перезагрузок, вызванных приостановкой функционирования;
- Журнал перезагрузок, вызванных нажатием кнопки <Reset> (Сброс к заводским настройкам) на передней панели коммутатора;
- Журнал перезагрузок, вызванных командой Reboot (перезагрузка);
- Журнал перезагрузок, вызванных нажатием кнопки <Reboot> (перезагрузка) на странице веб-интерфейса;
- Журнал переерезагрузок системы.

Журнала учета эксплуатации содержит следующую информацию:

- Изменение состояния порта;
- Изменение состояния питания;
- Журнал перезагрузок, вызванных командой Reboot (перезагрузка);
- Журнал перезагрузок, вызванных нажатием кнопки <Reboot> (перезагрузка) на странице веб-интерфейса;

Поддерживается максимум 1024 записи журнала. Когда значение записей превысит 1024, будет создан новый журнал, который будет записываться «поверх» старого журнала.

20.2.2. Настройка через WEB-интерфейс

1. Настройте параметры системного журнала.

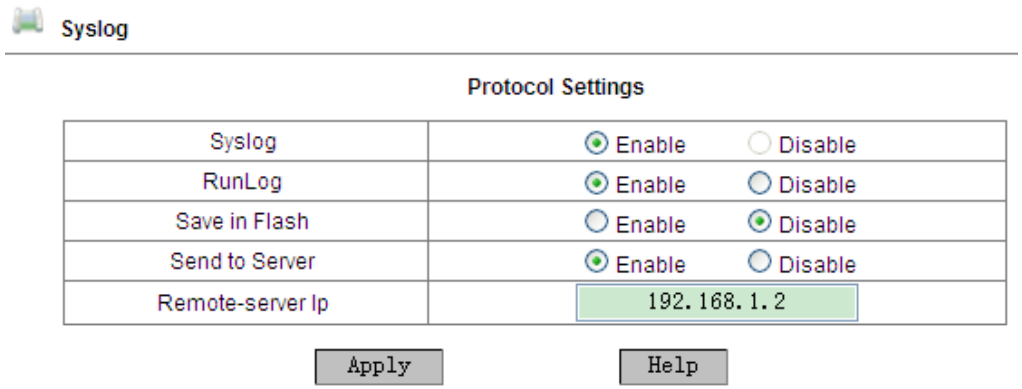


Рис. 151. Настройка параметров системного журнала

Системный журнал задач (Syslog)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Enable (Включено)

Описание: Включение/Выключение системного журнала задач. При установке режима «Enable» система сразу начинает запись информации.

Журнала учета эксплуатации (RunLog)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Enable (Включено)

Описание: Включение/Выключение журнала учета эксплуатации. При установке режима «Enable» система сразу начинает запись информации.

Запись во Flash-память (Save in Flash)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Описание: Включение или Выключение функции записи во flash-память. После включения данного режима записи можно будет просматривать в интерфейсе коммутатора.

Передача данных на сервер (Send to Server)

Настраиваемые опции: Enable/Disable (Включить/Выключить)

Значение по умолчанию: Disable (Выключено)

Описание: Включение или Выключение функции передачи записей системного журнала на сервер. После включения данного режима записи журнала могут быть загружены на сервер Syslog в режиме реального времени.

Настройка IP адреса сервера (Remote-server Ip)

Настроив IP-адрес сервера для загрузки системного журнала на сервер Syslog (например, посредством программы Tftp32), пользователи могут просматривать журналы в люлое время (см. рис. 152).

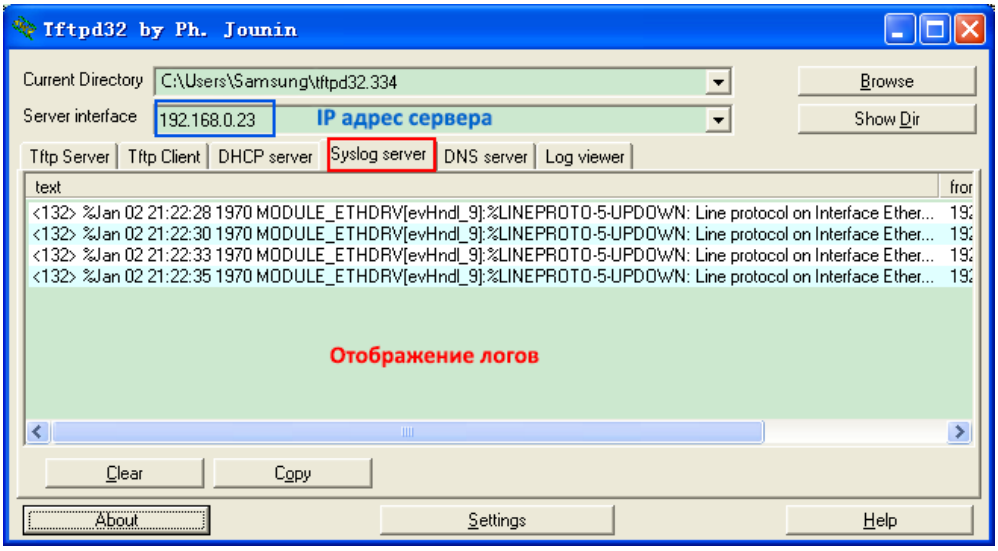


Рис. 152. Передача записей системного журнала на сервер

2. Настройте параметры загрузки.

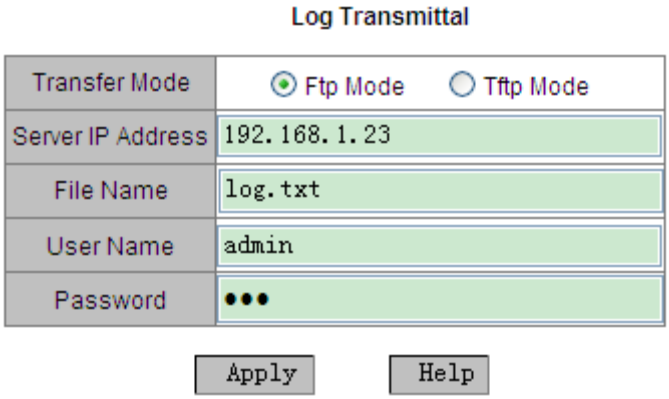


Рис. 153. Загрузка системного журнала через FTP режим

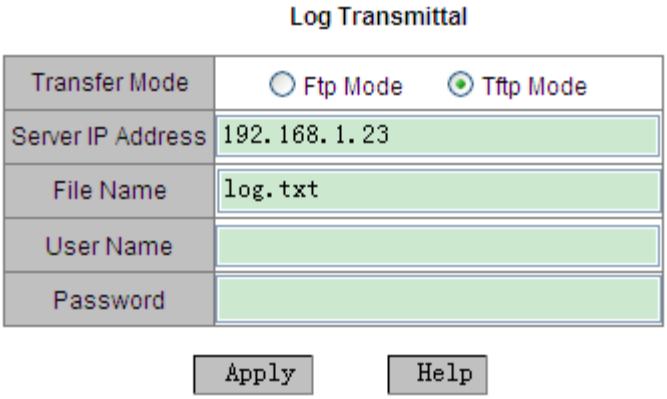


Рис. 154. Загрузка системного журнала через TFTP режим

Режим передачи (Transfer Mode)
Настраиваемые опции: Ftp Mode/Tftp Mode (Режим FTP/Режим TFTP)
Значение по умолчанию: Ftp Mode (Режим FTP)
Описание: Выбор режима загрузки записей системного журнала на сервер.
IP адрес сервера (Server IP Address)
Настраиваемый формац: A.B.C.D
Описание: Настройка IP адреса сервера FTP/TFTP.
Имя файла (File Name)
Настраиваемый диапазон: 1~32 символов
Описание: Назначение имени файла для загрузки на сервер записей системного журнала.
Имя пользователя (User Name)
Настраиваемый диапазон: 1~32 символов
Описание: Ввод имени пользователя FTP. Если выполняется загрузка с помощью TFTP, имя пользователя вводить не нужно.
Пароль (Password)
Настраиваемый диапазон: 1~32 символов
Описание: Ввод пароля пользователя FTP. Если выполняется загрузка с помощью TFTP, пароль вводить не нужно.

3. Отображение информации системного журнала

Runlog

SEQ ID	EVENT TYPE	TIME	CONTENT
15	port link alarm	THU AUG 25 10:54:07 2011	Port alarm: entity id:3 state:Link down
14	software reboot	THU AUG 25 10:46:37 2011	software system reboot.
13	port link alarm	THU AUG 25 10:43:04 2011	Port alarm: entity id:3 state:Link up
12	port link alarm	THU AUG 25 10:42:37 2011	Port alarm: entity id:3 state:Link down
11	software reboot	THU JAN 01 21:38:15 1970	software system reboot.
10	power alarm	THU JAN 01 20:41:13 1970	Power alarm: entity id:2 state:Power down
9	port link alarm	THU JAN 01 16:25:42 1970	Port alarm: entity id:5 state:Link up
8	port link alarm	THU JAN 01 16:25:38 1970	Port alarm: entity id:5 state:Link down
7	port link alarm	THU JAN 01 16:23:01 1970	Port alarm: entity id:5 state:Link up
6	port link alarm	THU JAN 01 16:22:57 1970	Port alarm: entity id:5 state:Link down
5	port link alarm	THU JAN 01 00:00:13 1970	Port alarm: entity id:5 state:Link up
4	port link alarm	THU JAN 01 00:00:10 1970	Port alarm: entity id:2 state:Link up
3	port link alarm	THU JAN 01 00:00:06 1970	Port alarm: entity id:1 state:Link up
2	software reboot	THU JAN 01 07:37:14 1970	software system reboot.
1	port link alarm	THU JAN 01 07:37:05 1970	Port alarm: entity id:8 state:Link up
0	port link alarm	THU JAN 01 07:37:01 1970	Port alarm: entity id:8 state:Link down

Apply Help

Рис. 155. Загрузка системного журнала через TFTP режим

Системный журнал (Log)
Отображаемая информация: {SEQ ID, EVENT TYPE, TIME, CONTENT} (Идентификатор записи, Тип события, Время события, Содержание события).
Описание: Отображение записей системного журнала.

В процессе загрузки информации системного журнала серверы FTP/TFTP должны находиться в состоянии онлайн.

21. Протокол SNMP

21.1. SNMPv2 (протокол SNMP версии 2)

21.1.1. Введение

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

21.1.2. Реализация

Для управления устройствами, SNMP использует архитектуру «manager/agent» (менеджер/агент). Таким образом, по функциональности он включает две составляющие: «NMS» и «Агент».

- Network Management Station (NMS) - это рабочая станция, на которой работает SNMP-приложение для управления сетью клиентов, играющая основную роль в управлении сетью с помощью протокола SNMP.
- Агент - это программный процесс на управляемом устройстве. Он отвечает за прием и обработку запросов от NMS. При возникновении аварийной ситуации агент автоматически информирует об этом NMS.

NMS является средством управления сетью SNMP, а Агент управляется сетью SNMP. Обмен информацией управления между NMS и Агентом осуществляется через протокол SNMP. SNMP обеспечивает выполнение 5 основных операций:

- 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 тревоги агент автоматически отправит сообщение «Trap» в NMS, чтобы сообщить о возникновении аномальных событий.

21.1.3. Описание

Агент SNMP данной серии коммутаторов поддерживает версии SNMPv2 и SNMPv3. При этом SNMPv2 совместим с SNMPv1.

SNMPv1 использует принцип аутентификации по имени сообщества (Community Name Authentication). Имя сообщества работает как пароль и используется для ограничения доступа Агента SNMP к SNMP NMS. Если имя сообщества SNMP-сообщения не может пройти аутентификацию устройства, отправленное сообщение будет удалено.

SNMPv2 также использует аутентификацию по имени сообщества. Он не просто совместим с SNMPv1, но и расширяет функции SNMPv1. Корректная совместная работа NMS и Агента основывается на согласованной версии SNMP. Агент может быть настроен для работы с несколькими версиями одновременно и использовать разные версии для связи с разными NMS.

21.1.4. Описание MIB (Management Information Base)

Любой управляемый ресурс можно рассматривать как объект, соответственно он называется управляемым объектом.

MIB (Management Information Base) - это совокупность всех управляемых объектов. MIB определяет иерархические отношения между управляемыми объектами и определяет основные атрибуты объектов, например, имя объекта, права доступа, типы данных и т.д. У каждого Агента есть своя MIB. NMS может читать или записывать объекты в MIB в соответствии со своими правами. Связь NMS, Агента и MIB показана на рисунке 156.

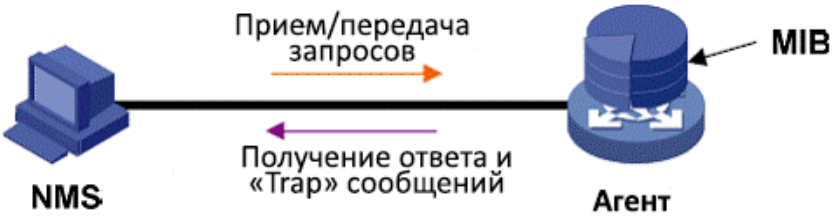


Рис. 156. Взаимосвязь NMS, Агента и базы MIB

MIB определяет древовидную структуру, где каждый узел дерева является управляемым объектом. Каждый узел дерева содержит OID (Идентификатор объекта), который может указывать позицию узла в структуре дерева MIB. OID управляемого объекта A равен 1.2.1.1 (см. рис. 157).

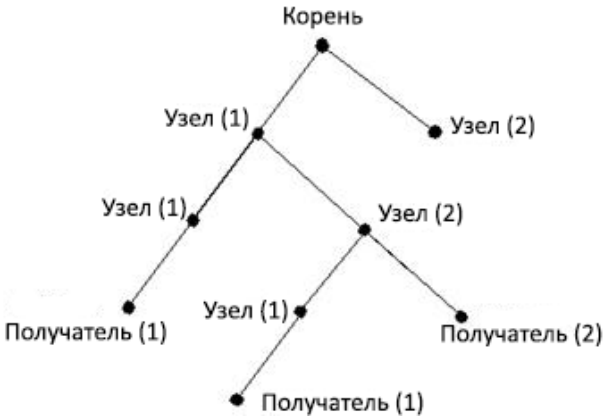


Рис. 157. Структура дерева MIB

21.1.5. Настройка через WEB-интерфейс

1. Включите протокол SNMP

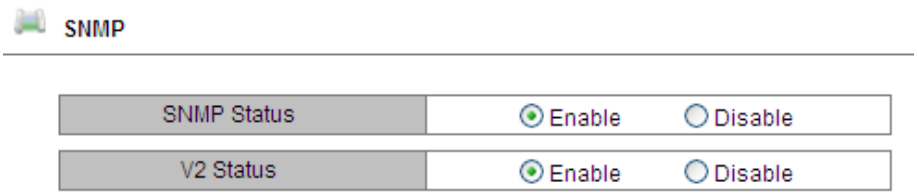


Рис. 158. Включение протокола SNMP и выбор версии SNMP

Статус SNMP (SNMP Status)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Enable (Включено)
Описание: Включение/Выключение протокола SNMP.
Статус версии 2 (V2 Status)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Enable (Включено)
Описание: Включение версии SNMPv2, которая совместима с версией SNMPv1.

2. Настройка прав доступа

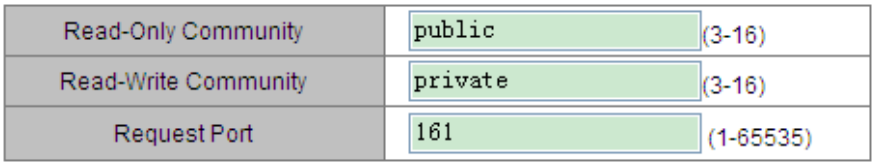


Рис. 159. Настройка прав доступа

Сообщество «Только чтение» (Read-Only Community)
Настраиваемый диапазон: 3~16 символов
Значение по умолчанию: Public (Открытый)
Описание: NMS может только читать информацию MIB, если имя сообщества, переданное в сообщении SNMP, отправленном из NMS, совпадает с именем сообщества, установленным здесь.
Имя пользователя (User Name)
Настраиваемый диапазон: 3~16 символов
Значение по умолчанию: Private (Персональный)
Описание: NMS может и читать и записывать информацию MIB, если имя сообщества, переданное в сообщении SNMP, отправленным из NMS, совпадает с именем сообщества, установленным здесь.
Порт запроса (Request Port)
Настраиваемый диапазон: 1~65535
Значение по умолчанию: 161
Описание: Настройка порта, который принимает запросы SNMP.

3. Настройка сообщений «Trap».

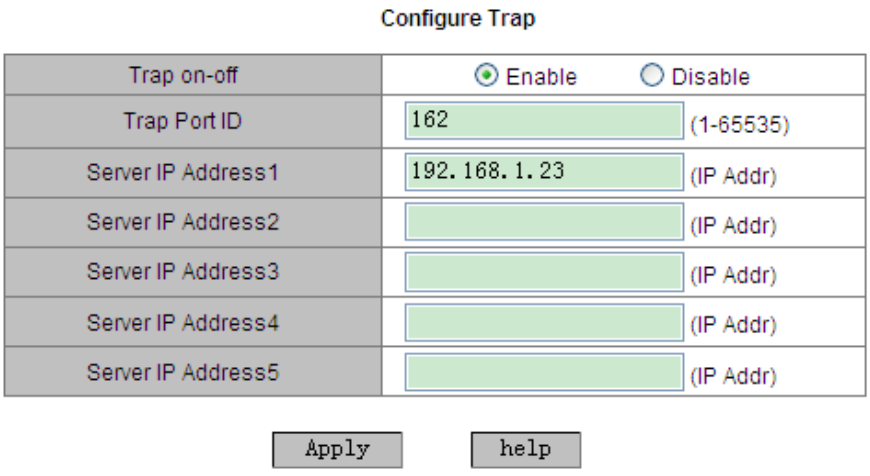


Рис. 160. Настройка сообщений Trap

Включение сообщений «Trap» (Trap on-off)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Enable (Включено)

Описание: Включение/Выключение функции отправки сообщений «Trap».

Настройка идентификатора порта для отправки сообщений «Trap» (Trap Port ID)

Настраиваемый диапазон: 3~65535

Значение по умолчанию: 162

Описание: Настройка идентификатора порта, передающего сообщения «Trap».

IP адрес сервера (Server IP Address)

Настраиваемый формат: A.B.C.D

Описание: Настройка IP адреса сервера, который будет получать сообщения «Trap». Максимально поддерживается до 5 IP адресов.

4. Отображение IP адресов сервера управления.

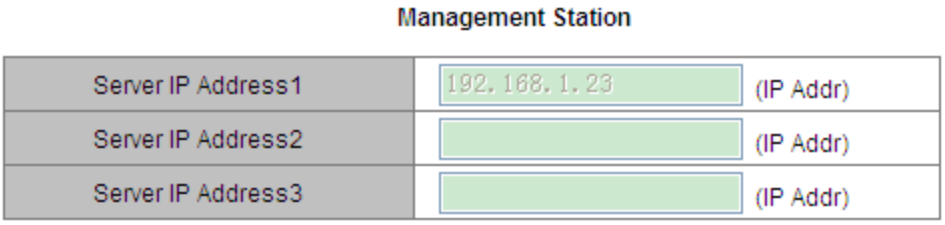


Рис. 161. IP адрес сервера управления

Нет необходимости вручную устанавливать IP адреса сервера. Они будут автоматически отображаться в процессе загрузки на сервере программного обеспечения управления сетью и в информации о модуле MIB на устройстве с функцией чтение/запись.

21.1.6. Пример типовой настройки

NMS с SNMP подключается к коммутатору через сеть Ethernet. IP адрес NMS: 192.168.1.23, а IP адрес коммутатора: 192.168.1.2. NMS управляет и контролирует Агента с помощью протокола SNMPv2, который может читать и записывать информацию MIB Агента, а Агент автоматически отправляет сообщения «Trap» в NMS, когда у Агента происходит аварийная ситуация (см. рис. 162).

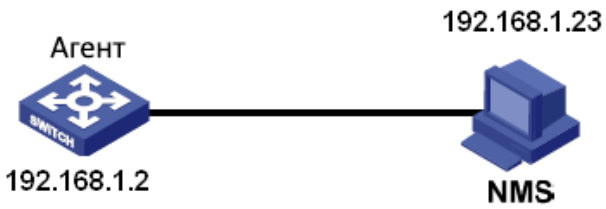


Рис. 162. Пример настройки SNMPv2

Настройка Агента:

1. Включите протокол SNMP версии v2 (см. рис. 158);
2. Настройте права доступа для имени сообщества «Read-Only» как «public», а для имени сообщества «Read-Write» «private», порту запроса присвойте значение 161 (см. рис. 159).

3. Включите режим «Trap» сообщений, идентификатору порта с включенным режимом «Trap» должно быть присвоено значени 162, IP адрес сервера: 192.168.1.23 (см. рис. 160).

Если пользователю необходимо управлять и контролировать Агента, необходимо использовать соответствующее программное обеспечение, например, Symanitron NMS.

21.2. SNMPv3

21.2.1. Введение

SNMPv3 предоставляет собой механизм аутентификации USM (User-Based Security Model). Пользователь может настроить функции шифрования и аутентификации. Аутентификация используется для проверки легальности отправителя сообщения для того, чтобы избежать доступа нелегальных пользователей. SNMPv3 обеспечивает шифрование передаваемых сообщений между NMS и агентом, чтобы избежать их незаконного просмотра. Комбинация аутентификации и шифрования улучшает безопасность связи между SNMP NMS и Агентом SNMP.

21.2.2. Реализация

SNMPv3 имеет 4 таблицы конфигурации, для каждой из которых может создать 16 записей. Эти таблицы определяют, могут ли указанные пользователи н получать доступ к информации MIB.

Пользовательская таблица используется для создания пользователей. Каждый пользователь может использовать разные политики безопасности для реализации функций аутентификации, шифрования и других функций безопасности.

Таблица доступа может обращаться к информации узла MIB, сопоставляя имя группы, контекстное имя и устанавливать соответствующий уровень безопасности.

Групповая таблица - это совокупность нескольких пользователей. Права доступа устанавливаются для группы пользователей и применимы для всех пользователей в группе. Контекстная таблица - это читаемые строки символов для идентификации пользователей. Это не имеет никакого отношения к конкретной модели безопасности.

21.2.3. Настройка через WEB-интерфейс

1. Настройка пользовательской таблицы.

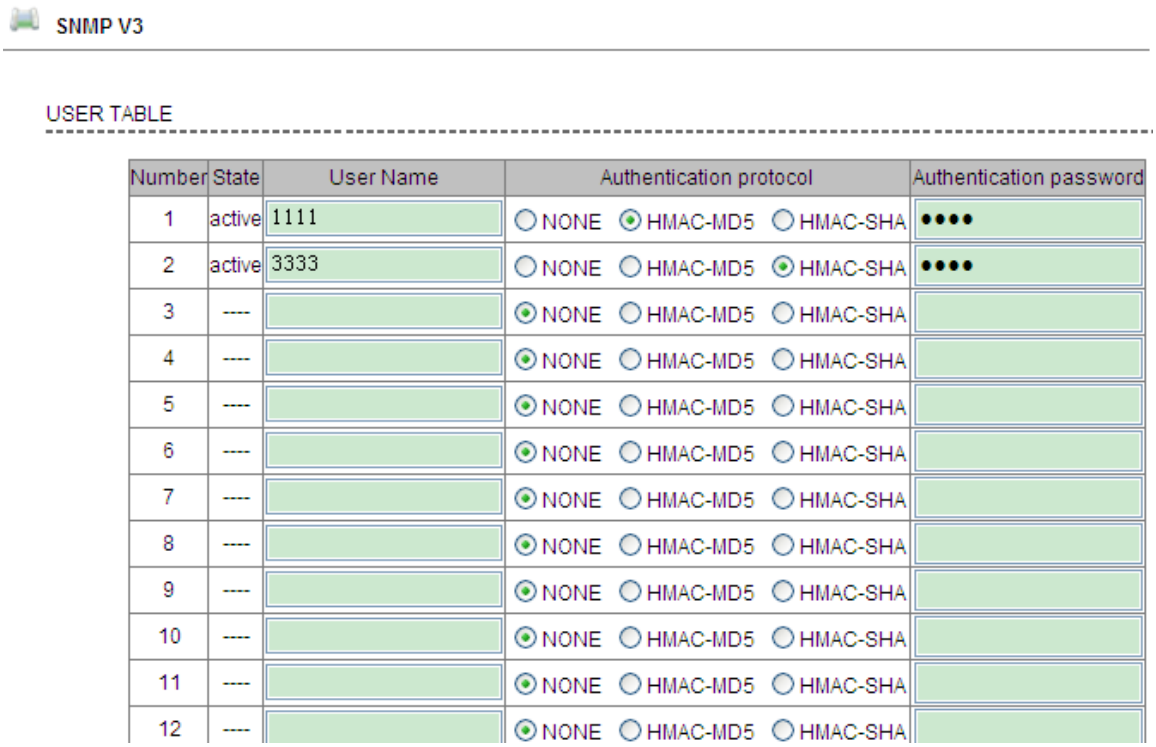


Рис. 163. Настройка таблицы пользователей SNMPv3

Имя пользователя (User Name)
Настраиваемый диапазон: 4~16 символов
Описание: Создание имени пользователя.
Протокол аутентификации (Authentication Protocol)
Настраиваемые опции: NONE/HMAC-MD5/HMAC-SHA
Значение по умолчанию: NONE
Описание: Выбор типа алгоритма шифрования для аутентификации.
Пароль для аутентификации (Authentication Password)
Настраиваемый диапазон: 4~16 символов
Описание: Настройка пароля пользователя.

1. Настройка таблицы доступа

ACCESS TABLE

Number	GroupName	ContextName	SecurityModel	SecurityLevel
1	1111	2222	SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
2	3333	4444	SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
3			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
4			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
5			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
6			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
7			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
8			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
9			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
10			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
11			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
12			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
13			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
14			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
15			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv
16			SNMP V3 SNMP V2	NoAuthNoPriv AuthNoPriv

Рис. 164. Настройка таблицы доступа SNMPv3

Имя группы (Group Name)
Настраиваемый диапазон: 4~16 символов
Описание: Настройка имени группы. Для данной серии коммутаторов каждая группа предназначена только для одного пользователя, поэтому имя группы должно совпадать с именем пользователя, установленным в таблице пользователей.
Контекстное имя (Context Name)
Настраиваемые опции: 4~16 символов
Описание: Настройка контекстного имени.
Модель безопасности (Security Model)
Настраиваемый диапазон: SNMPv3/ SNMPv2
Описание: Значение SNMPv3 указывает на использование технологии USM. SNMPv3 выбирается принудительно.
Уровень безопасности (Security Level)
Настраиваемые опции: NoAuthNoPriv/AuthNoPriv
Значение по умолчанию: NoAuthNoPriv
Описание: Настройка необходимости аутентификации и шифрования при доступе к информации MIB. Значение NoAuthNoPriv: не требуется ни аутентификация, ни шифрование; значение AuthNoPriv: нужна аутентификация, шифрование не требуется.

2. Настройка контекстной таблицы

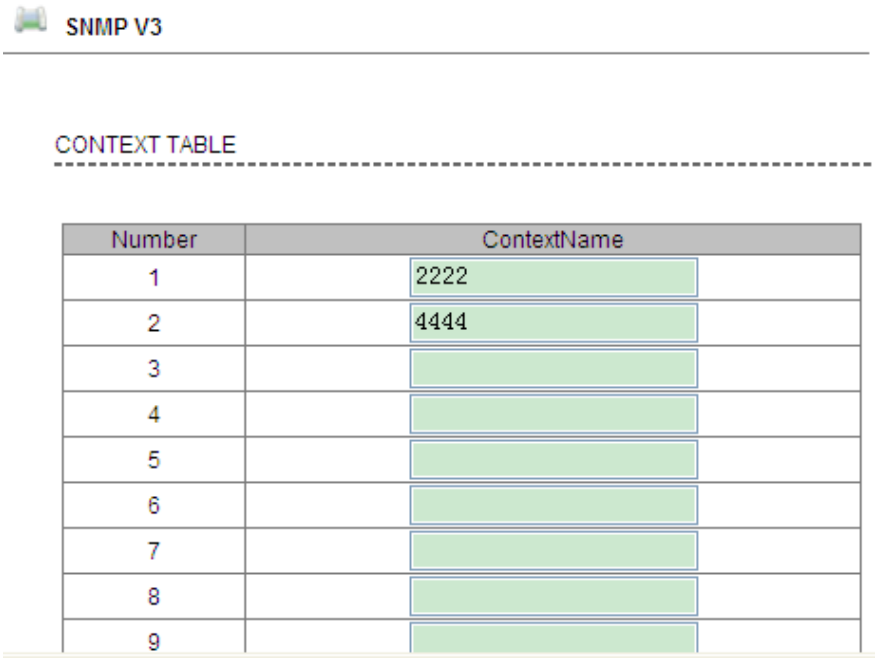


Рис. 165. Настройка контекстной таблицы SNMPv3

Имя группы (Group Name)
Настраиваемый диапазон: 4~16 символов
Описание: Определение серии управляемых объектов, к которым можно получить доступ по протоколу SNMP. Это имя должно совпадать с контекстным именем, установленным в таблице доступа.

3. Настройка групповой таблицы

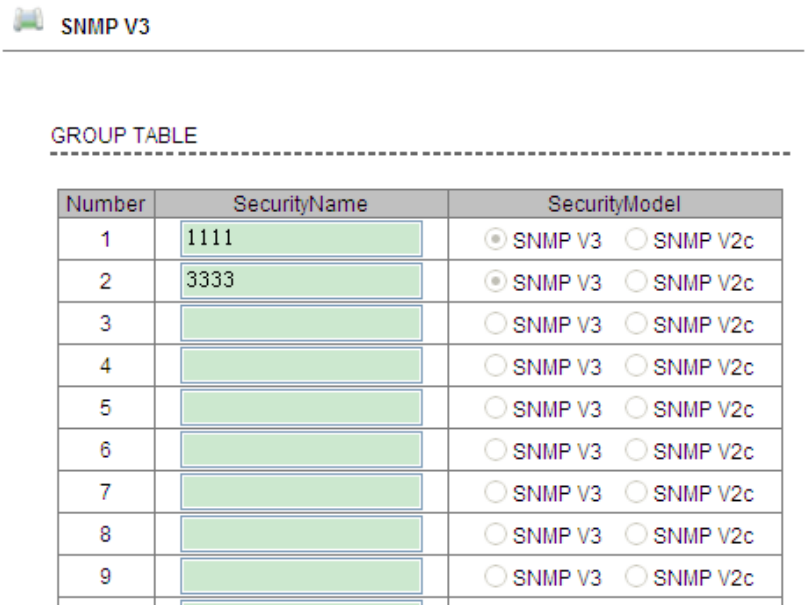


Рис. 166. Групповая таблица SNMPv3

Имя безопасной группы (Security Name)
Настраиваемый диапазон: 4~16 символов
Описание: Настройка имени группы легальных пользователей. Для данной серии коммутаторов каждая группа предназначена только для одного пользователя, поэтому имя безопасной группы должно совпадать с именем пользователя, установленным в таблице пользователей.
Модель безопасности (Security Level)
Настраиваемые опции: SNMPv3/SNMPv2
Значение по умолчанию: SNMPv3
Описание: Параметр SNMPv3 означает использование технологии USM. В настоящее время SNMPv3 выбирается принудительно.

21.2.4. Пример типовой настройки

Как показано на рис. 167, SNMP NMS подключается к коммутатору через сеть Ethernet, IP адрес NMS: 192.168.1.23, IP адрес коммутатора: 192.168.1.2. Пользователь с именем «111» контролирует и управляет Агентом по SNMPv3, протокол аутентификации: HMAC-MD5, уровень безопасности: AuthNoPriv.

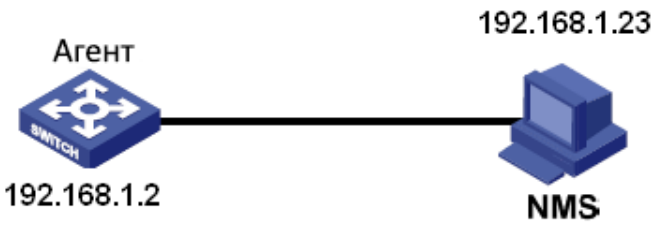


Рис. 167. Пример настройки SNMPv3

Настройка Агента:
1. Настройте таблицу пользователей SNMPv3. Задайте имя пользователя «111», выберите протокол аутентификации HMAC-MD5 и установите пароль аутентификации «аааа» (см. рис. 163).
2. Настройте таблицу доступа SNMPv3. Задайте имя группы «1111», а имя контекстное имя «2222», выберите уровень безопасности «AuthNoPriv» (см. рис. 164).
3. Настройте контекстную таблицу SNMPv3. Задайте имя контекста «2222» (см. рис. 165).
4. Настройте групповую таблицу SNMPv3. Задайте имя безопасной группы «1111» (см. рис. 166).

Если пользователю необходимо управлять и контролировать Агента, необходимо использовать соответствующее программное обеспечение, например, Symanitron NMS.

22. Протокол DHCP

Благодаря непрерывному расширению масштабов сетей и возрастанию их уровня сложности, особенно в условиях частых перемещений устройств (таких как ноутбуки или устройства в беспроводной сети), количество которых превосходит распределяемые IP адреса, протокол BOOTP, который специально предназначен для настройки статических

хостов, становится все более неспособным удовлетворить реальные потребности сети. Поэтому для быстрого доступа к сети и повышения коэффициента использования ресурсов IP адресов необходимо было разработать автоматический механизм назначения IP адресов, основанный на BOOTP. Для решения этих проблем и был создан протокол DHCP (Dynamic Host Configuration Protocol, Протокол динамической конфигурации хоста).
Протокол DHCP использует модель взаимодействия клиент/сервер. Клиент отправляет на сервер запрос на конфигурацию, а сервер, соответственно, отвечает на этот запрос отправкой параметров конфигурации, а именно назначает IP адрес для клиента, обеспечивая динамическую настройку IP адресов. Структура типичного приложения DHCP показана на рис. 168.

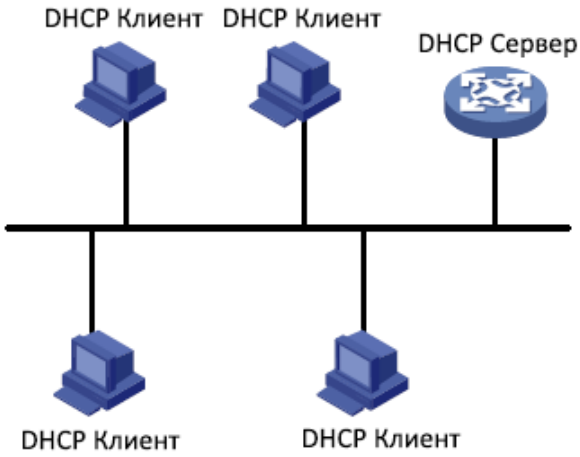


Рис. 168. Пример настройки SNMPv3

В процессе динамического получения IP адресов сообщения передаются в режиме широковещательной передачи, поэтому требуется, чтобы клиент DHCP и сервер DHCP сервер находились в одном сегменте. Если они находятся в разных сегментах, клиент может подключиться к серверу с помощью функцию DHCP relay для получения IP адресов и других параметров конфигурации. Коммутаторы данной серии не поддерживают функцию DHCP relay, поэтому клиент и сервер должны находиться в одном сегменте.

DHCP поддерживает два типа механизмов распределения IP адресов.

- Статическое распределение (Static allocation): сетевой администратор статически связывает фиксированные IP адреса с несколькими конкретными клиентами, такими как сервер WWW, и отправляет привязанные IP адреса клиентам посредством протокола DHCP. Этот механизм распределения содержит связку IP адреса порта и MAC адреса.
- Динамическое распределение: сервер DHCP динамически выделяет IP адрес клиенту. Этот механизм распределения может назначать либо постоянный IP адрес, либо IP адрес с ограниченным сроком действия. Когда срок действия истекает, клиенту необходимо повторно получить IP адрес.

Сетевой администратор может выбрать механизм распределения DHCP для каждого клиента.

22.1. Настройка сервера DHCP

22.1.1. Введение

Сервер DHCP является поставщиком услуг DHCP. Он использует сообщения DHCP для связи с клиентом DHCP, для того чтобы назначить подходящий IP адрес клиенту, а также, по мере необходимости, назначить другие сетевые параметры клиенту. Сервер DHCP обычно используется для распределения IP адресов при следующих условиях:

- Большой масштаб сети. Слишком сложно вручную осуществить конфигурацию сети, сложно управлять такой сетью.
- Количество хостов превышают число назначаемых IP адресов и невозможно назначить фиксированный IP адрес для каждого хоста.
- Только несколько хостов в сети нуждаются в фиксированных IP адресах.

22.1.2. Пул адресов DHCP

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

1. IP адрес, статически связанный к MAC адресу клиента или идентификатор порта, подключенный к серверу.
2. IP адрес, который записан на сервере DHCP, когда-либо был выделен клиенту.
3. IP адрес, который указан в запросе, полученном от клиента.
4. Первый доступный IP адрес, найденный в пуле адресов.
5. Если нет доступного IP адреса, проверяется IP адрес, срок действия которого истекает, и у которого были конфликты в процессе использования. Если такой IP адрес найден, он присваивается клиенту. Если нет, то не происходит никакого процесса.

22.1.3. Настройка через WEB-интерфейс

1. Включение DHCP сервера

Configuration Options	Configuration Information
DHCP server status	(•) Enable ( ) Disable
DHCP server mode	( ) Common-Mode (•) Port-Mode

Рис. 169. Статус сервера DHCP

Статус сервера DHCP (DHCP server status)
Настраиваемые опции: Enable/Disable (Включить/Выключить)
Значение по умолчанию: Disable (Выключено)
Описание: Выбор данного коммутатора в качестве сервера DHCP для назначения клиенту IP адреса.

2. Выбор режима работы сервера DHCP

Configuration Options	Configuration Information
DHCP server status	(•) Enable ( ) Disable
DHCP server mode	( ) Common-Mode (•) Port-Mode

Рис. 170. Режим сервера DHCP

Режим сервера DHCP (DHCP server mode)
Настраиваемые опции: Common-mode/Port-mode (Общий режим/Режим порта)
Значение по умолчанию: Common mode (Общий режим)
Описание: Общий режим (Common mode) обеспечивает динамическое распределение IP адресов и привязку статического MAC адреса. Режим порта (Port-mode) означает, что выполняется настройка IP адреса требуемого порта.

3. Настройка режима Port-mode.

При выборе режима Port-mode в режиме настройки DHCP сервера необходимо распределить привязку статических IP адресов по портам (см. рис. 171).

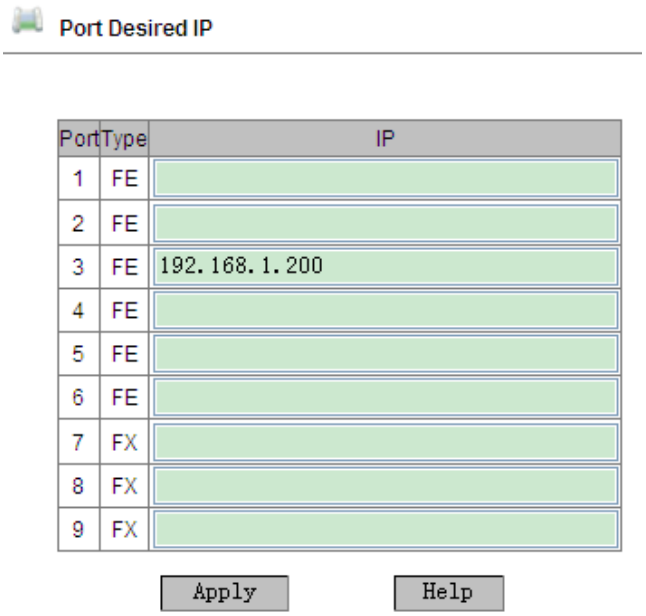


Рис. 171. IP-адрес требуемого порта

IP-адрес требуемого порта - это статическая настройка IP адреса порта. Когда порт получает запрос от клиента, IP-адрес, привязанный к порту, будет выделен для клиента. Этот режим распределения IP-адресов имеет наивысший приоритет, а период действия составляет 1000 дней 23 часа 59 минут.

IP-адрес, привязанный к порту и сервер DHCP должны находиться в одном сегменте сети.

Когда для назначения IP-адресов выбран режим Port-mode, вам необходимо настроить сервер DHCP (см. рис. 172).

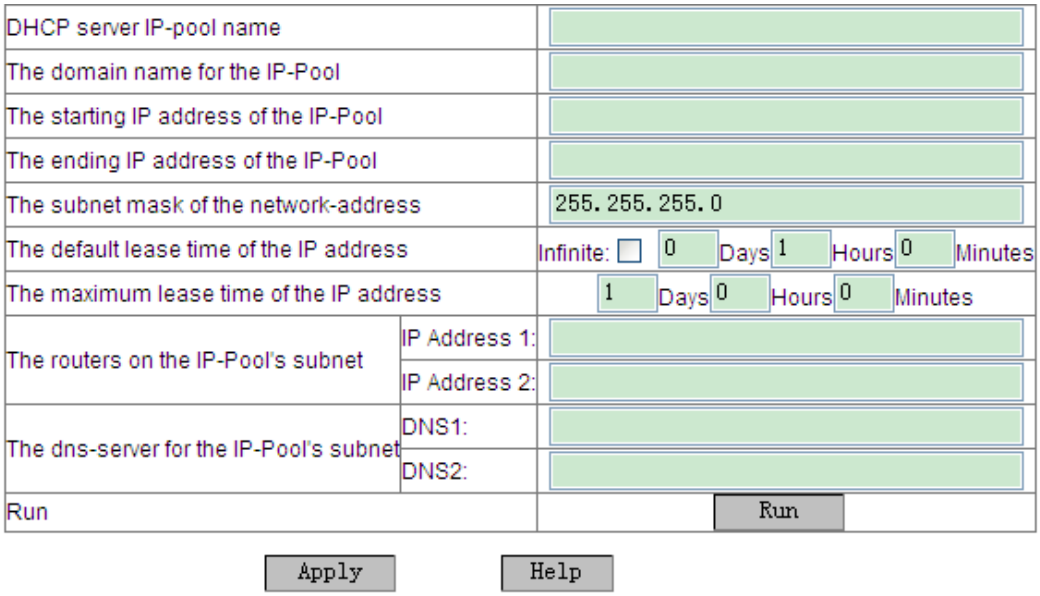


Рис. 172. Настройка сервера DHCP для режима Port-mode

После настройки нажмите кнопку <Run>, чтобы назначить соответствующие IP адреса клиентам.

4. Настройка режима Common mode

Когда режим сервера DHCP сервера установлен в значение Common-Mode, подразумевается, что присутствует привязка статических MAC адресов к динамическому распределению IP адресов. При наличии связки статических MAC адресов система распределяет соответствующий IP адрес, привязанный к MAC адресу. В противном случае динамически выделяет IP адреса из пула адресов. Конфигурация привязки статического MAC адреса показана на рис. 173 и рис. 174; конфигурация динамического распределения IP адресов показана на рисунке 175.

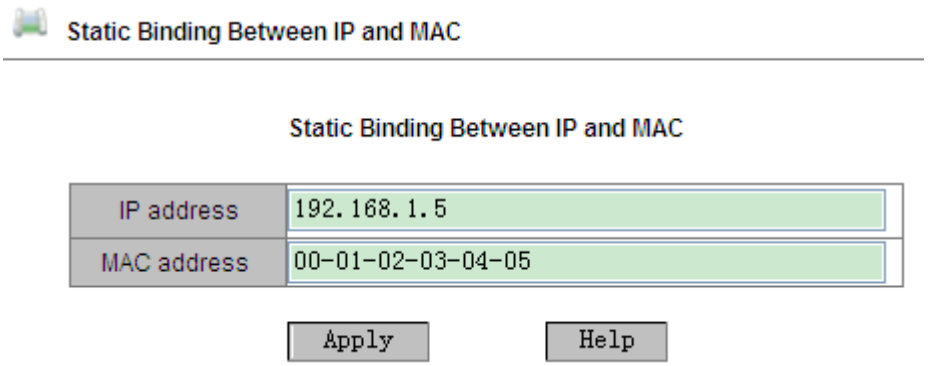


Рис. 173. Привязка статических MAC адресов

Привязка статических MAC адресов - это привязка MAC адреса клиента к IP адресу. Если сервер получает сообщение с запросом на получение IP адреса, MAC адрес которого настроен в данном разделе, клиенту будет выделен IP адрес, связанный с этим MAC

адресом. Для функционирования такого режима распределения IP адресов необходима соответствующая настройка сервера (см. рис. 175).
После настройки можно посмотреть «Список привязки статических MAC адресов к IP адресам. Отметьте в поле «Index» соответствующую запись, чтобы удалить соответствующую привязку.

The list of Static Binding Between IP and MAC

Index	IP Address	MAC Address
☐	192.168.1.200	00-72-74-76-78-7A
☐	192.168.1.5	00-01-02-03-04-05

Delete

Рис. 174. Список привязки статических MAC адресов

DHCP server IP-pool name		1
The domain name for the IP-Pool		a
The starting IP address of the IP-Pool		192. 168. 1. 100
The ending IP address of the IP-Pool		192. 168. 1. 201
The subnet mask of the network-address		255. 255. 255. 0
The default lease time of the IP address		Infinite: ☐ 0 Days 1 Hours 0 Minutes
The maximum lease time of the IP address		1 Days 0 Hours 0 Minutes
The routers on the IP-Pool's subnet	IP Address 1:	192. 168. 1. 1
	IP Address 2:	
The dns-server for the IP-Pool's subnet	DNS1:	
	DNS2:	
Run		Run

Apply Help

Рис. 175. Настройка сервера в режиме Common mode

Имя пула IP адресов сервера DHCP (DHCP server IP-pool name)
Настраиваемый диапазон: 1~15 символов;
Описание: Настройка имени пула IP адресов.
Имя домена пула IP адресов (The domain name for the IP-Pool)
Настраиваемый диапазон: 1~60 символов;
Описание: Настройка имени домена пула IP адресов.
Начальный IP адрес пула / Конечный IP адрес пула (The starting IP address of the IP-Pool / The ending IP address of the IP-Pool)
Настраиваемый формат: A.B.C.D (начальный и конечный IP адреса должны находиться в одном сегменте сети).
Маска подсети сетевого адреса (The subnet mask of the network-address)

Значение обычно настроено как 255.255.255.0. При распределении динамических адресов необходимо задать диапазон пула IP адресов, а диапазон адресов определяется маской подсети.

Время действия IP адресов по умолчанию (The default lease time of the IP address)

Настраиваемый диапазон: 0 дней : 0 часов : 1 минута – 1000 дней : 23 часа : 59 минут / Бесконечность (Infinite);

Значение по умолчанию: 0 дней : 1 час : 0 минут

Описание: Если сообщение с запросом IP адреса, отправленное клиентом, не содержит действительного времени действия, время действия IP адреса, выделенного сервером, устанавливается в значение по умолчанию.

Максимальное время действия IP адресов (The maximum lease time of the IP address)

Настраиваемый диапазон: 0 дней : 0 часов : 1 минута – 1000 дней : 23 часа : 59 минут;

Значение по умолчанию: 1 день : 0 часов : 0 минут

Описание: Когда клиент отправляет на сервер сообщение с запросом IP адреса, время действия сообщения не может быть больше максимального времени действия IP адреса. Для различных пулов адресов сервер DHCP может устанавливать различное время действия адреса, при этом адреса в одном и том же пуле адресов DHCP имеют одинаковое время действия.

Маршрутизация в подсети пула IP адресов (The routers on the IP-Pool's subnet)

Настраиваемый диапазон: Адреса, которые находятся в том же сегменте, что и пул адресов;

Описание: Если клиент DHCP посещает хост, находящийся в другом сегменте, то данные должны пересылаться через шлюзы. Когда сервер DHCP распределяет IP адреса клиентам, он может одновременно указывать адреса шлюза. Пул адресов DHCP может настроить максимально два адреса шлюза.

Сервер DNS для подсети пула IP адресов (The dns-server for the IP-Pool's subnet)

Описание: Когда происходит подключение к какому-либо хосту сети при помощи имени домена, оно должно быть присвоено IP адресу, который назначен посредством DNS. Если клиент DHCP подключается узлу сети с использованием имени домена, когда IP адреса клиентам назначает сервер DHCP, он может одновременно назначить IP адрес сервера имени домена. Пул адресов DHCP может настроить максимум два адреса DNS.

После настройки нажмите кнопку <Run>, чтобы назначить соответствующие IP адреса клиентам.

22.1.4. Пример типовой настройки

Как показано на рис. 176, коммутатор A работает как сервер DHCP, а коммутатор B работает как клиент DHCP. Порт 3 коммутатора A подключается к порту 4 коммутатора B. Клиент отправляет сообщения с запросом IP адреса, а сервер может назначить IP адрес клиенту тремя способами.

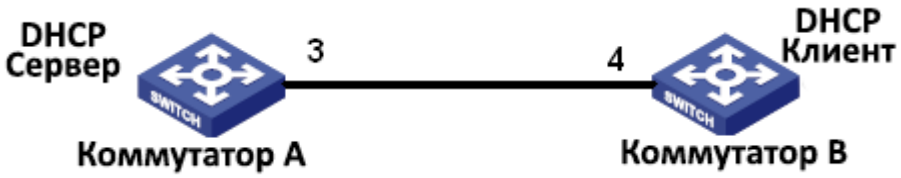


Рис. 176. Пример типичной настройки DHCP

Привязка IP адреса к порту:

1. Настройка коммутатора A:
   - Установите статус сервера DHCP в состояние «Enable» (Включено), см. рис. 169;
   - В разделе настроек сервера DHCP выберите режим «Port-Mode», см. рис. 170;
   - Настройте маску подсети как 255.255.255.0, см. рис. 172;
   - К порту 3 привяжите IP адрес 192.168.1.200, см. рис. 171;
   - Нажмите кнопку <Run> в интерфейсе настроек сервера, чтобы активировать работу сервера.
2. Настройка коммутатора B:
   - Настройте IP адрес клиента DHCP в разделе настроек IP адреса коммутатора B, см. рис. 14;
   - Коммутатор B получит IP адрес 192.168.1.200 и маску подсети 255.255.255.0 от сервера DHCP, см. рис. 177.

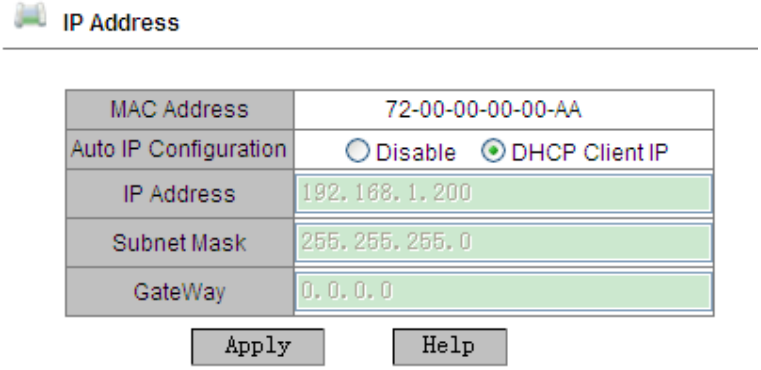


Рис. 177. Получение IP адреса клиентом DHCP

Метод привязки статического MAC адреса:

1. Настройка коммутатора A:
   - Установите статус сервера DHCP в состояние «Enable» (Включено), см. рис. 169;
   - В разделе настроек сервера DHCP выберите режим «Common mode», см. рис. 170;
   - Задайте имя пула IP адресов равным «1», назначьте имени домена пула адресов значение «a», настройте начальный адрес пула адресов как 192.168.1.100 и конечный адрес как 192.168.1.200, настройте маску подсети: 255.255.255.0 и адрес шлюза как 192.168.1.1, параметр «время действия» установите в значение «по умолчанию», см. рис. 172;
   - Привяжите MAC адрес коммутатора B «00-72-74-76-78-7a» к IP адресу 192.168.1.250, см. рис. 173;
   - Нажмите кнопку <Run> в интерфейсе настроек сервера, чтобы активировать работу сервера.
2. Настройка коммутатора B:

- Настройте IP адрес клиента DHCP в разделе настроек IP адреса коммутатора B, см. рис. 14;
- Коммутатор B получит IP адрес 192.168.1.250, маску подсети 255.255.255.0 и адрес шлюза 192.168.1.1 от сервера DHCP, см. рис. 178.

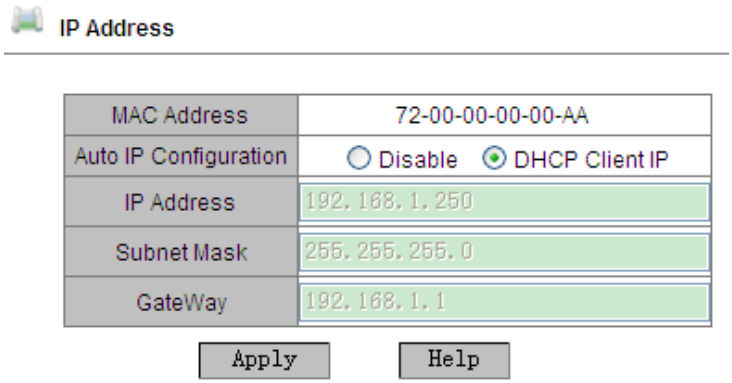


Рис. 178. Получение IP адреса клиентом DHCP

Динамическое получение IP-адреса из пула адресов:

1. Настройка коммутатора A:
   - Установите статус сервера DHCP в состояние «Enable» (Включено), см. рис. 169;
   - В разделе настроек сервера DHCP выберите режим «Common mode», см. рис. 170;
   - Задайте имя пула IP адресов равным «1», назначьте имени домена пула адресов значение «a», настройте начальный адрес пула адресов как 192.168.1.100 и конечный адрес как 192.168.1.200, настройте маску подсети: 255.255.255.0 и адрес шлюза как 192.168.1.1, параметр «время действия» установите в значение «по умолчанию», см. рис. 172;
   - Нажмите кнопку <Run> в интерфейсе настроек сервера, чтобы активировать работу сервера.
2. Настройка коммутатора B:
   - Настройте IP адрес клиента DHCP в разделе настроек IP адреса коммутатора B, см. рис. 14;
   - DHCP-сервер по порядку выполняет поиск возможных к назначению IP адресов в пуле адресов и выделяет первый найденный свободный IP-адрес, а также присваивает другие сетевые параметры для коммутатора B. Маска подсети: 255.255.255.0, а адрес шлюза - 192.168.1.1 (см. рис. 179).

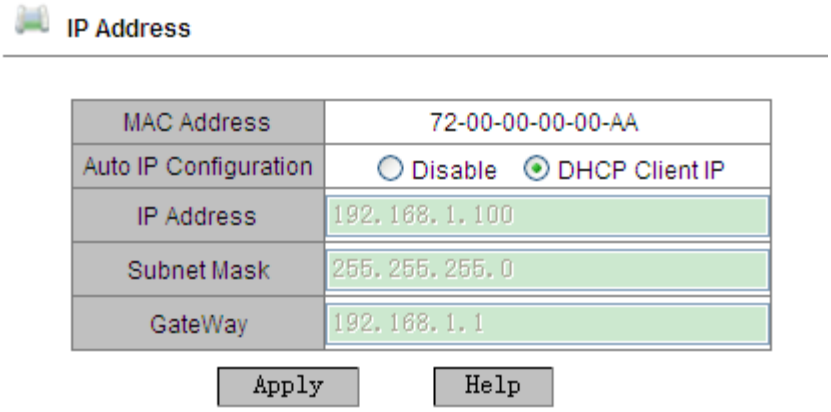


Рис. 179. Получение IP адреса клиентом DHCP

22.2. DHCP Snooping

22.2.1. Введение

DHCP Snooping - это функция мониторинга сервисов DHCP на 2-м уровне, которая также является функцией безопасности DHCP, обеспечивающей безопасность клиента. Механизм безопасности DHCP Snooping осуществляет контроль за тем, чтобы только доверенный порт мог перенаправить сообщение с запросом клиента DHCP на действительный сервер. Кроме того DHCP Snooping может контролировать источник ответного сообщения сервера DHCP, гарантируя клиенту получение IP адреса от действительного сервера, предотвращая назначения IP адресов или параметров конфигурации другим хостам от поддельных или недопустимых серверов DHCP.
Механизм безопасности DHCP Snooping делит порты на доверенные и ненадежные.

- Доверенный порт: это порт, который подключается к действительному серверу DHCP. Доверенный порт обычно перенаправляет сообщения с запросом клиентов DHCP и ответные сообщения серверов DHCP, чтобы клиенты DHCP могли получать действительные IP адреса гарантированно.
- Ненадежный порт: это порт, который подключен к недействительному серверу DHCP. Ненадежный порт не перенаправляет сообщения с запросом клиентов DHCP и ответные сообщения серверов серверов DHCP, чтобы клиенты DHCP не получали недействительные IP адреса.

22.2.2. Настройка через WEB-интерфейс

1. Включение функции DHCP Snooping.

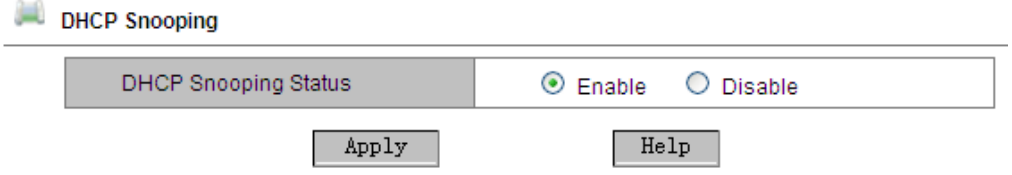


Рис. 180. Статус DHCP Snooping

Статус DHCP Snooping (DHCP Snooping Status)
Настраиваемые опции: Enable/Disable (Включено/Выключено)
По умолчанию: Disable (Выключено)
Описание: Включение/Выключение функции DHCP Snooping.

У коммутатора, который работает и как сервер DHCP и как клиент, нельзя включить функцию DHCP Snooping.

2. Настройка доверенных портов.

Trust-Port Settings

Port	Type	Protocol Status
1	FE	(•) Trust ( ) Untrust
2	FE	( ) Trust (•) Untrust
3	FE	(•) Trust ( ) Untrust
4	FE	( ) Trust (•) Untrust
5	FE	(•) Trust ( ) Untrust
6	FE	( ) Trust (•) Untrust
G1	GX	( ) Trust (•) Untrust
G2	GX	( ) Trust (•) Untrust
G3	GX	( ) Trust (•) Untrust

Apply Help

Рис. 181. Настройка доверенных портов

Статус протокола (Protocol Status)
Настраиваемые опции: Trust/Untrust (Доверенный/Ненадежный)
Значение по умолчанию: Untrust (Ненадежный)
Описание: Установка порта в режимы Доверенный/Ненадежный. Порты, которые соединяются с действительными DHCP-серверами прямо или косвенно, являются доверенными портами.

Настройка порта как доверенного и назначение его транковым портом (Port Trunk) являются взаимоисключающими. Порт, принадлежащий транковой группе, нельзя настроить как доверенный порт. Доверенный порт не может быть присоединен к транковой группе.

22.2.3. Пример типовой настройки

Как показано на рис. 182, клиент DHCP запрашивает IP адрес у сервера DHCP. В сети присутствует недействительный сервер DHCP. Настройте порт 1 как доверенный с помощью функции DHCP Snooping, чтобы можно было переслать сообщение с запросом клиента DHCP на сервер DHCP и направить ответное сообщение сервера DHCP клиенту DHCP. Установите порт 3 как ненадежный, который не сможет переслать сообщение с запросом клиента DHCP и получить ответное сообщение недействительного сервера DHCP, чтобы гарантировать клиенту получение действительного IP адреса от действительного сервера DHCP.

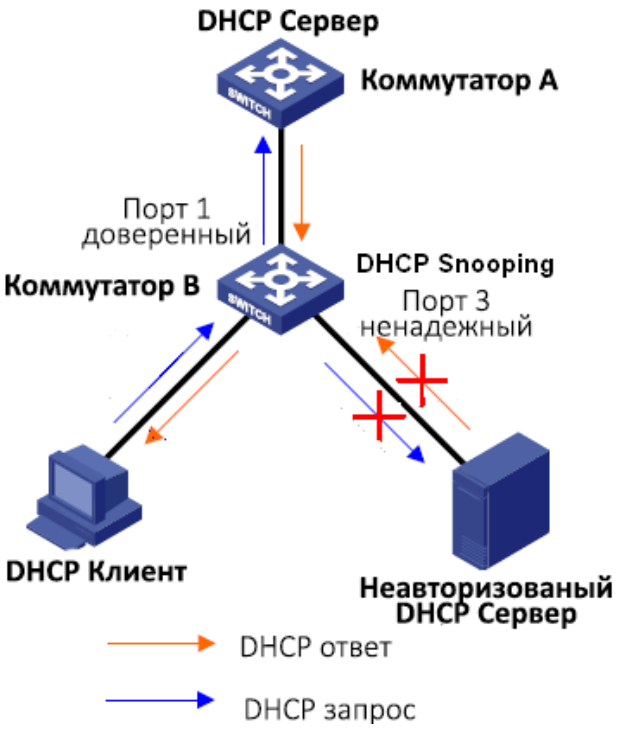


Рис. 182. Пример типовой настройки DHCP Snooping

Настройка коммутатора B:

- Включите функцию DHCP Snooping, см. рис. 180
- Настройте порт 1 коммутатора B как доверенный (Trust), а порт 3 настройте как ненадежный (Untrust), см. рис. 181.

22.3. Функция Option 82 DHCP

22.3.1. Введение

Функция Option 82 (Relay Agent Information Entry) обеспечивает запись информацию о клиенте. Когда DHCP Snooping с поддержкой Option 82 получает сообщение с запросом от клиента DHCP, он добавляет соответствующее поле Option 82 в сообщение, а затем передает сообщение на сервер DHCP. Сервер, поддерживающий Option 82, может гибко распределять адреса в соответствии с сообщением Option 82. После того, как функция Option 82 была включена, в сообщение необходимо добавить поле Option 82. Поле Option 82 коммутаторов данной серии содержит два подпараметра: вспомогательную опцию 1 (Circuit ID, идентификатор порта запроса) и вспомогательную опцию 2 (Remote ID, идентификатор самого DHCP). Ниже представлены форматы этих двух подпараметров:

- Подпараметр 1 содержит идентификатор VLAN и номер порта, который получает сообщение с запросом от клиента DHCP.

Формат полей подпараметра 1:

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

Тип подпараметра: тип подпараметра 1-й из 1-го;
Длина: количество байтов, которые занимают идентификатор VLAN и номер порта;
VLAN ID: на устройстве с включенной функцией DHCP Snooping - идентификатор VLAN порта, который получает сообщение с запросом от клиента DHCP;
Номер порта: на устройстве с включенной функцией DHCP Snooping - номер порта, который получает сообщение с запросом от клиента DHCP.

- Содержимым подпараметра 2 является MAC-адрес устройства с функцией DHCP Snooping, которое получает сообщение с запросом от клиента DHCP или строку символов, настроенную пользователями.

Формат полей MAC адреса подпараметра 2:

Тип подпараметра (0x02)	Длина (0x06)	MAC адрес
Один байт	Один байт	6 байт

Формат полей строки символов подпараметра 2:

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

Тип подпараметра: тип подпараметра 2-й из 2-х;
Длина: количество байтов, которые занимают содержимое подпараметра 2; MAC-адрес занимает 6 байтов, а строка символов занимает 16 байт;
MAC адрес: содержимое подпараметра 2 является MAC адресом устройства с функцией DHCP Snooping, которое получает сообщение с запросом от клиента DHCP.
Строка символов: содержимое подпараметра 2 составляет 1~16 символов, заданных пользователями. (Символ указывается кодом ASCII, и каждый символ занимает один байт). Длина строки является фиксированным значением: 16 байт. Если заданная длина строки символов меньше 16 байт, необходимо заполните недостающие символы нулями.

22.3.2. DHCP Snooping с поддержкой функции Option 82

Если устройство с функцией DHCP Snooping поддерживает функцию Option 82, то когда DHCP Snooping получает сообщение с запросом DHCP, оно обрабатывает это сообщение в соответствии с тем, содержит ли сообщение Option 82 и политику клиента, а затем перенаправляет обработанное сообщение на сервер DHCP. Метод обработки показан в таблице:

Получение сообщения с запросом от клиента DHCP	**Конфигурационная политика**	**Обработка сообщения с запросом устройством с DHCP Snooping**
Сообщение с запросом содержит поле Option 82	Отбрасывание	Отбросить запрос
	Удержание	Сохранить формат сообщения без изменений и переслать
	Замещение	Заменить поле Option 82 в сообщении полем Option 82 устройства Snooping и переслать новое

		сообщение
Сообщение с запросом не содержит поле Option 82	Отбрасывание/ Сохранение/ Замещение	Добавить в сообщение поле Option 82 устройства Snooping и переслать его

Когда устройство с функцией DHCP Snooping получает ответное сообщение от сервера DHCP, и если сообщение содержит поле Option 82, поле Option 82 удаляется, ответное сообщение обрабатывается в соответствии с политикой сервера.

Получение ответного сообщения от клиента DHCP	**Конфигурационная политика**	**Обработка ответного сообщения устройством с DHCP Snooping**
Ответное сообщение содержит поле Option 82	Отбрасывание/ Сохранение	Поле Option 82 удаляется в ответном сообщении и сообщение пересылается
Ответное сообщение не содержит поле Option 82	Отбрасывание	Отбросить ответное сообщение
	Сохранение	Сохранить формат сообщения без изменений и переслать сообщение

22.3.3. Настройка через WEB-интерфейс

1. Настройка DHCP Snooping Option 82.

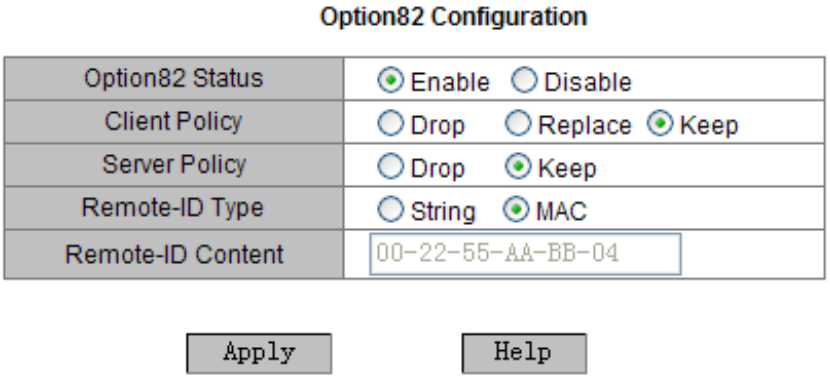


Рис. 183. Настройка функции Option 82 на устройстве с DHCP Snooping

Статус функции Option 82 (Option 82 Status)
Настраиваемые опции: Enable/Disable (Включено/Выключено)
По умолчанию: Disable (Выключено)
Описание: Включение/Выключение функции Option 82 на устройстве с DHCP Snooping.
Политика клиента (Client Policy)
Настраиваемые опции: Drop/Replace/Keep (Отбрасывание/Замещение/Сохранение)
Значение по умолчанию: Keep (Сохранение)

Описание: Настройка политики клиента. Устройство с функцией DHCP Snooping обрабатывает сообщение с запросом, отправленное от клиента в соответствии с политикой клиента.

Политика сервера (Server Policy)

Настраиваемые опции: Drop/Keep (Отбрасывание/Сохранение)

Значение по умолчанию: Keep (Сохранение)

Описание: Настройка политики сервера. Устройство с функцией DHCP Snooping обрабатывает ответное сообщение, отправленное с сервера в соответствии с политикой сервера.

Тип идентификатора DHCP (Remote-ID Type)

Настраиваемые опции: String/MAC

Значение по умолчанию: MAC

Описание: Настройка содержимого подпараметра 2. MAC означает, что содержимое подпараметра 2 является MAC адресом устройства с функцией DHCP Snooping, которое принимает сообщение с запросои от клиента. String означает, что содержимое подпараметра 2 является строкой символов, определяемой пользователем.

Содержимое идентификатора DHCP (Remote-ID Content)

Настраиваемые опции: MAC адрес/1~16 символов

Значение по умолчанию: MAC

Описание: Когда тип идентификатора DHCP настроен как MAC, содержимое Remote ID автоматически становится MAC адресом текущего устройства Snooping. Когда для типа идентификатора DHCP установлено значение String, содержимое Remote ID настраивается пользователем. Содержимое конфигурации составляет 1~16 символов (1 символ = 1 байт).

22.3.4. Поддержка функции Option 82 сервером DHCP

Если для сервера DHCP установлена поддержка функции Option82, то сервер DHCP получая сообщение с запросом, будет по-разному отвечать на них в зависимости от содержимого поля Option82 и настроек сервера.

Конфигурация сервера DHCP включает следующие переменные:

- Класс (Class): каждый сервер DHCP может настроить 32 класса. Каждый класс содержит три переменные: диапазон IP-адресов, флаг Match-always и и информацию об агенте DHCP-relay.
- Информация об агенте DHCP-relay используется для сопоставления с полем Option82. Поля считаются совпадающими, если в обеих переменных записаны одинаковые значения.
- Если установлен флаг Match-always, считается что поля «Информация об агенте DHCP-relay» и «Option82» всегда совпадают без необходимости дополнительной проверки. В противном случае поля проверяются на совпадение коммутатором.

Согласно конфигурации указанных выше переменных, сервер обрабатывает сообщение с запросом следующим образом:

<table>
<tr><th>Прием сообщения с запросом от клиента DHCP</th><th colspan="2">Политика настроек</th><th>Обработка сообщений с запросом сервером DHCP</th></tr>
<tr><td rowspan="4">Сообщение с запросом содержит поле Option 82</td><td colspan="2">Переменная "Match-always" включена</td><td>Поле Option82 добавляется в ответное сообщение и назначается IP адрес и другие параметры для клиента</td></tr>
<tr><td rowspan="2">Переменная "Match-always" выключена</td><td>Значение поля информации об агенте DHCP-relay установлено</td><td>• Значение поля информации об агенте DHCP-relay сопоставимо с полем Option82: в ответное сообщение добавляется поле Option82, клиенту назначается IP адрес и другие параметры
• Значение поля информации об агенте DHCP-relay не соответствует полю Option82: сервер не выделяет IP адрес клиенту</td></tr>
<tr><td>Значение поля информации об агенте DHCP-relay не установлено</td><td>Сервер не выделяет IP адрес клиенту</td></tr>
<tr><td colspan="2">Флаг "Match-always" включен</td><td>Ответное сообщение не содержит поля Option 82, клиенту присваивается IP адрес и другие параметры.</td></tr>
<tr><td>Сообщение с запросом не содержит поле Option 82</td><td colspan="2">Флаг "Match-always" выключен</td><td>Сервер не выделяет IP адрес клиенту</td></tr>
</table>

Если сервер DHCP не поддерживает функцию Option 82, то когда сервер DHCP получает сообщение, содержащее поле Option 82, в ответном сообщении не содержится поля Option 82 и сервер может назначить клиенту IP адрес и другие параметры. В таком случае сервер обрабатывает сообщение с запросом следующим образом:

Прием сообщения с запросом от клиента DHCP	**Обработка сообщений с запросом сервером DHCP**
Сообщение с запросом содержит поле Option 82	Сервер не выделяет IP адрес и другие параметры клиенту.

Сообщение с запросом не содержит поле Option 82	Ответное сообщение не содержит поля Option 82 и сервер выделяет IP адрес и другой параметр клиенту.

23. Расшифровка аббревиатур

Аббревиатура	Полное наименование	Наименование на русском языке
AAA	Authentication, Authorization, Accounting	Аутентификация, Авторизация, Учетная запись
ARP	Address Resolution Protocol	Протокол определения адреса
BOOTP	Bootstrap Protocol	Протокол автоматического получения клиентом IP адреса
BPDU	Bridge Protocol Data Unit	Протокол управления сетевыми мостами
CLI	Command Line Interface	Интерфейс командной строки
CRC	Cyclic Redundancy Check	Циклический избыточный код (алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных)
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки узла
DSCP	Differentiated Services Code Point	Точка кода дифференцированных услуг (элемент архитектуры компьютерных сетей, описывающий простой масштабируемый механизм классификации, управления трафиком
FTP	File Transfer Protocol	Протокол передачи данных
GARP	Generic Attribute Registration Protocol	Протокол регистрации основных атрибутов
GMRP	GARP Multicast Registration Protocol	Пртокол GARP для регистрации многоадресных групп
GVRP	GARP VLAN Registration Protocol	Пртокол GARP для регистрации VLAN
HTTP	Hyper Text Transport Protocol	Протокол передачи гипертекста (протокол прикладного уровня передачи данных)
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
LLDP	Link Layer Discovery Protocol	Протокол обнаружения уровня канала

MAC	Media Access Control	Управление доступом к среде (обеспечивает адресацию и механизмы управления доступом к
MIB	Management Information Base	База управляющей информации
NMS	Network Management Station	Станция управления сетью
OID	Object Identifier	Идентификатор объекта
QoS	Quality of Service	Качество обслуживания (технология предоставления различным классам трафика различных приоритетов в обслуживании)
RMON	Remote Network Monitoring	Дистанционный мониторинг сети (расширение SNMP, разработанное IETF)
RSTP	Rapid Spanning Tree Protocol	Быстрый протокол разворачивающегося дерева (версия протокола STP с ускоренной реконфигурацией дерева)
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)
SP	Strict Priority	Строгий приоритет (гарантирует, что чувствительные ко времени приложения передаются всегда)