SYMANITRON

Инновационные
промышленные сети

Промышленные коммутаторы серии SEWM2GX28P/SEWM3GX28P

Руководство по настройке

WEB-интерфейс

Оглавление

Введение

В настоящем руководстве описываются методы доступа и возможности программного обеспечения промышленных коммутаторов серии SEWM2GX28P/SEWM3GX28P. 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 • Возможности программного обеспечения
2. Способы подключения к устройству	• Варианты просмотра и отображения • Подключение через консольный порт • Подключение с использованием Telnet • Подключение через Web-интерфейс
3. Пользователи	• Управление пользователями • Тип аутентификации
4. Система	• Основная информация • Управление конфигурацией • Управление часами • Обновление ПО (HTTP, FTP, TFTP) • Активная версия прошивки • Обновление языка • Перезагрузка
5. Службы	• SSL • SNMP v1/v2c/v3 • SSH • TACACS+ • RADIUS • DNS • RMON
6. Тревожная сигнализация	•
7. Управление функциями	• Конфигурация порта • VLAN • Настройка IP • Агрегация портов • Резервирование • Sy2-Ring • Настройка ARP • Настройка ACL

	• Настройка MAC-адреса • POE • IGMP snooping • Настройка DHCP • Настройка IEEE 802.1X • GMRP • PIM# • NAT# • IGMP# • Настройка маршрутизации# • GMRP • Статический маршрут • Настройка QoS • VRRP#
8. Диагностика	• Системный журнал • Зеркалирование трафика • LLDP • Trace Route • Ping • IPSG • DDM

Отмеченные функции не поддерживаются коммутаторами второго уровня SEWM2GX28P.

Условные обозначения

1. Условные обозначения в тексте

Формат	Описание
< >	Скобки < > обозначают «кнопки». Например, нажмите кнопку <Set>
[ ]	Скобки [ ] обозначают имя окна или имя меню. Например, нажмите пункт меню [File]
→	Мультиуровневое меню разделяется посредством знака «→». Например, [Start] → [All Programs] → [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

2. Условные обозначения CLI

Формат	Описание
Bold	Означает команды и ключевые слова. Например, **show version** будет показываться с использованием шрифта **Bold**
Italic	Указывает на значение параметра, которое необходимо ввести. Например, для команды **show vlan** *vlan id* вместо *vlan id* следует вводить актуальный идентификатор VLAN

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

Коммутаторы серии SEWM2GX28P/SEWM3GX28P могут использоваться различных отраслях промышленности, таких как энергетика, железнодорожный транспорт, горнодобывающие предприятия и т.д. Они могут эффективно работать в суровых условиях. Коммутаторы поддерживают протоколы резервирования, такие как MSTP/RSTP, Sy2-Ring и DRP, обеспечивая надежную работу системы.

1.2 Функциональные возможности ПО

Коммутаторы данной серии предоставляют множество программных функций, удовлетворяющих различным требованиям клиентов:

- Протоколы резервирования: DRP, STP/RSTP, VRRP и MSTP;
- Протоколы многоадресной передачи: IGMP Snooping, GMRP, PIM-SM, PIM-DM;
- Атрибуты коммутации: VLAN, PVLAN, GVRP, QoS и ARP;
- Управление пропускной способностью: статическая агрегация портов, LACP, ограничение скорости портов и подавление штормов;
- Безопасность: управление пользователями, управление доступом, SSH, SSL, TACACS+, RADIUS, IEEE 802.1X, ACL, IP Source Guard и изоляция портов;
- Протоколы синхронизации: SNTP, NTP;
- Управление устройством: обновление программного обеспечения, загрузка/выгрузка файла конфигурации, запись и выгрузка журнала;
- Диагностика устройства: зеркало порта, LLDP;
- Функция сигнализации: сигнализация питания, сигнализация порта, сигнализация звонка и сигнализация конфликта IP/MAC-адресов;
- Сетевое управление: CLI, Telnet, Web. DHCP и мониторинг сети при помощи SNMP v1/v2c/v3;
- Сетевые функции: NAT, DNS.

2. Подключение к устройству

Устройство можно настраивать одним из нижеперечисленных способов:

- через консольный порт;
- посредством Telnet/SSH;
- с использованием WEB-интерфейса.

2.1 Варианты просмотра и отображения

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

Таблица 1 – Режимы настройки

Подсказка	Тип отображения	Функция	Команда
Switch#	Привилегированный режим	• Просмотр недавно использованных команд • Просмотр версии программного обеспечения • Просмотр информации об ответе на операцию ping • Загрузка/выгрузка файла конфигурации • Восстановление конфигурации по умолчанию • Перезапуск коммутатора • Сохранение текущей конфигурации • Отображение текущей конфигурации. • Обновление программного обеспечения	Введите «**configure terminal**» для переключения из привилегированного режима в режим настройки Введите «**exit**» для возврата в основной режим
Switch (config)#	Режим настройки	Настройка всех функциональных возможностей коммутатора	Введите «**exit**» или «**end**» для возврата в привилегированный режим

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

2.2 Подключение через консольный порт

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

1. Подключите кабель DB9 к ПК и консольному порту устройства.

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

Рисунок 1 – Запуск Hyper Terminal

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

Рисунок 2 – Создание нового подключения

4. Выберите COM-порт для подключения.

Рисунок 3 – Выбор COM порта для подключения

Чтобы убедиться, что консольный порт выбран верно, проверьте его статус в диспетчере устройств Windows: [My Computer] → [Property] → [Hardware] → [Device Manager] → [Port].

---

5. Настройте параметры COM порта. Скорость (Bits per second): 115200, биты данных (Data bits): 8, четность (Parity): None, стоповые биты (Stop bits): 1, управление потоком (Flow control): None, как показано на рисунке 4.

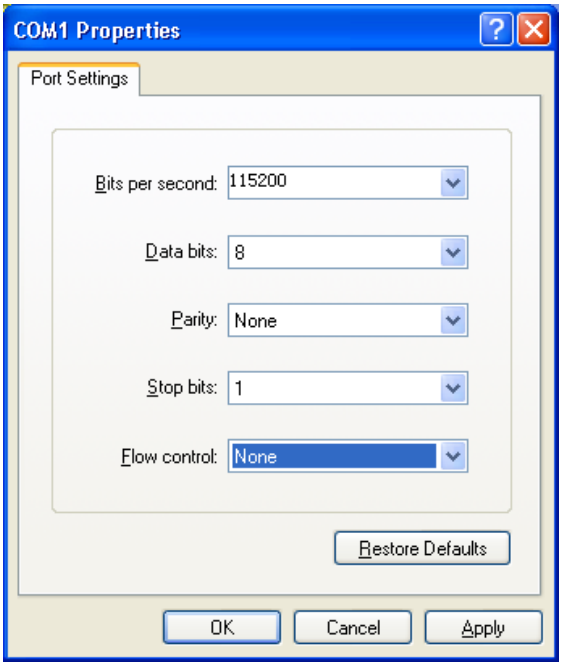


Рисунок 4 – Настройка параметров COM порта

6. Нажмите <OK>, чтобы войти в CLI коммутатора. Введите пользователя по умолчанию «admin» и пароль «123» для входа в привилегированный режим. Вы также можете ввести имена других созданных пользователей и их пароли, как показано на рисунке 5.

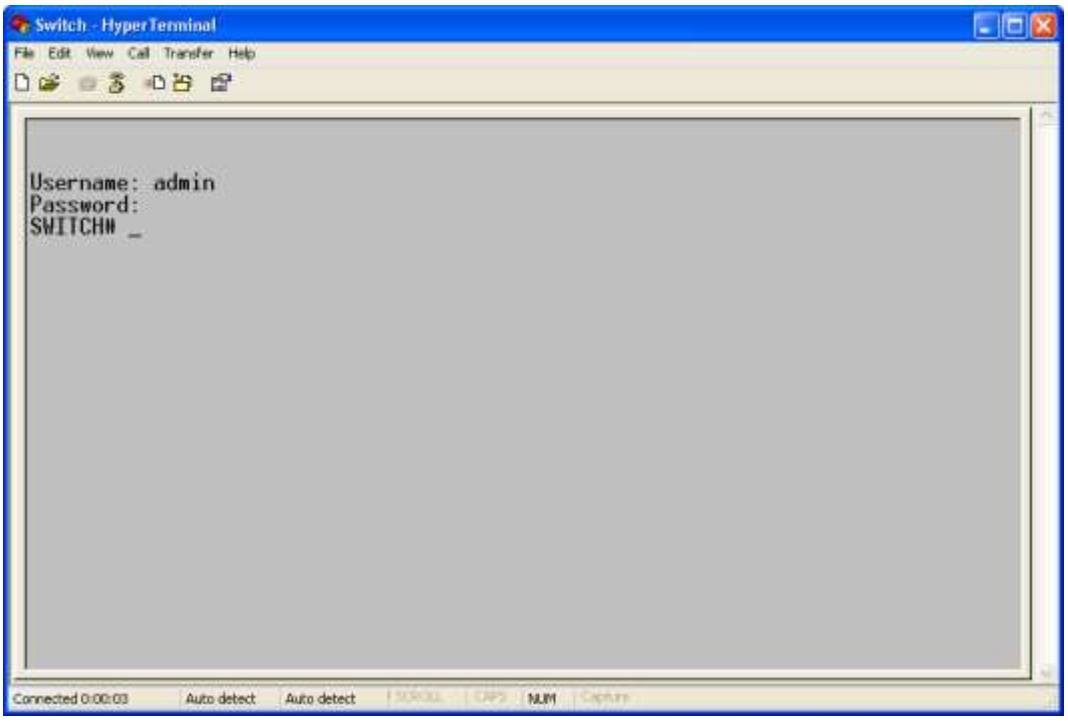


Рисунок 5 – Экран CLI

2.3 Подключение при помощи Telnet

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

1. Введите «telnet *IP-адрес*» в диалоговом окне <Run>, как показано на следующем рисунке:

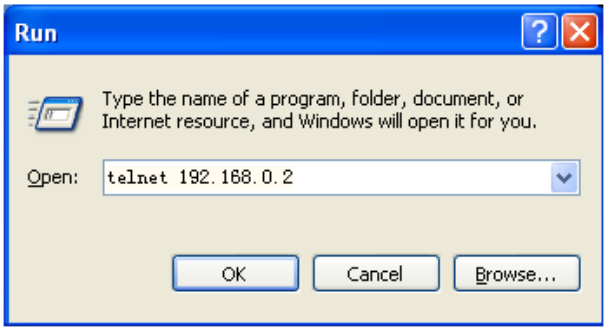


Рисунок 6 – Доступ через Telnet

Для дополнительной информации о подтверждении IP-адреса коммутатора обратитесь к разделу 7.3 настоящего руководства.

2. В интерфейсе Telnet введите имя пользователя «admin» и пароль «123». Нажмите <Enter> для входа.

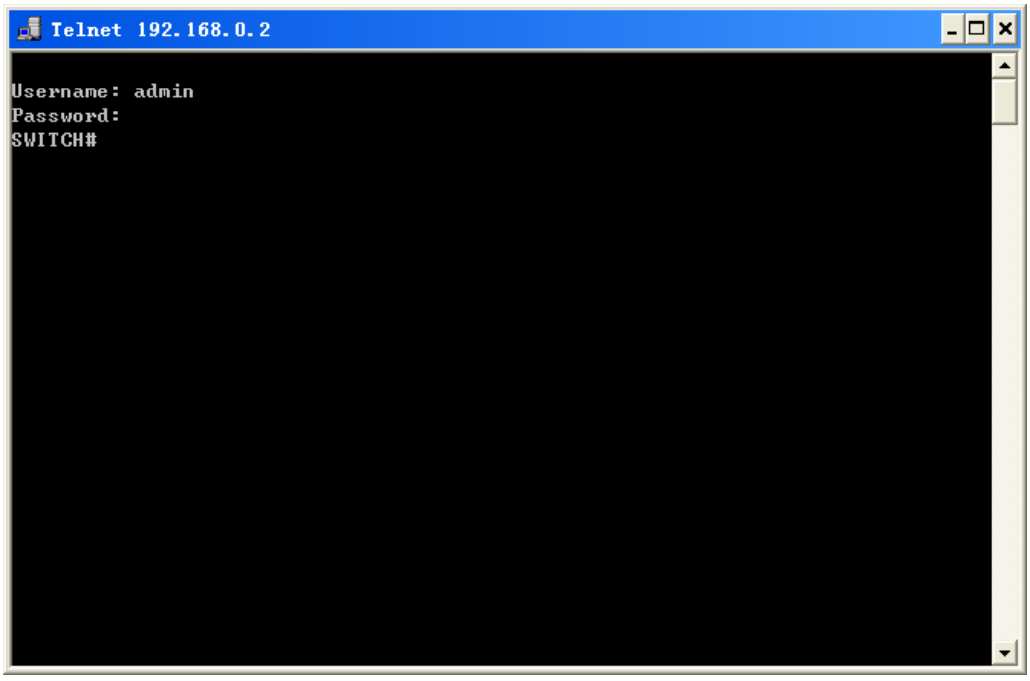


Рисунок 7 – Интерфейс терминала Telnet

2.4 Доступ через WEB-интерфейс

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

1. Введите IP-адрес в адресную строку браузера. Отобразится интерфейс входа в систему. Введите имя пользователя по умолчанию «admin», пароль «123» и подтверждение. Нажмите <Sign in>.

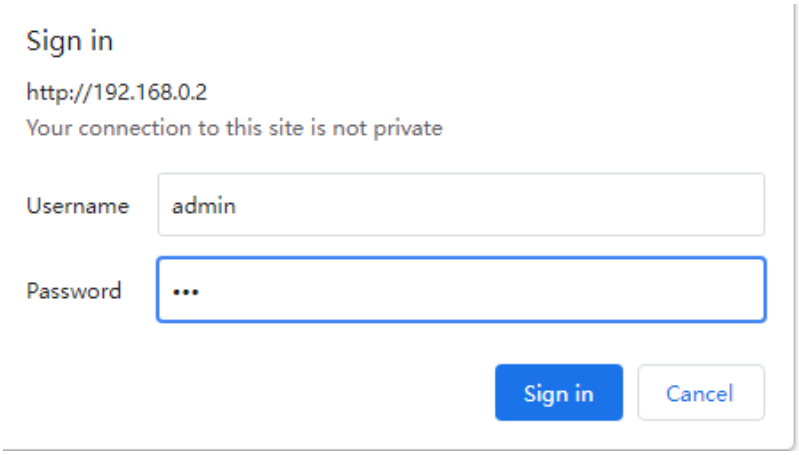


Рисунок 8 – Вход через веб-интерфейс

Для дополнительной информации о подтверждении IP-адреса коммутатора обратитесь к разделу 7.3 настоящего руководства.

2. После успешного входа в систему в левой части интерфейса появится дерево навигации, как показано на следующем рисунке.

Рисунок 9 – Страница веб-интерфейса

Вы можете развернуть или свернуть дерево навигации, нажимая значки «+» и «-». Нажмите <Home>, чтобы вернуться на домашнюю страницу, или кнопку со стрелкой в правом верхнем углу, чтобы выйти из веб-интерфейса.

3. Пользователи

3.1 Управление пользователями

3.1.1 Введение

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

3.1.2 Настройка с помощью WEB-интерфейса

1. Создание нового пользователя показано на рисунке 10.

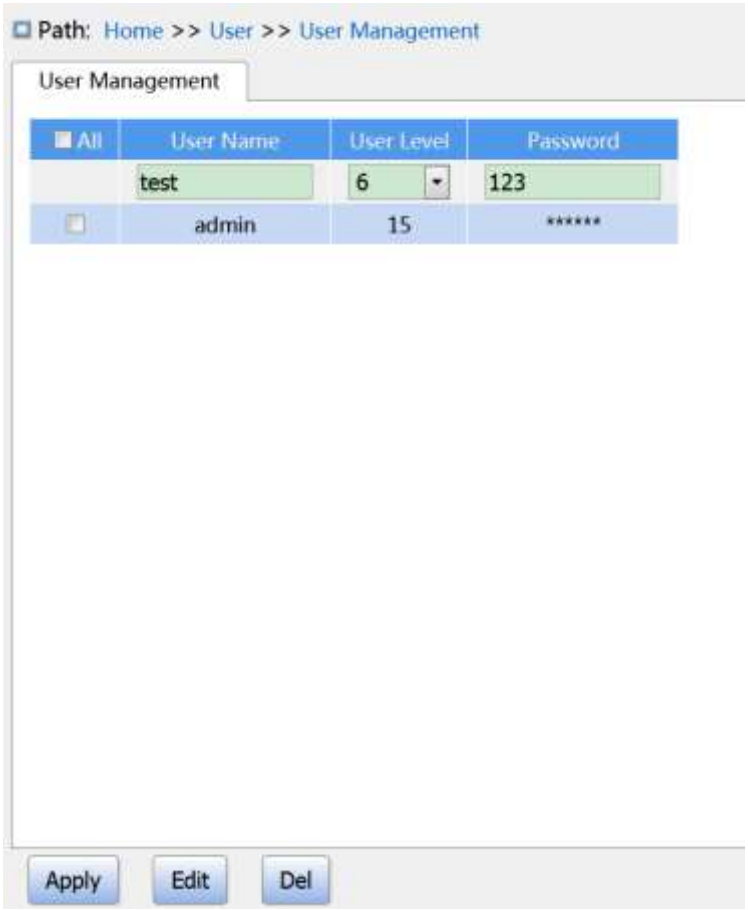


Рисунок 10 – Создание нового пользователя

Можно создать до 20 пользователей, присвоив им различные уровни.

User name

Диапазон: 1–31 символ.

Функция: создание имени пользователя.

User level

Диапазон: 0–15.

Функция: настройка уровня разрешений пользователя. Пользователи с разными уровнями разрешений имеют разные права доступа.

Password (пароль)

Диапазон: 0–31 символ.

Функция: создание пароля для входа пользователя.

2. Изменение настроек пользователя показано на рисунке 11.

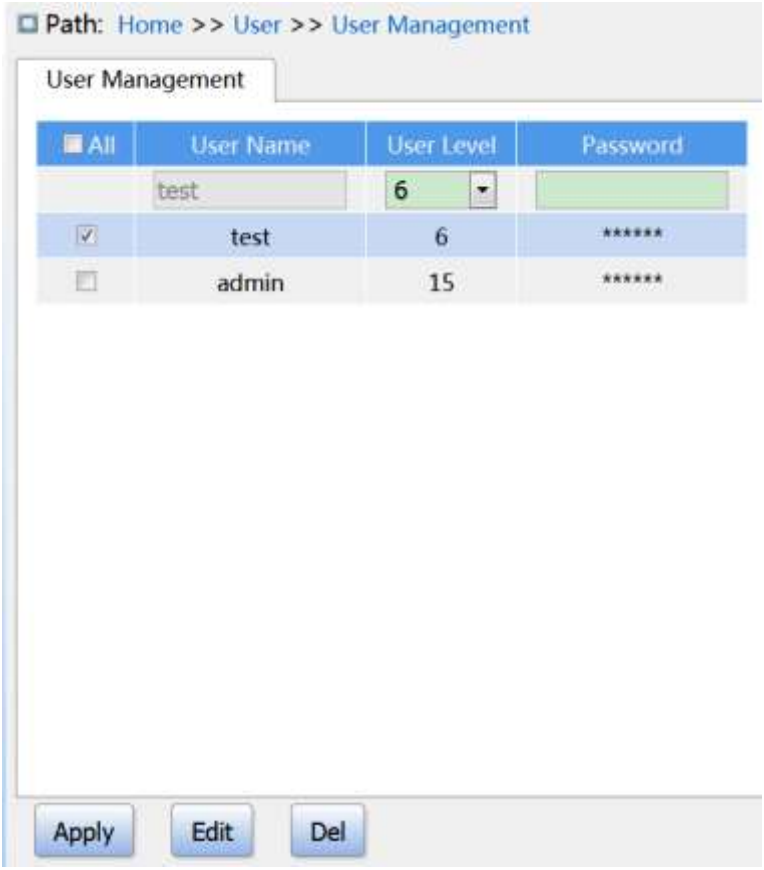


Рисунок 11 – Изменение настроек пользователя

Отметьте пользователя, настройки которого нужно отредактировать, нажмите кнопку <Edit>, чтобы изменить пароль и уровни разрешений.

Нажмите кнопку <Del>, чтобы удалить текущего пользователя.

Пользователь по умолчанию **admin** не может быть удален.

3. Настройка уровня привилегий групп показана на рисунке 12.

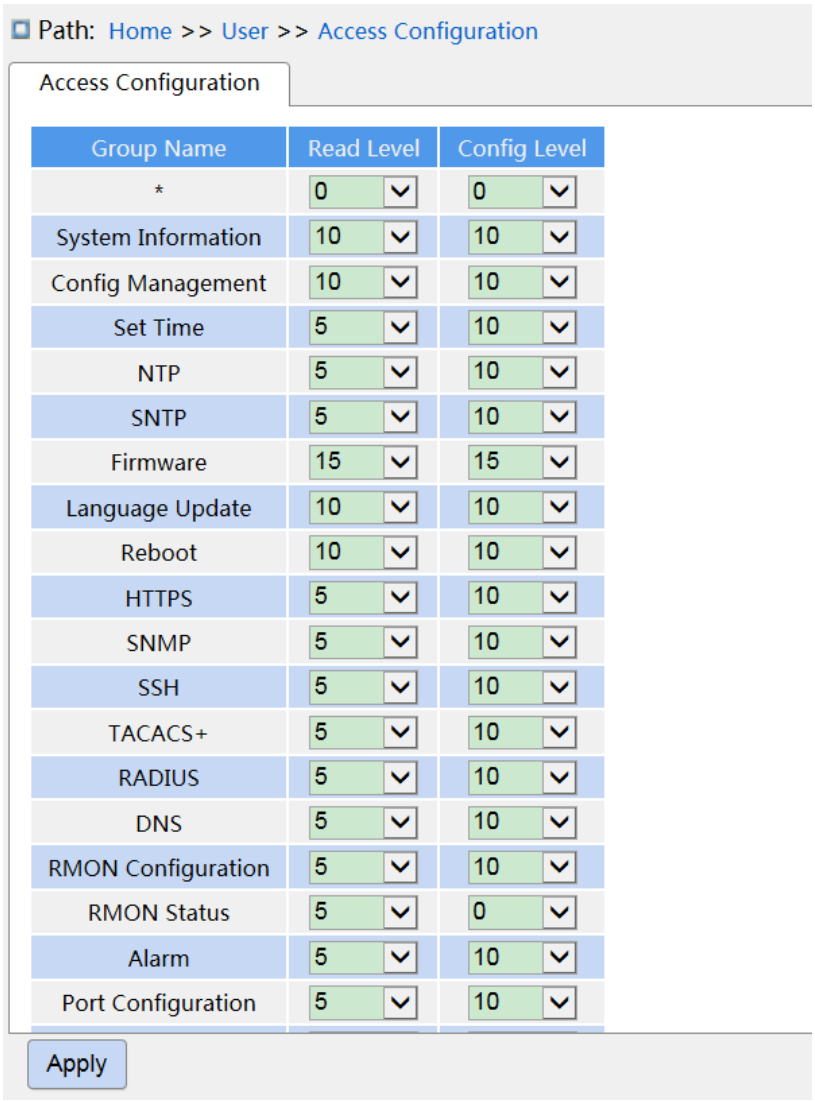


Рисунок 12 – Настройка групповых привилегий

Group Name

Варианты настройки: все функциональные группы.

Функция: выбор функциональной группы коммутатора для настройки.

Read Level

Варианты настройки: 0–15.

По умолчанию: 5.

Функция: настройка уровня, на котором пользователь может просматривать текущую функциональную группу. Разные уровни групп имеют разные требования к уровню разрешений для просмотра пользователями.

Config Level (уровень настроек)

Варианты настройки: 0–15.

По умолчанию: 10.

Функция: настройка уровня, на котором пользователь может управлять текущей функциональной группой. Различные уровни групп имеют разные требования к уровню разрешений для операций пользователя.

Когда уровень привилегий пользователя такой же или выше, чем уровень привилегий группы, пользователь может получить доступ к группе или настроить ее. Право доступа или настройки зависит от уровня привилегий пользователя.

3.2 Тип аутентификации

Настройка режима доступа к коммутатору, режим и порядок аутентификации показаны на рисунке 13.

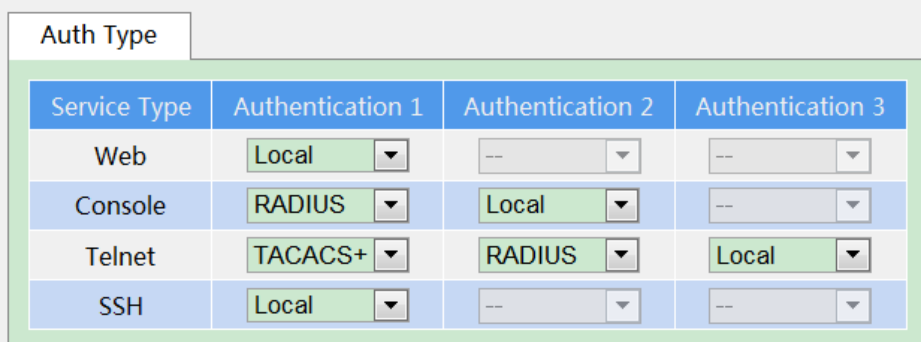


Рисунок 13 – Настройка аутентификации

Service Type

Варианты настройки: Web/Console/Telnet/SSH.

Функция: выбор режима доступа к коммутатору.

Authentication 1/Authentication 2/Authentication 3

Варианты настройки: --/local/tacacs/radius.

По умолчанию: local.

Функция: методы слева направо: Authentication 1, Authentication 2 и Authentication 3. Выбор порядка аутентификации. Сначала выполняется метод аутентификации 1. Если

аутентификация не удалась, выполняется метод аутентификации 2. Если оба метода терпят неудачу, выполняется метод аутентификации 3.

Описание: -- означает, что аутентификация отключена и вход в систему невозможен. **local** означает использование для выполнения аутентификации имени пользователя и пароля, установленных локально. **tacacs** означает использование имени пользователя и пароля, установленных на сервере TACACS+. **radius** означает использование имени пользователя и пароля, установленных на сервере RADIUS.

Если для аутентификации 1 и аутентификации 2 выбрано значение tacacs/radius, рекомендуется настроить аутентификацию 3 как local. Это позволит управляющему клиенту подключаться к коммутатору в качестве локального пользователя, если ни один из настроенных удаленных серверов аутентификации не работает.

Если для аутентификации 1 и аутентификации 2 выбрано значение tacacs/radius, рекомендуется настроить аутентификацию 3 как local. Это позволит управляющему клиенту подключаться к коммутатору в качестве локального пользователя, если ни один из настроенных удаленных серверов аутентификации не работает.

---

4. Система

4.1 Основная информация

Информация о системе включает тип и имя устройства, MAC-адрес, версию аппаратной платформы, прошивки и программного обеспечения, дату компиляции, процент использования процессора и оперативной памяти, время работы системы, сведения о местонахождении и контактные данные, как показано на рисунке 14.

Рисунок 14 – Основная информация

4.2 Управление конфигурацией

1. Сохранение информации о текущей конфигурации показано на рисунке 15.

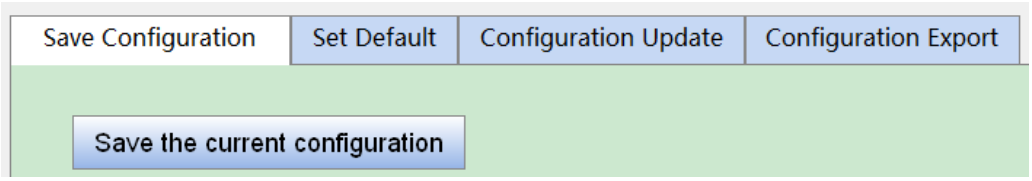


Рисунок 15 – Сохранение текущей конфигурации

2. Восстановление заводских настроек по умолчанию показано на рисунке 16.

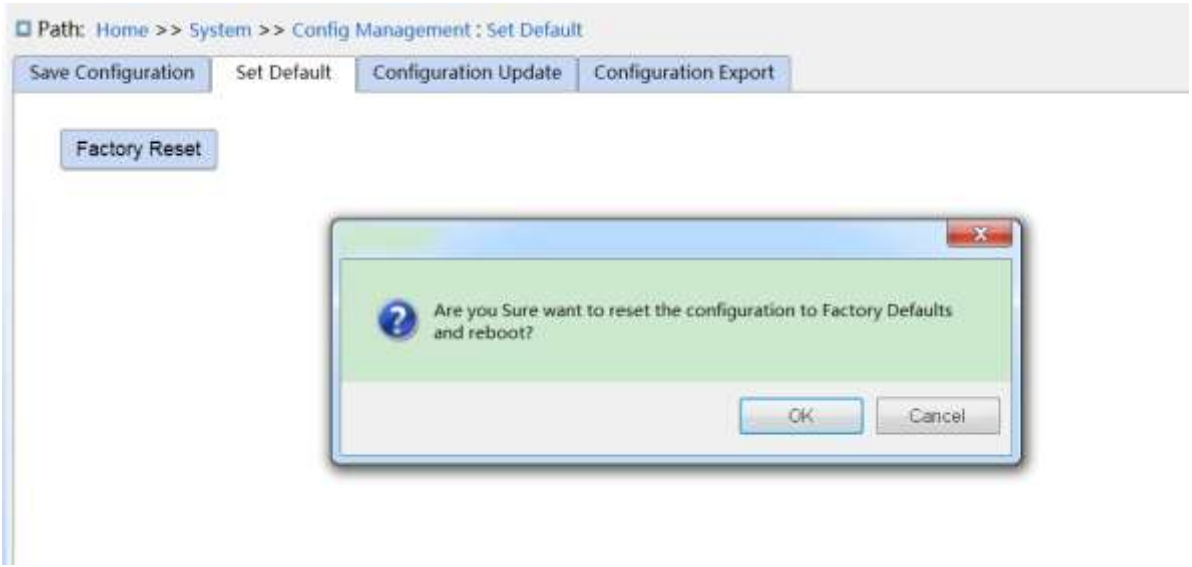


Рисунок 16 – Восстановление заводской конфигурации

3. Экспорт конфигурации. Сохранение файла конфигурации с коммутатора локально или на сервер показано на рисунках 17–19.

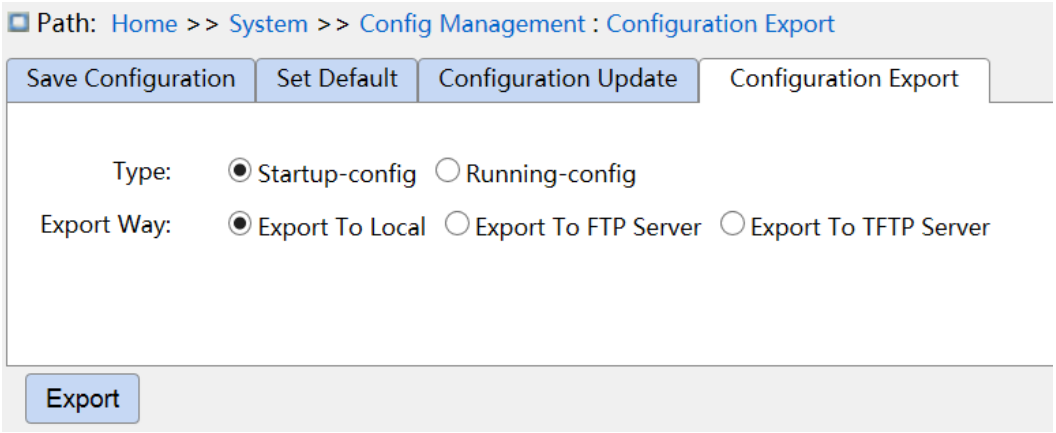


Рисунок 17 – Экспорт файла конфигурации – HTTP

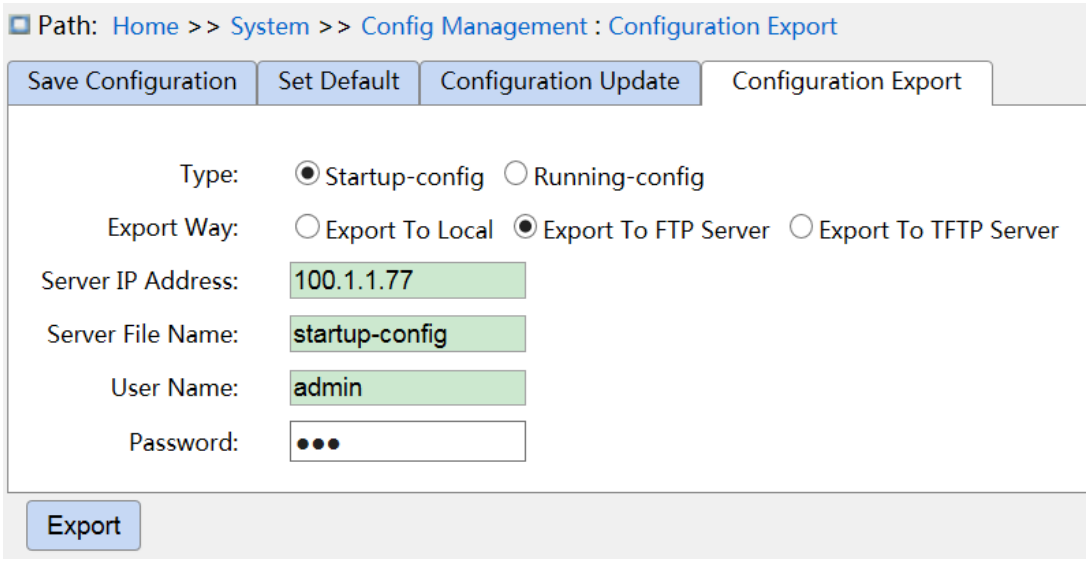


Рисунок 18 – Экспорт файла конфигурации – FTP

Server IP address

Формат: A.B.C.D.

Описание: настройка IP-адреса FTP-сервера.

Server file name

Диапазон: 1–63 символа

Описание: настройка имени файла конфигурации, хранящегося на FTP-сервере.

{User name, Password}

Диапазон: {1–63 символа, 1–63 символа}

Описание: ввод имени пользователя и пароля, созданных на FTP-сервере.

- Для передачи файла по FTP необходимо настроить логин и пароль FTP, а также IP-адрес FTP-сервера.
- В процессе передачи файла не выключайте FTP-сервер.

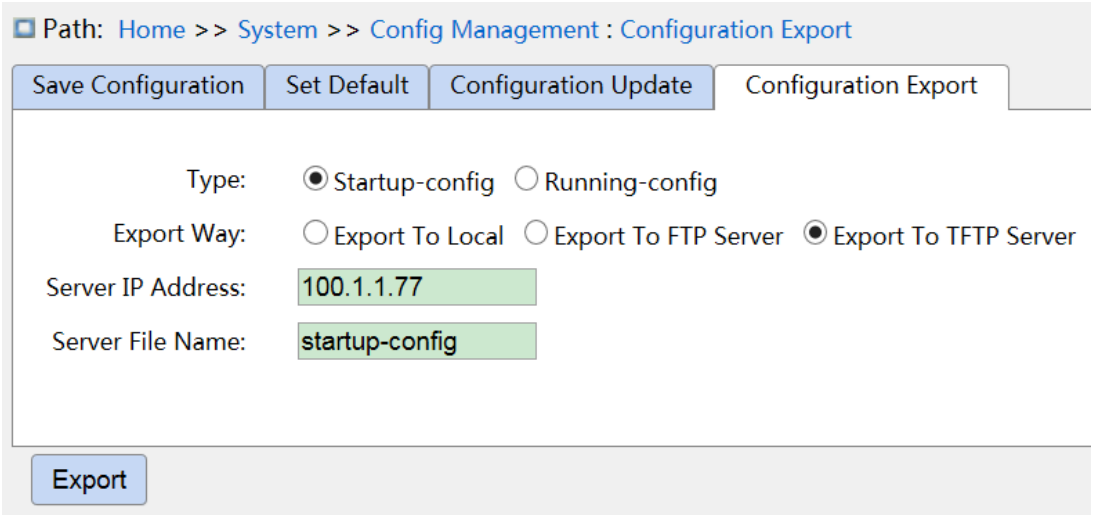


Рисунок 19 – Экспорт файла конфигурации – TFTP

Вы можете сохранить файл локально или на сервере. «Running-config» – это текущий рабочий файл конфигурации коммутатора, а «Startup-config» – это файл конфигурации, который используется при запуске. Он содержит начальные или «стартовые» настройки, которые загружаются при каждом включении коммутатора. Выберите файл и нажмите <Export> для сохранения файла в выбранной директории.

4. Обновление конфигурации. Загрузите файл конфигурации из локального каталога или с сервера, чтобы использовать его в качестве нового стартового файла коммутатора, как показано на рисунках 20–22.

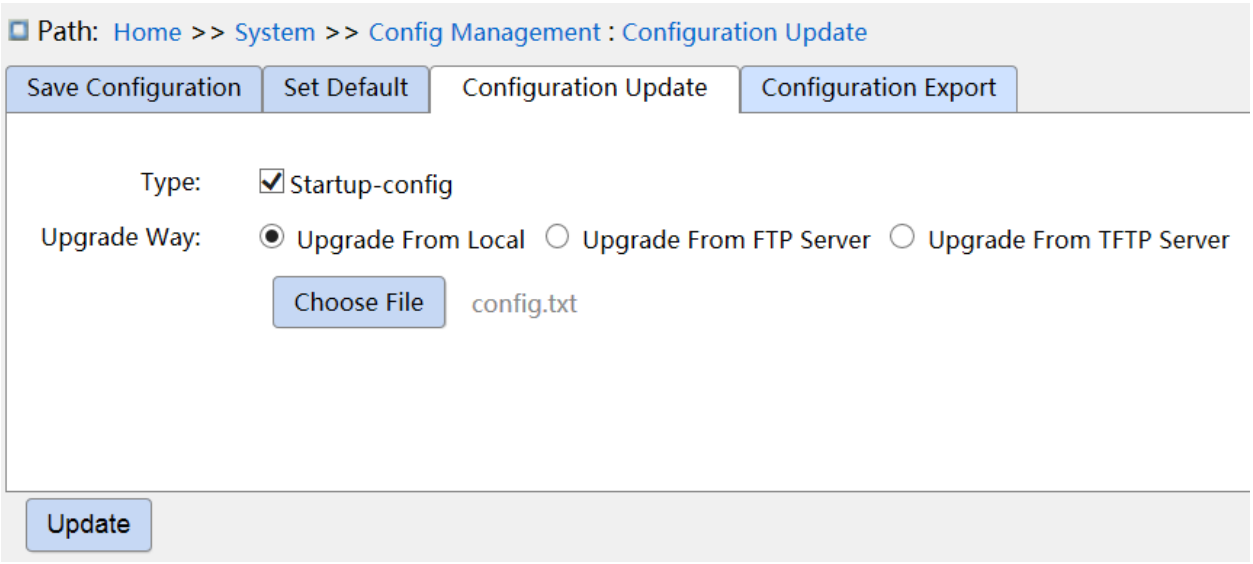


Рисунок 20 – Загрузка файла конфигурации – HTTP

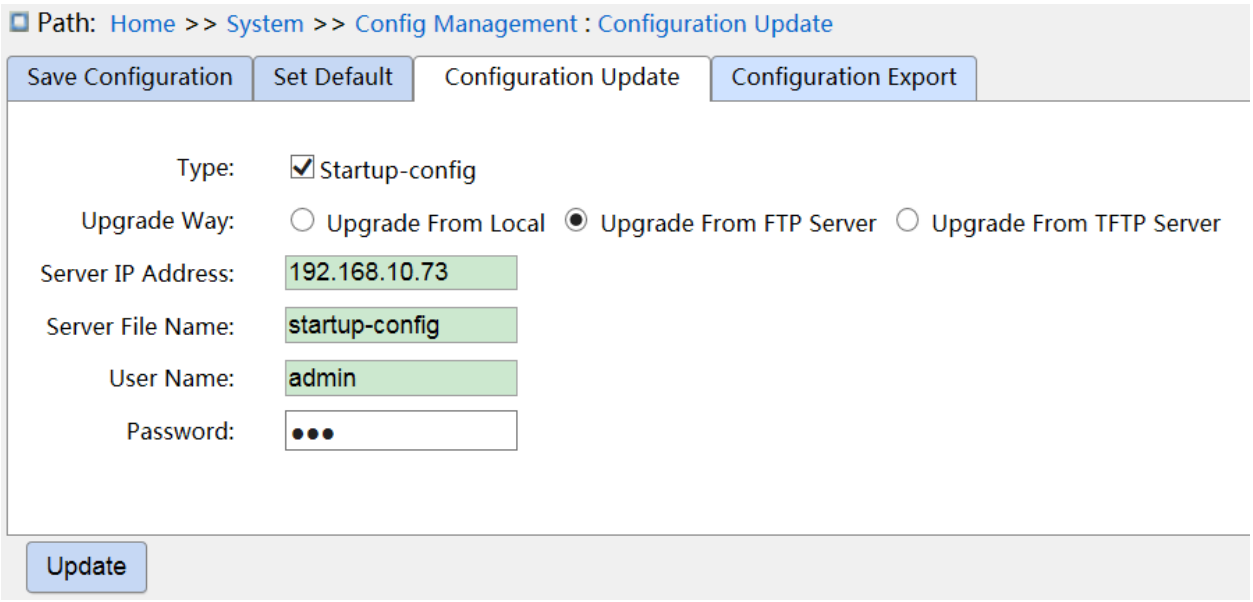


Рисунок 21 – Загрузка файла конфигурации – FTP

Server IP address

Формат: A.B.C.D.

Описание: настройка IP-адреса FTP-сервера.

Server file name

Диапазон: 1–63 символа.

Описание: имя файла обновления прошивки, хранящегося на FTP-сервере.

{User name, Password}

Диапазон: {1–63 символа, 1–63 символа}.

Описание: ввод имени пользователя и пароля, созданных на FTP-сервере.

- Для передачи файла по FTP необходимо настроить логин и пароль FTP, а также IP-адрес FTP-сервера.
- В процессе передачи файла не выключайте FTP-сервер.

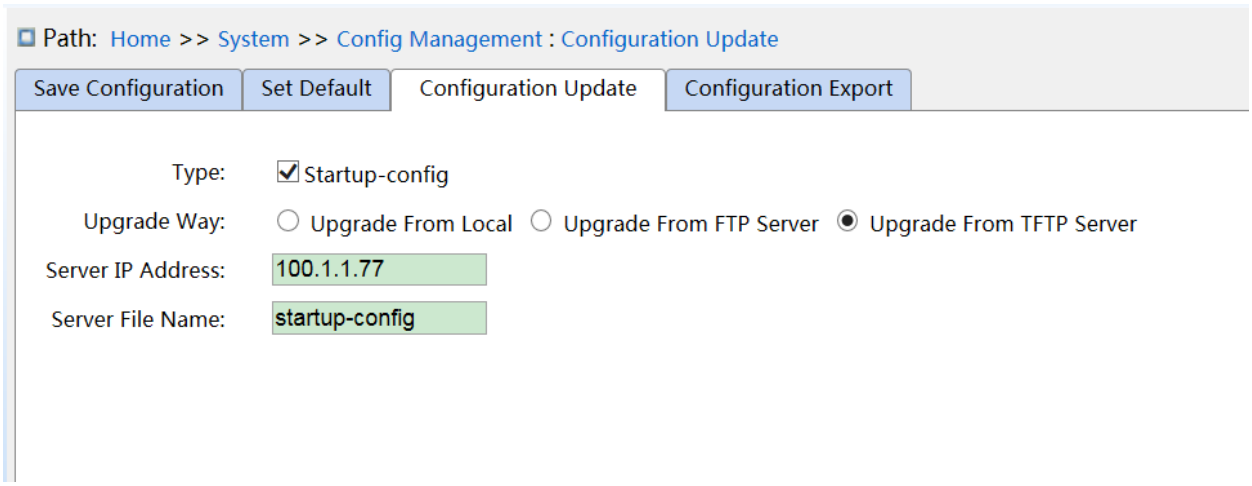


Рисунок 22 – Загрузка файла конфигурации – TFTP

Вы можете загрузить файл конфигурации из локальной папки или с сервера на коммутатор в качестве нового файла запуска. Новый файл заменит исходный файл startup-config. Нажмите <Update>, чтобы загрузить файл конфигурации на коммутатор и обновить прошивку.

4.3 Управление часами

4.3.1 DST

Чтобы в полной мере использовать дневной свет и экономить энергию летом, вы можете выполнить настройку DST (DST: летнее время). Конфигурация летнего времени может быть повторяющейся (recurring) и неповторяющейся (non-recurring).

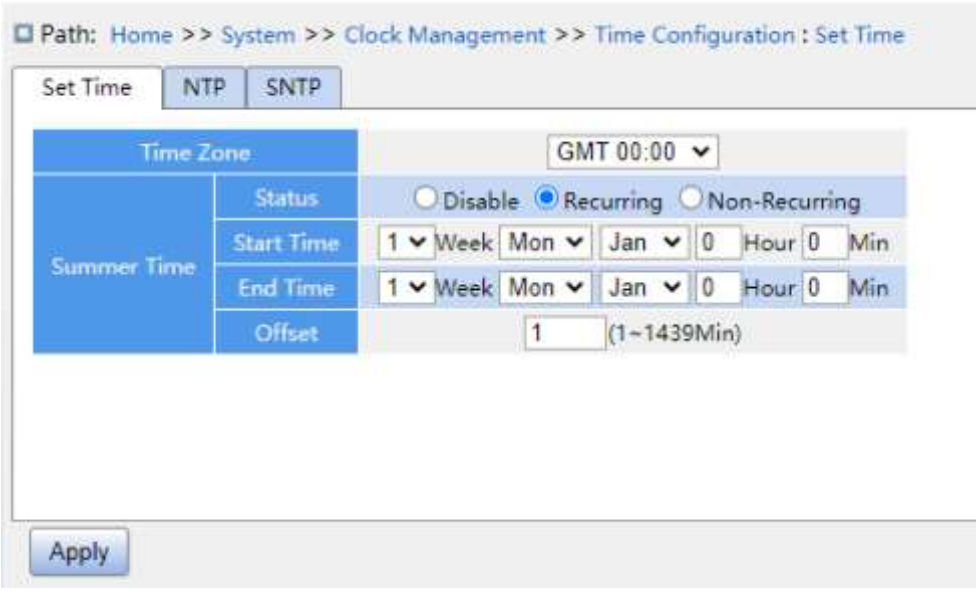


Рисунок 23 – Повторяющаяся конфигурация

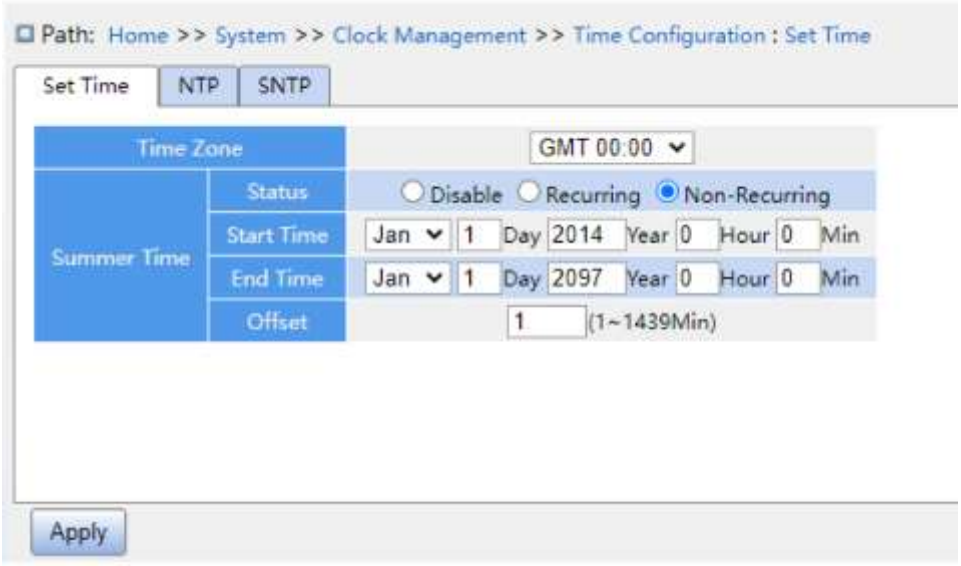


Рисунок 24 – Неповторяющаяся конфигурация

Time zone

Функция: выбор часового пояса.

DST status

Варианты настройки: disable/recurring/non-recurring.

Функция: включение функции DST и настройка периодичности.

Start Time/End Time

Функция: после включения DST установите временной диапазон для летнего времени. Неповторяющийся режим позволяет настроить год, месяц, день, час и минуту, назначив рабочий диапазон летнего времени, как показано на рисунке 23. Можно выбрать временной интервал между 00:00 1 января 2014 года и 23:59 1 июля 2097 года. Повторяющийся режим позволяет настроить месяц, неделю, дату, час и минуту, чтобы назначить рабочий диапазон летнего времени в пределах года, как показано на рисунке 22. Таким образом, переход осуществляется ежегодно, пока активна настройка.

Offset

Диапазон: 1–1439 мин.

По умолчанию: 1 мин.

Функция: настройка смещения времени, то есть, на сколько следует переводить часы.

- Время начала и время окончания должны отличаться.
- Время начала – это зимнее время, время окончания – летнее.

Пример: если летнее время продолжается с 10:00:00 1 апреля до 9:00:00 1 октября, то смещение DST составляет 60 минут.

Период DST начинается в момент действия зимнего времени с 10:00:00 1 апреля и сразу переходит на 11:00:00 летнего времени. Когда летнее время заканчивается в 9:00:00 1 октября, оно возвращается к 8:00:00 зимнего времени.

4.3.2 NTP

NTP (протокол сетевого времени) используется для синхронизации времени между выделенным сервером времени и клиентом. NTP может синхронизировать часы всех устройств с эталонными сетевыми часами, и системное время устройств в сети будет одинаковым. Таким образом коммутатор может предоставлять различные услуги на основе одного и того же времени. Локальная система, работающая с NTP, может получать синхронизацию от других источников времени или синхронизировать другие часы, сама будучи источником.

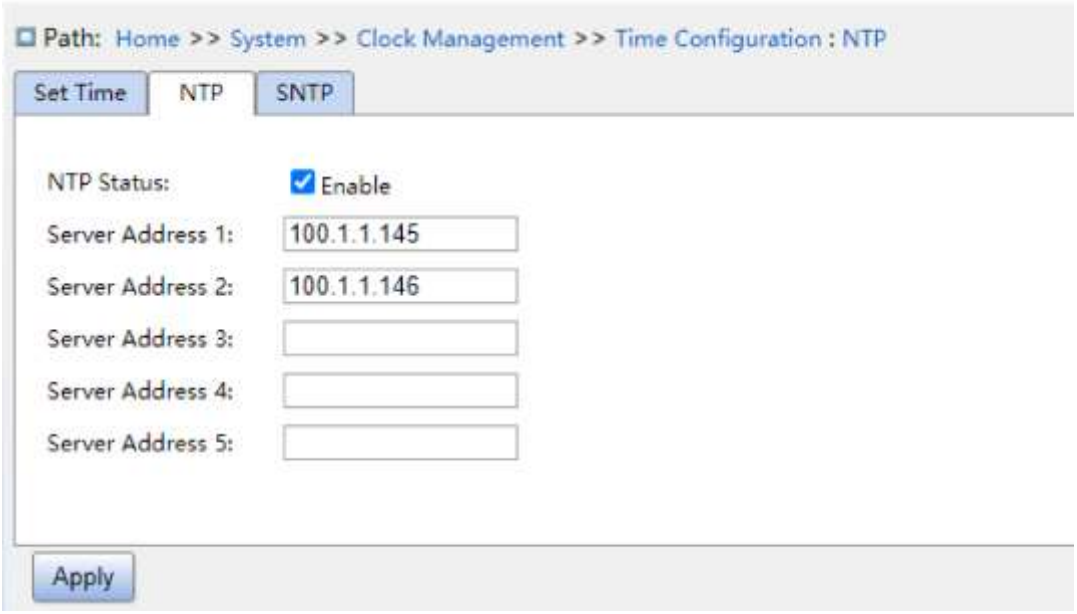


Рисунок 25 – Настройка NTP

NTP status

Варианты настройки: enable/disable.

По умолчанию: disable.

Функция: включение/отключение ли глобальной службы NTP.

- Протоколы NTP и SNTP являются взаимоисключающими. Поскольку NTP и SNTP используют один и тот же порт UDP, оба они не могут быть включены одновременно.

- Службы NTP можно настроить и сохранить как при включенном, так и при отключенном протоколе.

Server address 1 / server address 2 / server address 3 / server address 4 / server address 5

Формат: A.B.C.D

Функция: настройте IP-адрес NTP-сервера, и клиент будет калибровать время в соответствии с его сообщениями.

4.3.3 SNTP

Протокол SNTP (простой протокол сетевого времени) синхронизирует время путем запроса и ответа между сервером и клиентом. Коммутатор как клиент калибрует время в соответствии с сообщением сервера.

- Когда протокол SNTP включается на коммутаторе, SNTP-сервер должен быть активен.
- Информация о времени в протоколе SNTP представляет собой стандартную информацию о времени нулевого часового пояса.

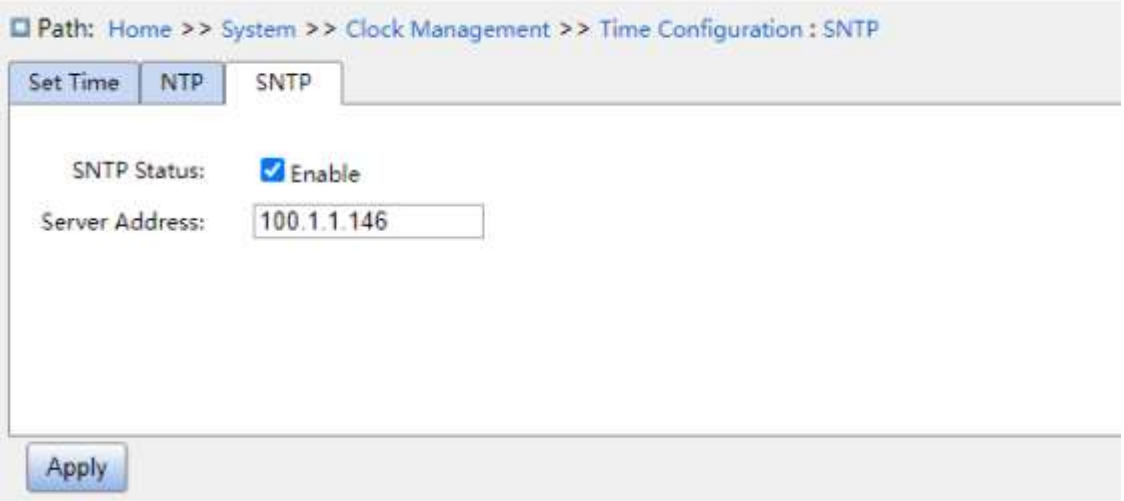


Рисунок 26 – Настройка SNTP

SNTP status

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение SNTP.

Server address

Формат: A.B.C.D

Функция: настройте IP-адрес SNTP-сервера, и клиент будет калибровать время в соответствии с его сообщениями.

4. Проверьте, синхронизировано ли время коммутатора с временем сервера.

Откройте страницу [System] → [Basic Information], чтобы просмотреть информацию о системном времени, как показано ниже.

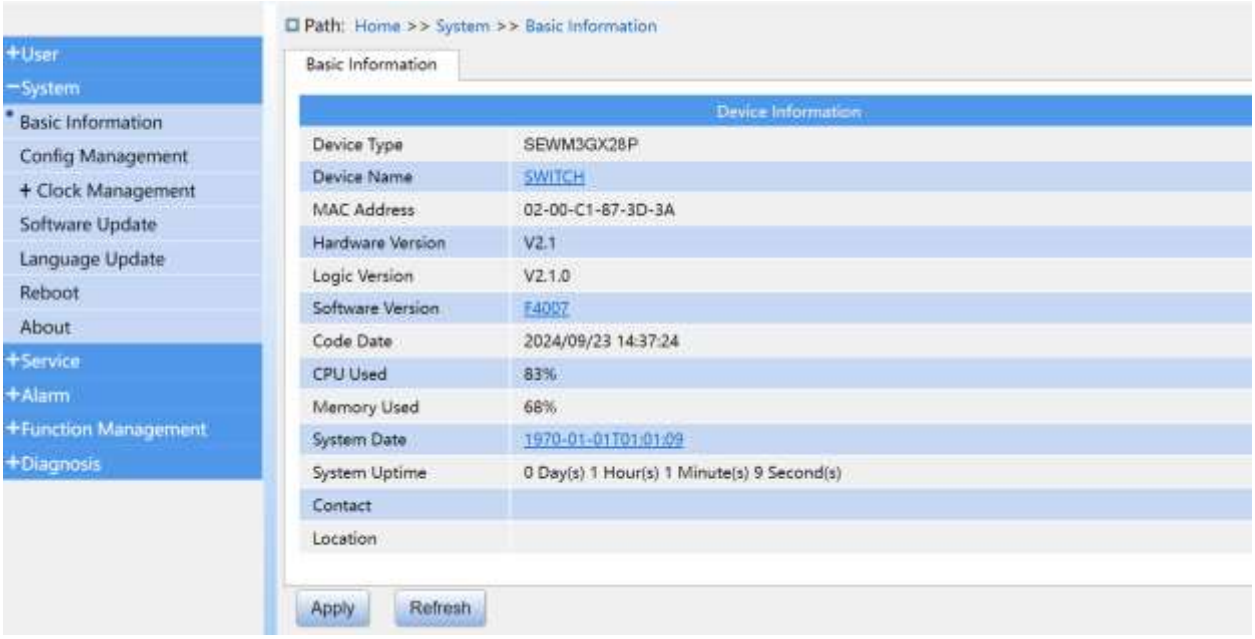


Рисунок 27 – Просмотр информации о времени

4.3.4 PTP

1. PTP – это протокол синхронизации точного времени по всей компьютерной сети. В локальной сети он достигает точности часов в диапазоне субмикросекунд, что делает его пригодным для систем измерения и управления. Ниже показана конфигурация часов PTP:

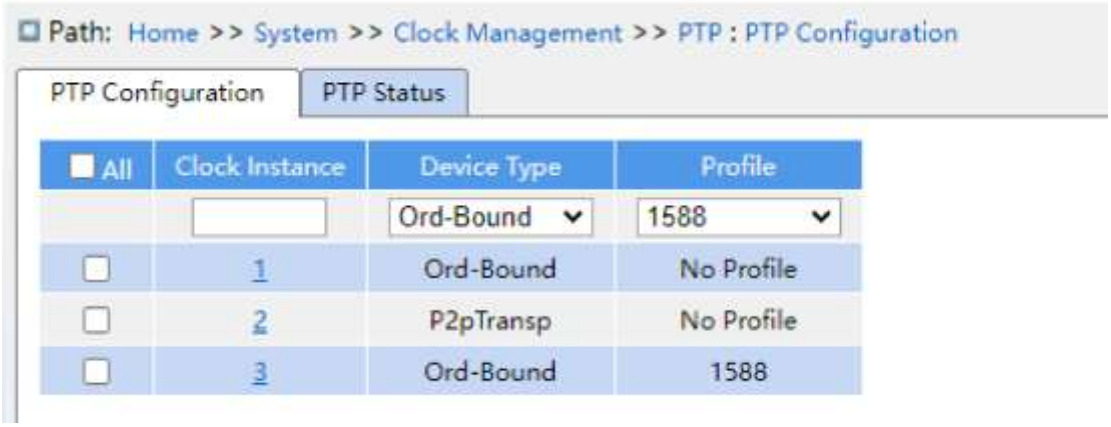


Рисунок 28 – Конфигурация PTP

Clock Instance

Диапазон: 0–3

Функция: ID экземпляра часов.

Clock Type

Варианты настройки: Ord-Bound / P2pTransp / E2eTransp / Masteronly / Slaveonly

Функция: указывает тип экземпляра часов. Существует пять типов устройств:

Ord-Bound: обычные/граничные часы;

P2pTransp: одноранговые прозрачные часы;

E2eTransp: сквозные прозрачные часы;

Masteronly: только главные;

Slaveonly: только подчиненные.

Profile

Варианты настройки: No Profile/1588/802.1AS

Функция: выбор файла описания PTP.

No Profile: профиль PTP не будет применен, и PTP не будет запущен.

1588: указывает стандарт IEEE 1588.

802.1AS: указывает стандарт IEEE 802.1AS.

2. На рисунке 29 показан выбор портов для указанного экземпляра PTP-часов:

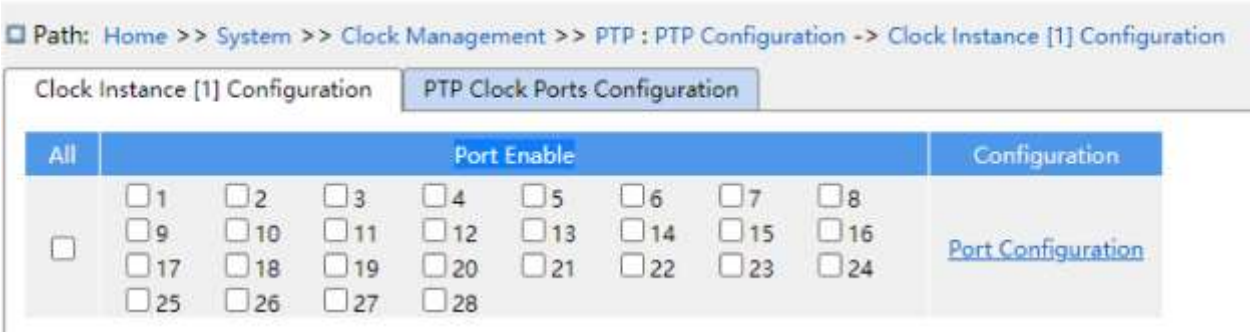


Рисунок 29 – Выбор PTP-портов

Port Enable

Функция: установите флажок для каждого порта, выбранного для этого экземпляра часов.

Configuration

Нажмите <Port Configuration>, чтобы перейти на страницу настройки портов.

3. Настройте порты для экземпляра часов PTP как показано на рисунке 30:

Рисунок 30 – Настройка PTP-портов

State

Функция: Текущее состояние порта.

MDR

Функция: MDR (Message Delay Request) – это интервал запроса задержки, объявленный главным устройством.

PeerMeanPathDel

Функция: задержка в пути, измеренная портом в режиме P2P. В режиме E2E это значение равно 0.

Anv

Функция: интервал выдачи сообщений-анонсов, когда устройство работает в качестве мастера.

ATo

Функция: тайм-аут для получения сообщений-анонсов на порту.

Syv

Функция: интервал выдачи сообщений синхронизации (Sync) главным устройством.

Dlm

Функция: механизм задержки (Delay Mechanism), используемый на данном порту.

e2e – измерение сквозной задержки (между источником и конечным узлом);

p2p – измерение задержки между одноранговыми узлами (точка-точка).

MPR

Функция: интервал, в течение которого отправляются сообщения Delay_Req для порта в режиме E2E. Это значение передается от мастера к слейву в сообщении-анонсе и отражается в поле MDR на слейве. Для режима P2P это значение соответствует интервалу отправки сообщений Pdelay_Req для порта.

Интерпретация этого параметра изменилась с версии 2.40. В предыдущих версиях значение интерпретировалось относительно интервала Sync, что нарушало стандарт. Теперь же значение интерпретируется как чистый интервал.

То есть, если MPR = 0, это означает, что будет отправляться 1 сообщение Delay_Req в секунду, независимо от частоты отправки сообщений Sync.

Delay Asymmetry

Функция: асимметрия задержки передачи для канала связи. См. IEEE 1588, раздел 7.4.2 «Communication path asymmetry».

Ingress latency

Функция: задержка на входе измеряется в нс, как определено в разделе 7.3.4.2 IEEE 1588.

Egress Latency

Функция: задержка на выходе измеряется в нс, как определено в разделе 7.3.4.2 IEEE 1588.

Version

Функция: текущая реализация поддерживает только PTP версии 2.

4. На рисунке 31 показано текущее время локальных часов:

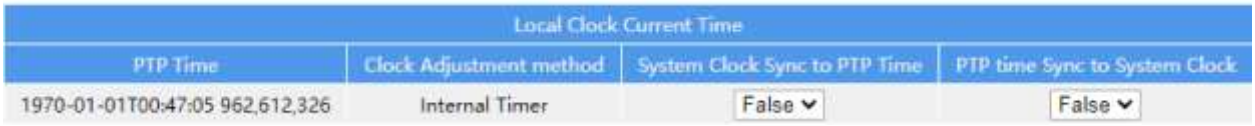


Рисунок 31 – Текущее время локальных часов

PTP Time

Функция: показывает фактическое время PTP с разрешением в наносекундах.

Clock Adjustment method

Функция: показывает фактический метод настройки часов. Метод зависит от доступного оборудования.

System Clock Sync to PTP Time

Функция: при значении «True» происходит синхронизация системных часов со временем PTP.

PTP time Sync to System Clock

Функция: при значении «True» происходит синхронизация времени PTP с системными часами.

5. На рисунке 32 показаны текущие данные часов:

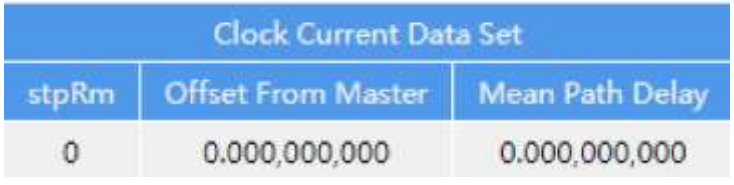


Рисунок 32 – Текущий набор данных

stpRm

Функция: удаленные шаги (Steps Removed): Это количество часов PTP, пройденных от главного мастера до локальных подчиненных часов.

Offset From Master

Функция: разница во времени между главными часами и локальными подчиненными часами, измеряемая в нс.

Mean Path Delay

Функция: среднее время распространения для канала связи между ведущим устройством и локальным ведомым устройством.

6. На рисунке 33 показаны данные родительских часов:

Clock Parent Data Set								
Parent Port Identity	Port	PStat	Var	Change Rate	Grand Master Identity	Grand Master Clock Quality	Priority1	Priority2
02:00:c1:ff:fe:eb:10:ba	0	False	0	0	02:00:c1:ff:fe:eb:10:ba	Cl:248 Ac:Unknwn Va:65535	128	128

Рисунок 33 – Набор данных родительских часов

Parent Port Identity

Функция: идентификатор часов родительского (мастер) устройства. Если локальные часы не являются подчиненными, значение будет равно идентификатору собственных часов.

Port

Функция: идентификатор порта родительского устройства.

PStat

Функция: статус родительских часов (всегда имеет значение «False»).

Var

Функция: наблюдаемое смещение родительских часов, масштабированное по логарифмической дисперсии.

Change Rate

Функция: наблюдаемая скорость изменения фазы родительских часов. Это означает, насколько смещение подчиненных часов отличается от мастера (единица измерения – наносекунды в секунду).

Grand Master Identity

Функция: идентификатор часов главного мастера. Если локальные часы не являются подчиненными, значение будет равно идентификатору собственных часов.

Grand Master Clock Quality

Функция: качество часов, объявленное главным мастером (см. описание набора данных по умолчанию: Clock Quality).

Priority1

Функция: приоритет 1, объявленный главным мастером.

Priority2

Функция: приоритет 2, объявленный главным мастером.

7. На рисунке 34 показан набор данных по умолчанию:

Clock Default Data Set

ClockId	Device Type	2 Step Flag	Port	Clock Identity	Dom	Clock Quality
2	P2pTransp	False	28	02:00:c1:ff:fe:eb:10:bb	0	Cl:248 Ac:Unknwn Va:65535

Priority1	Priority2	Protocol	One-Way	VLAN Tag Enable	VLAN ID	PCP	DSCP
128	128	Ethernet	False	False	1	0	0

Рисунок 34 – Набор данных по умолчанию

Clock Type

Функция: отображает тип экземпляра часов. Существует пять типов устройств:

Ord-Bound: обычные/граничные часы;

P2pTransp: одноранговые прозрачные часы;

E2eTransp: сквозные прозрачные часы;

Masteronly: только главные;

Slaveonly: только подчиненные.

2 Step Flag

Функция: значение «True», если используются двухшаговые события синхронизации и события Pdelay_Resp

Port

Функция: общее количество физических портов в узле.

Clock Identity

Функция: показывает уникальный идентификатор часов

Dom

Функция: домен часов [0…127].

Clock Quality

Функция: качество часов, определяемое системой и состоящее из 3 частей: класс часов (Cl), точность часов (Ac) и дисперсия OffsetScaledLog (Va), как определено в IEEE1588.

Значения точности часов определены в таблице 6 IEEE1588 (в данном примере точность часов установлена на «Unknown» по умолчанию).

Priority1

Функция: приоритет часов 1 [0…255], используемый алгоритмом выбора мастера BMC.

Priority2

Функция: приоритет часов 2 [0…255], используемый алгоритмом выбора мастера BMC.

Protocol

Функция: транспортный протокол, используемый механизмом PTP:

- Ethernet – PTP через Ethernet (многоадресная передача)
- ip4multi – PTP через IPv4 (многоадресная передача)
- ip4uni – PTP через IPv4 (одноадресная передача)

  Примечание – Протокол одноадресной передачи IPv4 работает только в часах Masteronly и Slaveonly (см. параметр Clock Type).
- ip6mixed – PTP через IPv6 (многоадресная и одноадресная передача)

  Примечание – В настоящее время поддерживается только для E2E (End-to-End) одношагового прозрачного устройства.
- EthIPv4IPv6Combo – PTP с использованием любой из инкапсуляций Ethernet, IPv4 или IPv6.

  Примечание: В настоящее время поддерживается только для E2E (End-to-End) одношагового прозрачного устройства.

В одноадресных часах Slaveonly также необходимо настроить, с каких главных часов запрашивать сообщения Announce и Sync.

One-Way

Функция: если значение «True», используются односторонние измерения. Этот параметр применяется только к ведомому устройству. В одностороннем режиме измерения задержки не выполняются, т. е. это применимо только в случае необходимости синхронизации частоты. Ведущее устройство всегда отвечает на запросы задержки.

VLAN ID

Функция: идентификатор VLAN, используемый для маркировки кадров PTP. Пакеты маркируются, если порт настроен для тегирования указанной VLAN.

PCP

Функция: значение приоритета, используемое для кадров PTP.

DSCP

Функция: значение DSCP, используемое при передаче пакетов, инкапсулированных в IPv4

8. На рисунке 35 показан набор данных свойств времени PTP-часов:

Рисунок 35 – Свойства времени

UTC Offset

Функция: в системах, использующих UTC в качестве шкалы времени, это смещение между TAI и UTC.

Valid

Функция: если «True», текущее значение UTC Offset является действительным.

Leap59

Функция: если «True», это поле указывает, что последняя минута текущего дня UTC содержит всего 59 секунд.

Leap61

Функция: если «True», это поле указывает, что последняя минута текущего дня UTC содержит 61 секунду.

Time Trac

Функция: «True» указывает, что временная шкала и значение текущего смещения UTC отслеживаются по отношению к первичному эталону.

Freq Trac

Функция: «True» указывает, что частота, определяющая временную шкалу, отслеживается по отношению к первичному эталону.

PTP Time Scale

Функция: «True» указывает, что часы главного мастера используют временную шкалу PTP.

Time Source

Функция: источник времени, используемый главными часами.

9. На рисунке 36 показано текущее состояние PTP:

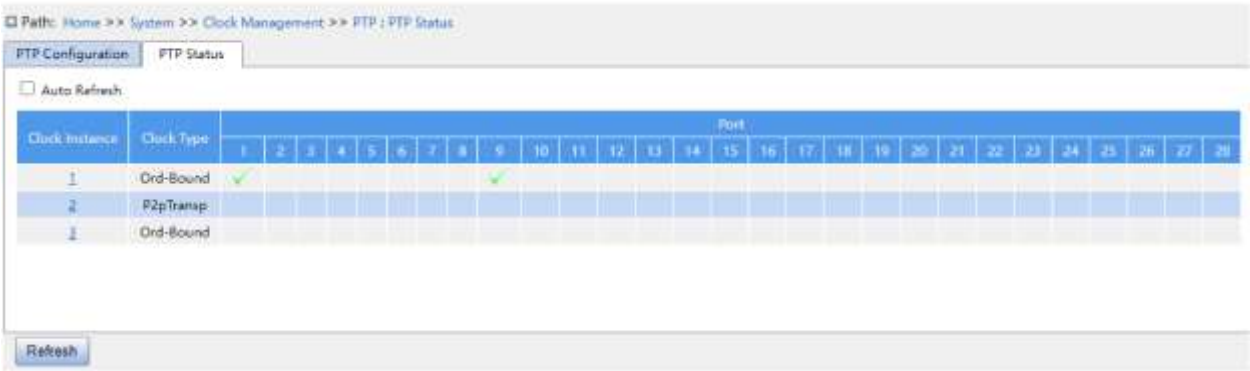


Рисунок 36 – Статус PTP

Clock Instance

Функция: указывает номер конкретного экземпляра часов [0...3].

Clock Type

Функция: отображает тип экземпляра часов. Существует пять типов устройств:

Ord-Bound: обычные/граничные часы;

P2pTransp: одноранговые прозрачные часы;

E2eTransp: сквозные прозрачные часы;

Masteronly: только главные;

Slaveonly: только подчиненные.

4.4 Обновление программного обеспечения

Периодически обновляя программное обеспечение можно добиться улучшения производительности коммутатора. Обновление состоит из ПО загрузчика и основного ПО операционной системы. В первую очередь всегда обновляется загрузчик. Можно также обновить только основное ПО, в таком случае загрузчик остается прежним. Версия программного обеспечения может быть обновлена локально или через протокол FTP/TFTP.

4.4.1 Локальное обновление

1. На рисунке 37 показан выбор обновления ПО из локального файла:

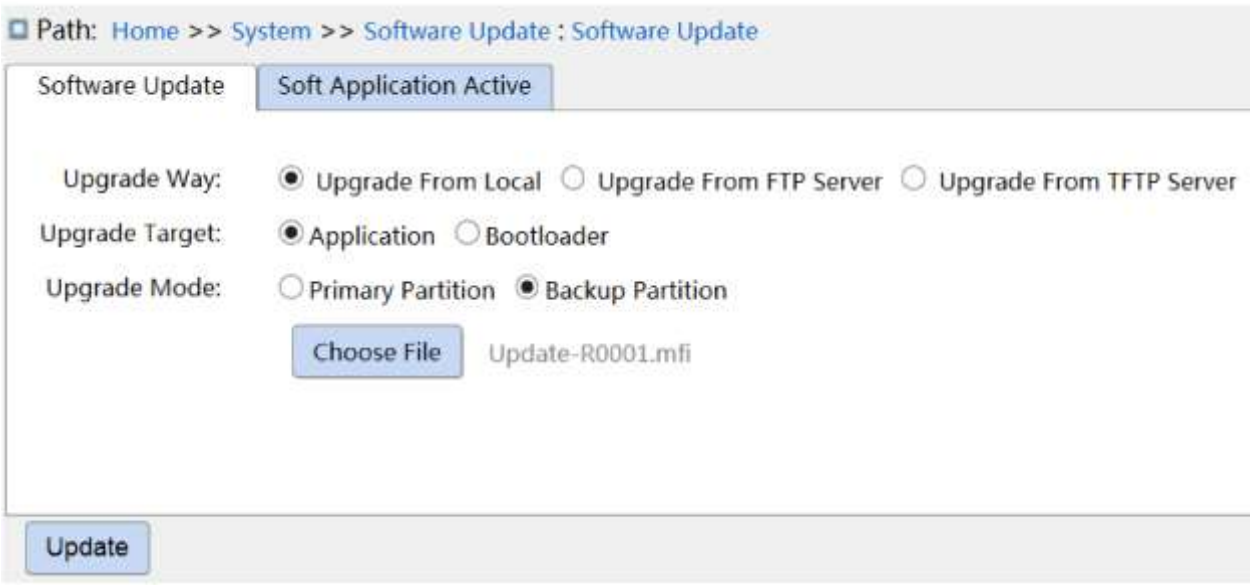


Рисунок 37 – Локальное обновление ПО

Upgrade way

Варианты настройки: Upgrade From Local / Upgrade From FTP Server / Upgrade From TFTP Server

Функция: выбор способа обновления. Обновление из локального каталога; обновление с FTP-сервера; обновление с TFTP-сервера

Upgrade target

Варианты настройки: Application / Bootloader

Функция: выбор цели обновления. версия программного обеспечения; версия загрузчика.

Upgrade mode

Варианты настройки: Primary Partition / Backup Partition

Описание: можно загрузить две версии программного обеспечения (основной раздел/резервный раздел), они могут быть одинаковыми или разными.

2. После успешного обновления, как показано на рисунке 38, активируйте версию программного обеспечения, перезапустив устройство, затем проверьте на странице информации о системе, является ли текущая версия программного обеспечения обновленной.

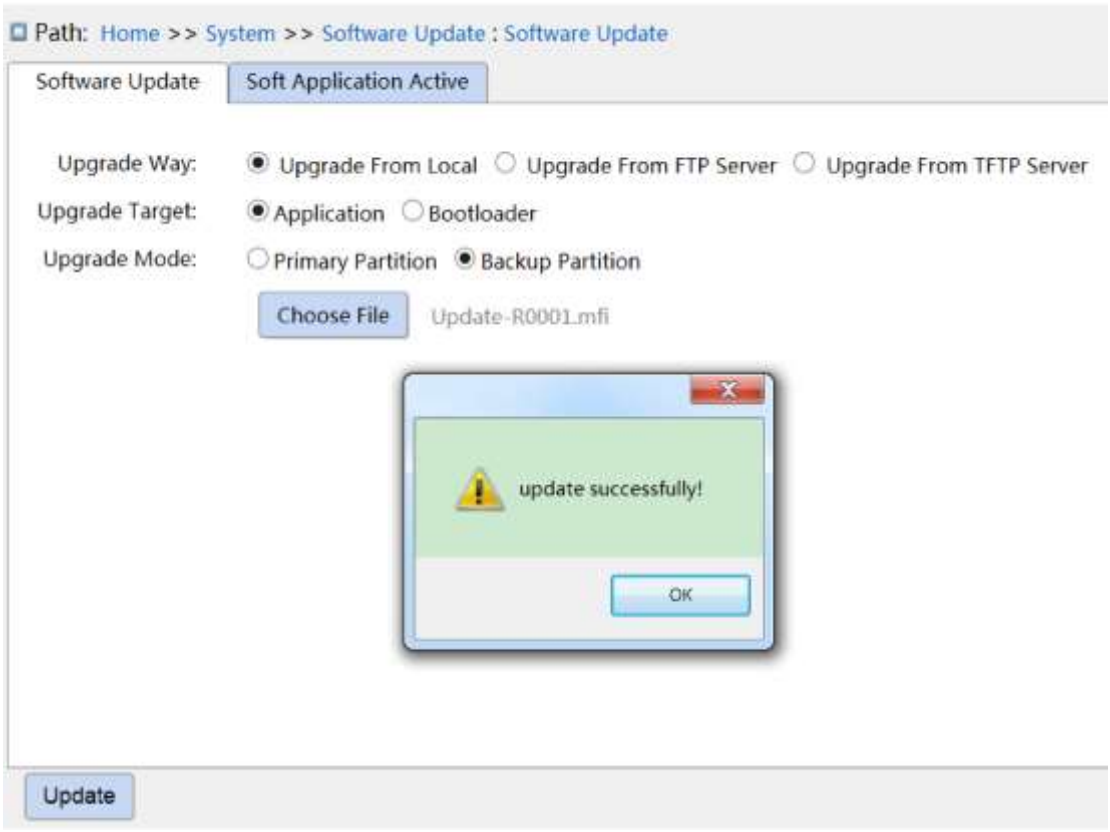


Рисунок 38 – Успешное обновление

- После завершения обновления перезагрузите устройство, чтобы активировать новую версию.

- В случае сбоя обновления не перезагружайте устройство во избежание потери файла прошивки и последующего некорректного запуска.

4.4.2 Обновление через FTP

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

1. Нажмите [Security] → [Users/Rights]. Откроется диалоговое окно «Users/Rights Security Dialog». Нажмите <New User>, чтобы создать нового пользователя FTP, как показано на рисунке 39. Создайте имя пользователя и пароль. Например, имя пользователя «admin» и пароль «123». Нажмите <OK>.

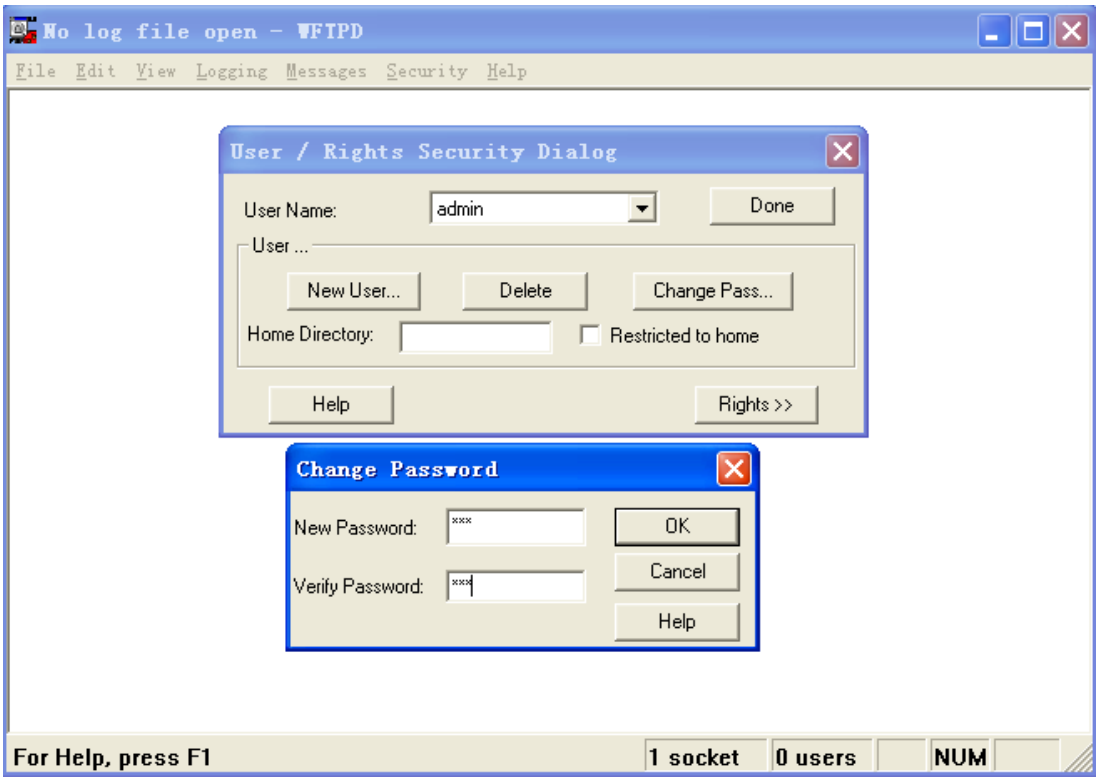


Рисунок 39 – Создание нового пользователя FTP

2. Укажите путь хранения файла с обновлением в «Home Directory», как показано на рисунке 40. Нажмите <Done>.

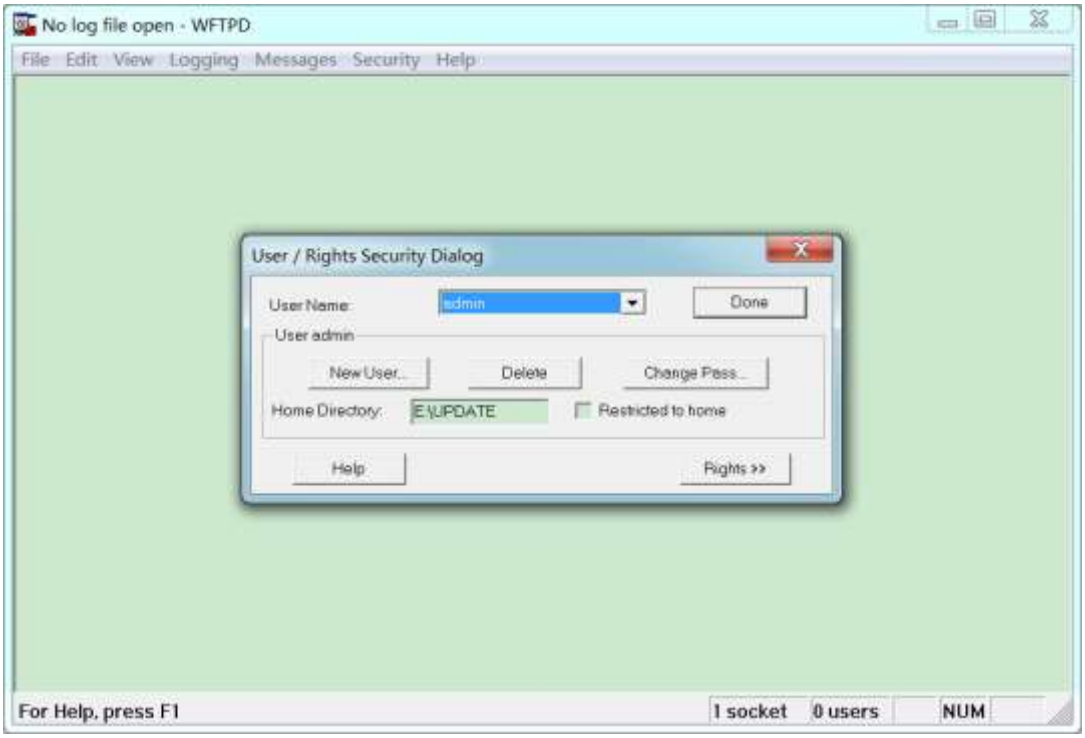


Рисунок 40 – Путь расположения файла

3. Нажмите [System] → [Software Update] в дереве навигации, чтобы перейти на страницу обновления программного обеспечения, как показано на рисунке 41. Введите IP-адрес FTP-сервера, имя пользователя FTP, пароль и имя файла на сервере. Нажмите <Update>.

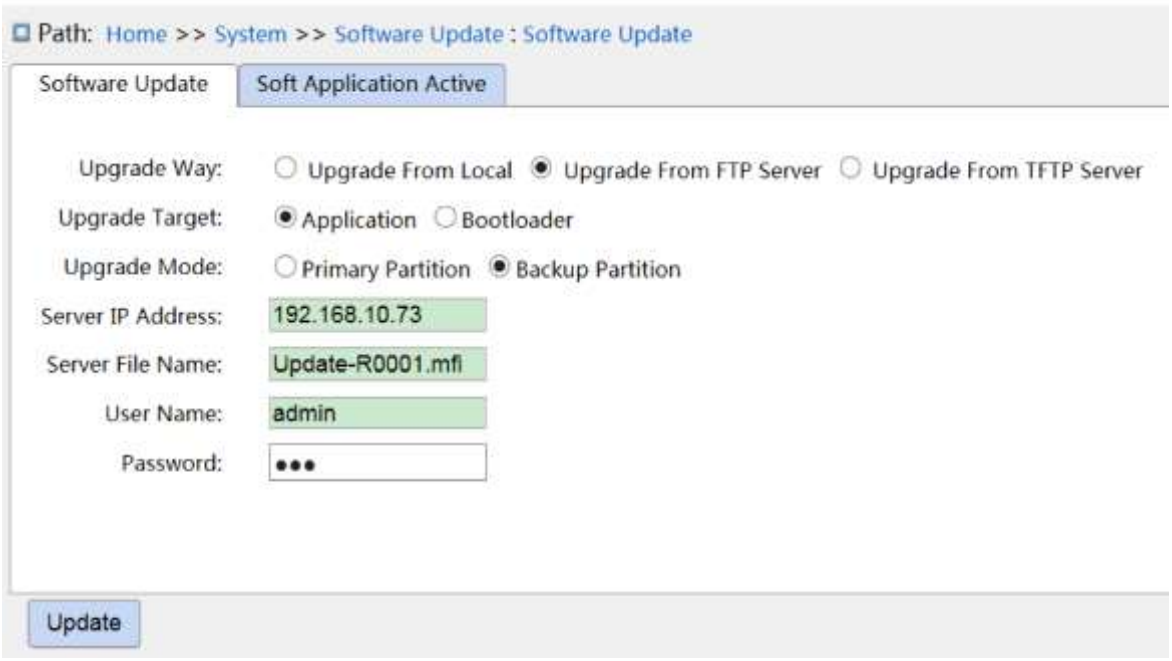


Рисунок 41 – Обновление прошивки через FTP

Upgrade Way

Варианты настройки: Upgrade From Local / Upgrade From FTP Server / Upgrade From TFTP Server

Функция: выбор способа обновления. Обновление из локального каталога; обновление с FTP-сервера; обновление с TFTP-сервера

Upgrade target

Варианты настройки: Application / Bootloader

Функция: выбор цели обновления. версия программного обеспечения; версия загрузчика.

Upgrade mode

Варианты настройки: Primary Partition / Backup Partition

Описание: можно загрузить две версии программного обеспечения (основной раздел / резервный раздел), они могут быть одинаковыми или разными.

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

---

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

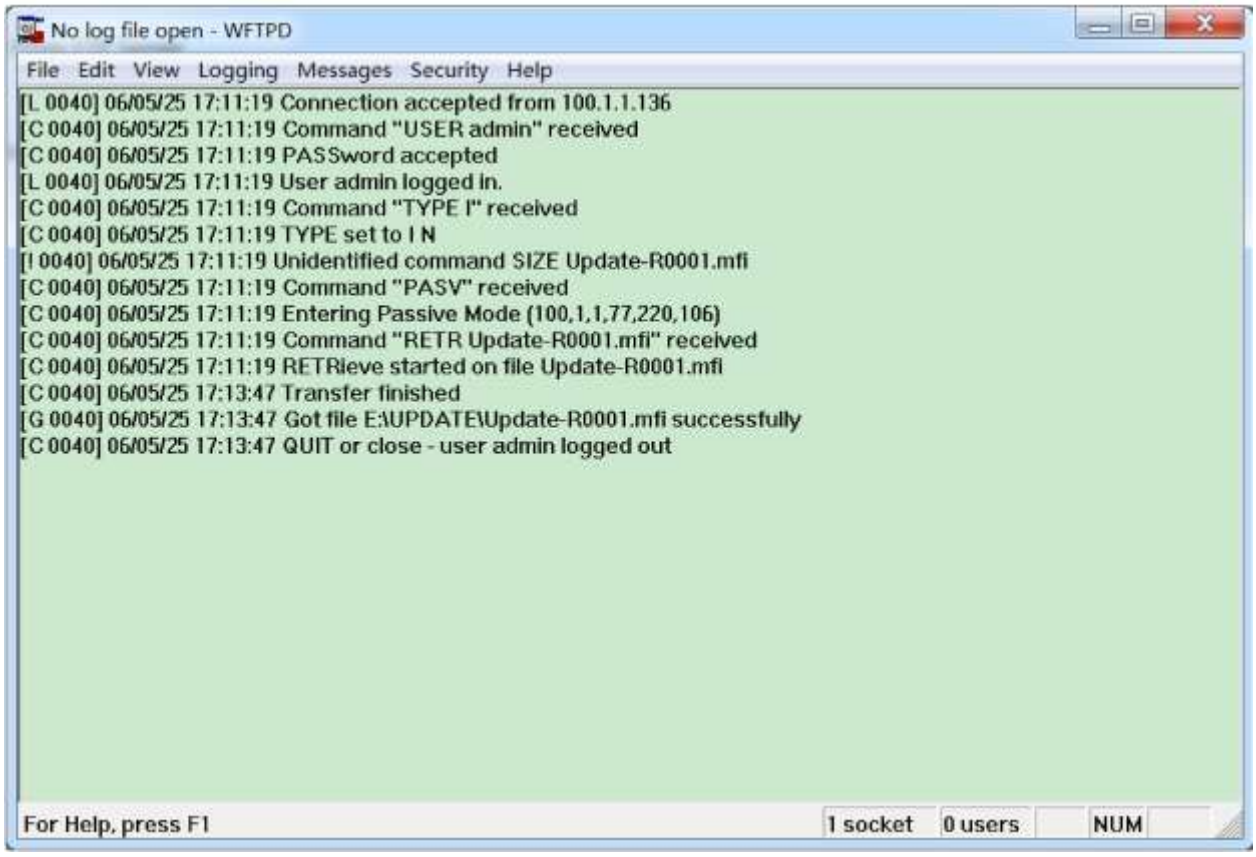


Рисунок 42 – Проверка связи с сервером FTP

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

5. Дождитесь завершения обновления, как показано на рисунке 43.

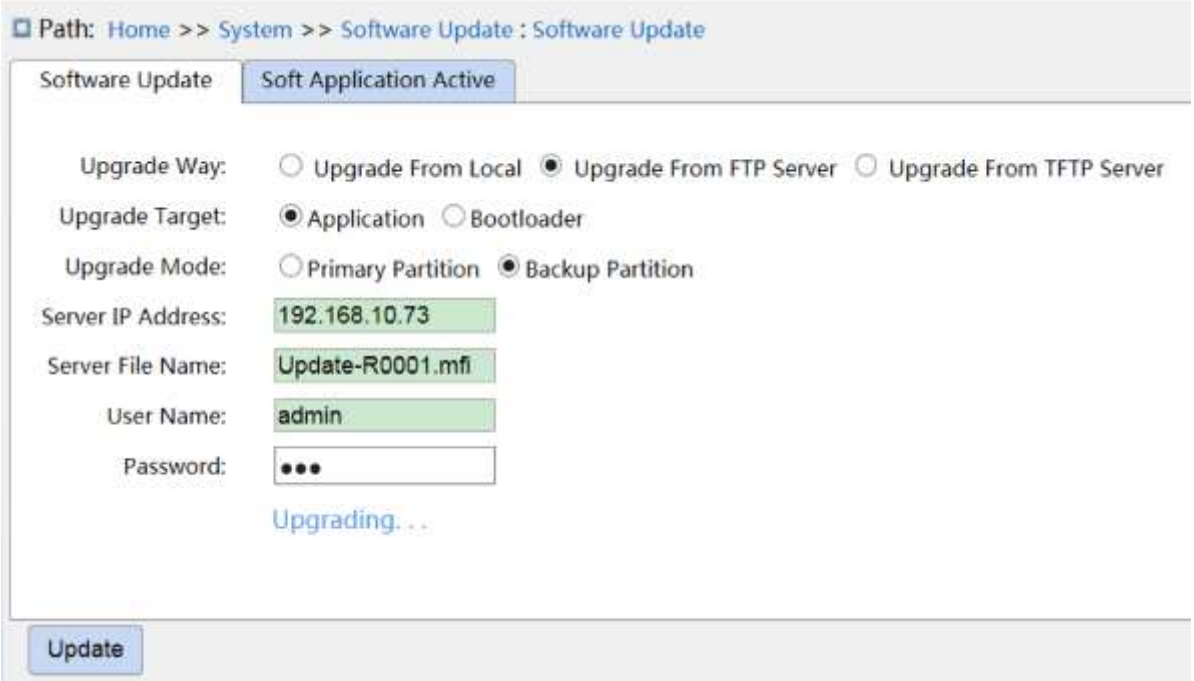


Рисунок 43 – Ход обновления

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

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

4.4.3 Обновление через TFTP

Установите TFTP-сервер. Ниже в качестве примера для обновления используется программное обеспечение TFTPD.

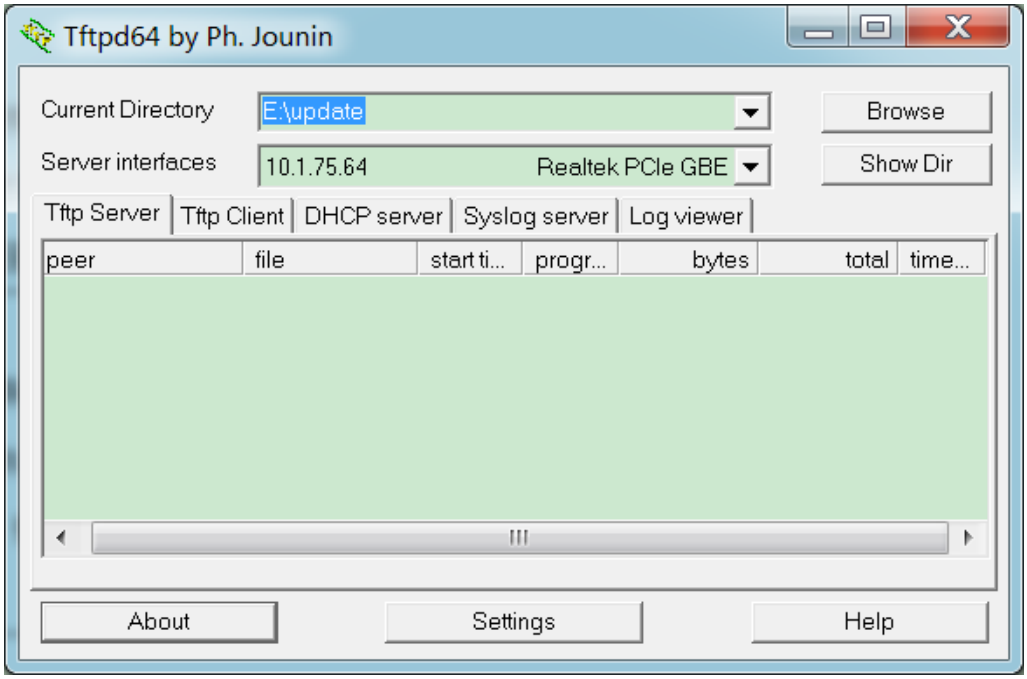


Рисунок 44 – Настройка сервера TFTP

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

2. Нажмите [System] → [Software Update] в дереве навигации, чтобы перейти на страницу обновления программного обеспечения, как показано ниже. Введите IP-адрес TFTP-сервера и имя файла на сервере. Нажмите <Update> и дождитесь завершения обновления.

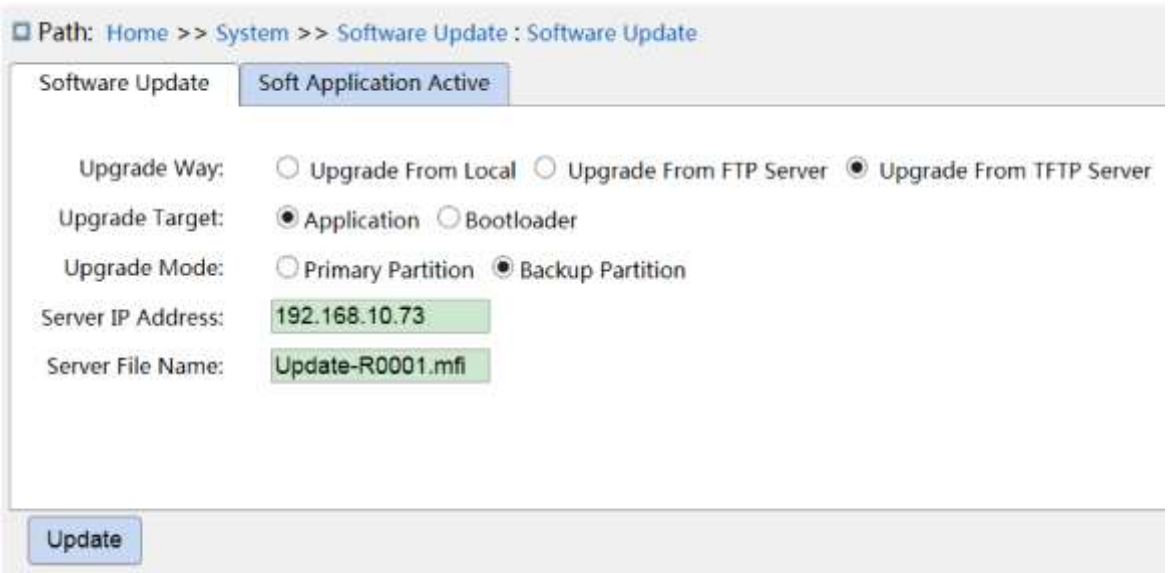


Рисунок 45 – Обновление прошивки через TFTP

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

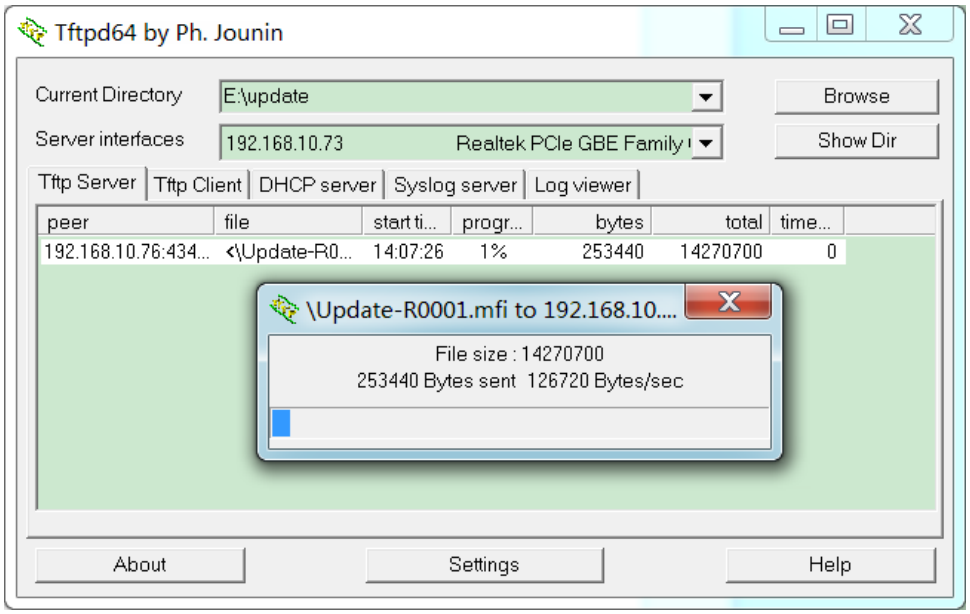


Рисунок 46 – Нормальная связь между TFTP-сервером и коммутатором

4. Дождитесь завершения обновления, как показано ниже.

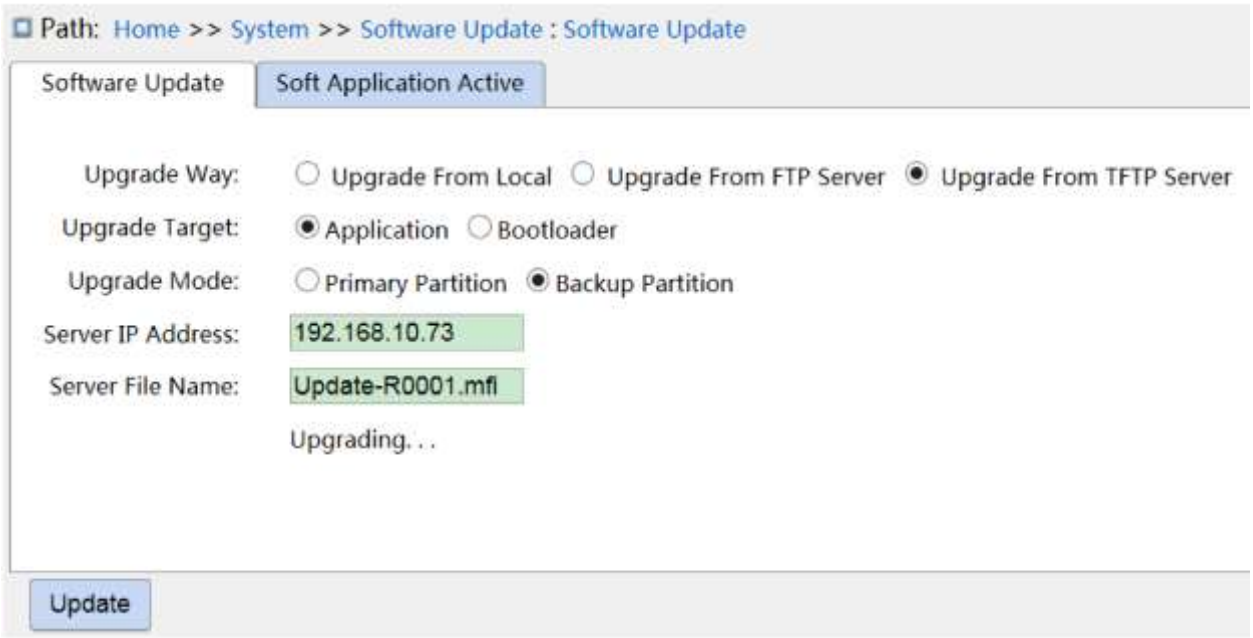


Рисунок 47 – Ход обновления

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

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

4.5 Активация прошивки

Активируйте версию прошивки, как показано на рисунке 48.

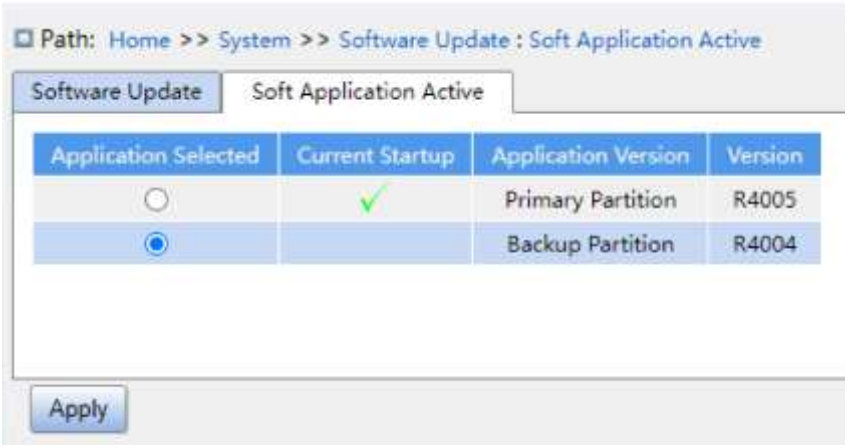


Рисунок 48 – Активация прошивки

Выберите одну версию и нажмите кнопку <Apply>, чтобы применить ее при следующем запуске. Активной может быть только одна версия. «Current Startup» указывает на текущее активное ПО.

4.6 Обновление языка

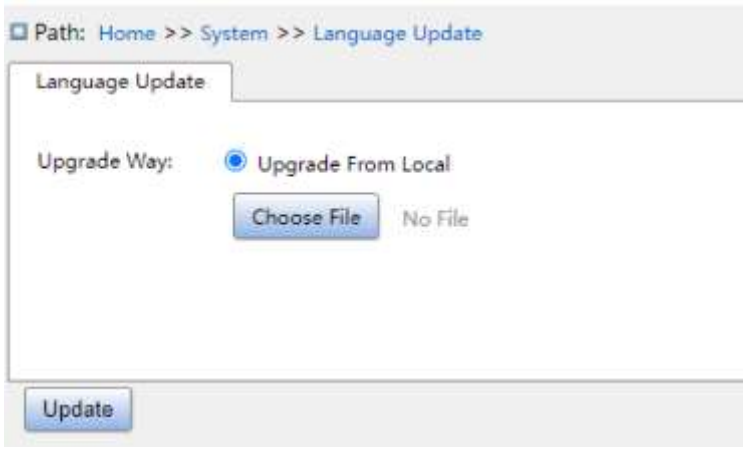


Рисунок 49 – Обновление языка

Upgrade Way

Варианты настройки: Upgrade From Local

Функция: загрузка языковых пакетов на устройства, поддерживающие мультиязычный доступ.

4.7 Перезапуск

Перезагрузите устройство, как показано ниже:

Рисунок 50 – Перезагрузка

Перед перезапуском устройства убедитесь, что текущая конфигурация сохранена. Все несохраненные изменения будут потеряны после перезагрузки.

5. Службы

5.1 SSL

5.1.1 Введение

SSL (Secure Socket Layer) – это протокол безопасности, который обеспечивает защищенное соединение для прикладных протоколов, основанных на TCP, таких как HTTPS. SSL шифрует данные на транспортном уровне, используя симметричный алгоритм шифрования для обеспечения конфиденциальности информации. Кроме того, он применяет секретный ключ для аутентификации, что гарантирует целостность и надежность передаваемых данных. Этот протокол широко используется в веб-браузерах, для отправки и получения электронной почты, сетевых факсов, а также в реальном времени для различных коммуникационных приложений, обеспечивая надежное шифрование для безопасной передачи данных по сети.

5.1.2 Настройка с помощью WEB-интерфейса

1. Включите HTTPS, как показано ниже.

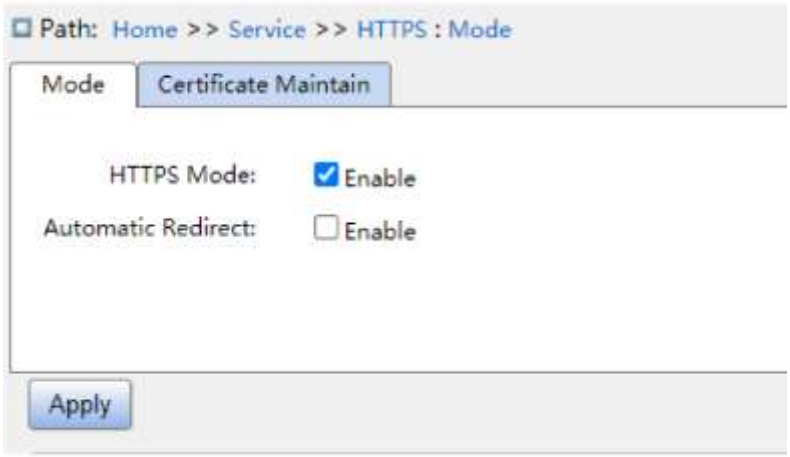


Рисунок 51 – Включение HTTPS

HTTPS Mode

Варианты настройки: Enable /Disable

По умолчанию: Disable

Функция: включение и отключение HTTPS. Если включено, вход в веб-интерфейс коммутатора возможен через http://*ip-адрес* и защищенный канал https://*ip-адрес*.

Automatic redirect

Варианты настройки: Enable /Disable

По умолчанию: Disable

Функция: Автоматическое перенаправление на https. Если включено, для входа на веб-страницы коммутатора разрешена только защищенная ссылка https://*ip-адрес*. Если отключено, на веб-страницу коммутатора можно войти через http и https. Параметр автоматического перенаправления можно настроить только при включенном статусе https.

2. На рисунке 52 показана настройка управления сертификатами.

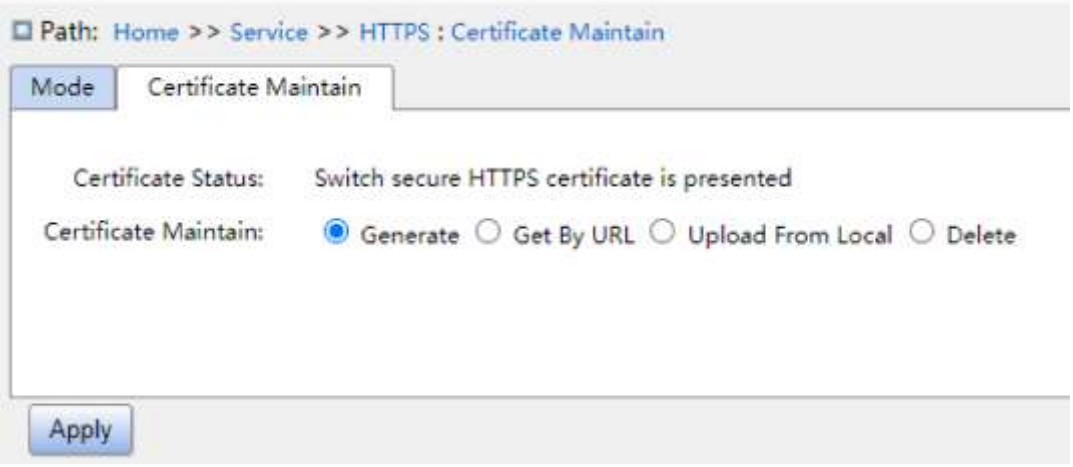


Рисунок 52 – Генерация сертификатов

Maintain

Варианты настройки: Generate / Get By URL / Upload From Local / Delete

Функция: выбор режима загрузки сертификата: сгенерировать, получить по URL, загрузить с локального устройства, удалить.

Get By URL → URL

Функция: указать веб-путь, например, https://10.10.10.10:80/image_path/new_image.dat

Upload From Local → Select File

Функция: выбор файла сертификатов HTTPS с локального устройства.

5.2 SNMP v1/SNMP v2c

5.2.1 Введение

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

5.2.2 Реализация

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

NMS (Network Management Station) – это станция, на которой запущен клиент программного обеспечения управления сетью с поддержкой SNMP. NMS является ядром SNMP-сети. Агент – это процесс, находящийся в памяти сетевого устройства. Он получает и обрабатывает запросы от NMS. Если возникает неполадка, агент самостоятельно оповещает о ней NMS. NMS – это менеджер сети SNMP, а агент – управляемое сетевое устройство. NMS и агенты обмениваются пакетами управления через SNMP. Протокол включает в себя следующие основные операции:

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

NMS отправляет пакеты Get-Request, Get-Next-Request и Set-Request для запроса данных, настройки и управления устройствами. После получения этих запросов, агенты отвечают сообщениями Get-Response. При возникновении неполадок, агент самостоятельно оповещает о них NMS с помощью trap-сообщения.

5.2.3 Пояснение

Коммутаторы данной серии поддерживают SNMP v2c. SNMP v2c обратно совместима с SNMPv1.

Для аутентификации SNMP v1 использует имя комьюнити. Оно играет роль пароля, ограничивая доступ NMS к агентам. Если имя комьюнити в SNMP запросе неизвестно коммутатору, запрос отклоняется и возвращается сообщение об ошибке.

SNMP v2c также использует имя комьюнити для аутентификации. Протокол обратно совместим с SNMPv1, при этом расширяя его возможности.

Для поддержки соединения между NMS и агентом, их версии SNMP должны совпадать. На агенте можно настроить разные версии SNMP, чтобы он мог использовать их для связи с разными NMS.

5.2.4 MIB

Любой настраиваемый ресурс называется объектом управления. База данных MIB (Management Information Base) хранит в себе все объекты управления. Она определяет иерархию объектов и их атрибуты, такие как имя, разрешения доступа, тип данных. Каждый агент имеет свою MIB. NMS может считывать и записывать данные в MIB, в зависимости от разрешений. На рисунке 53 показаны взаимосвязи между NMS, агентом и MIB.

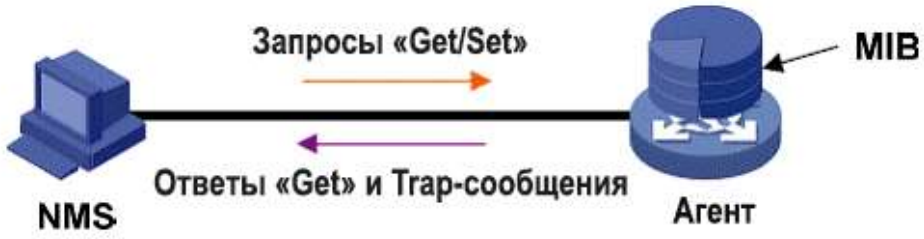


Рисунок 53 – Взаимодействие между NMS, агентом и MIB

MIB представляет из себя древовидную структуру. Узлы дерева являются объектами управления. Каждый узел имеет уникальный идентификатор (Object Identifier – OID), который определяет положение узла в структуре MIB. Как показано на рисунке 54, OID объекта A равен 1.2.1.1.

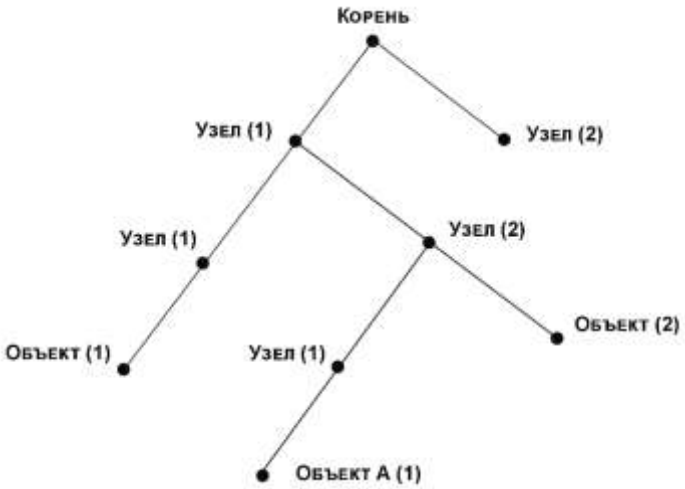


Рисунок 54 – Структура дерева MIB

5.2.5 Настройка с помощью WEB-интерфейса

1. Включите SNMP, как показано ниже:

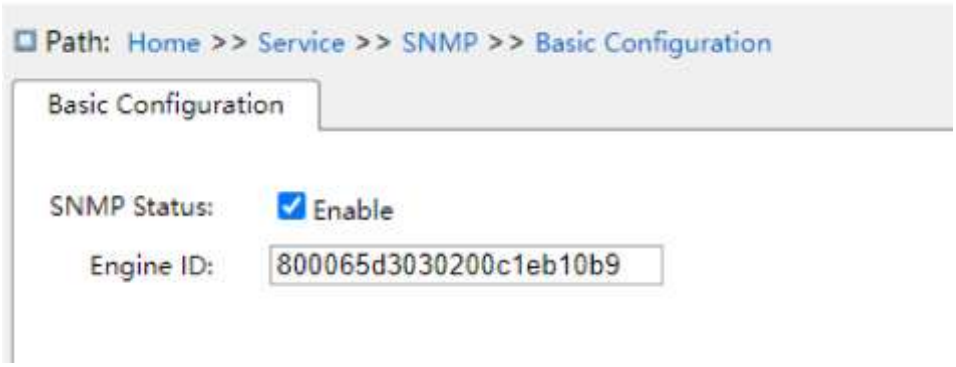


Рисунок 55 – Включение SNMP

SNMP Status

Варианты: Enable/Disable

По умолчанию: Enable

Функция: включение или отключение SNMP.

Engine ID

Диапазон: четное шестнадцатеричное число в диапазоне от 10 до 64. Оно не может быть равно нулю (0) или F (в шестнадцатеричном представлении).

Функция: Engine ID используется для настройки идентификатора системы SNMP версии 3. При изменении Engine ID информация о пользователе, соответствующая идентификатору устройства в таблице пользователей, будет потеряна.

2. На рисунке 56 показана настройка SNMP-комьюнити:

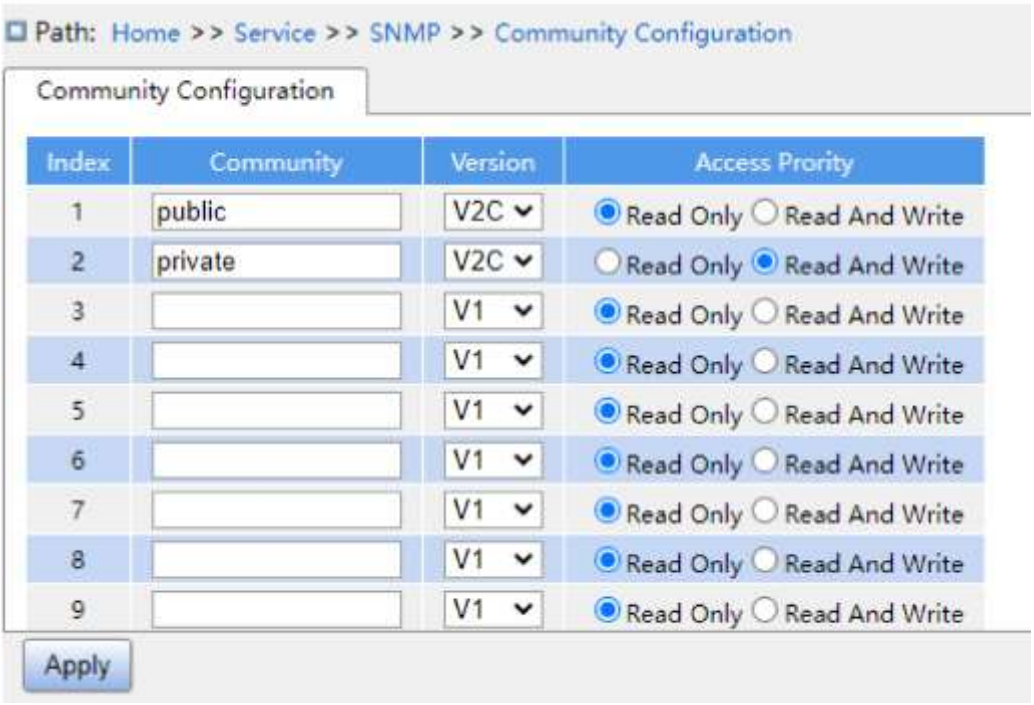


Рисунок 56 – Настройка комьюнити

Community

Диапазон: 1–32 символа

Функция: настройка комьюнити

Описание: доступ к информации из библиотеки MIB коммутатора возможен только в том случае, если имя комьюнити в SNMP-сообщении совпадает с заданной строкой комьюнити.

Примечание: можно настроить до 16 строк комьюнити.

Access Priority

Варианты настройки: Read Only / Read And Write

По умолчанию: Read Only

Функция: настройка прав доступа к библиотеке MIB.

Описание: информация библиотеки MIB может быть доступна с разрешениями только для чтения или для чтения и записи.

3. На рисунке 57 показана настройка функции Trap:

Рисунок 57 – Конфигурация Trap

Trap Name

Диапазон: 1–32 символа

Функция: настройка имени ловушки

Status

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: включение или отключение функции. Если выбрано «Enable», коммутатор будет отправлять соответствующие trap-сообщения на сервер.

Version

Варианты настройки: V1/V2c/V3

По умолчанию: V1

Функция: версия trap-сообщения, которое коммутатор отправляет на сервер.

Destination IP

Формат конфигурации: A.B.C.D

Функция: настройка адреса сервера, на котором принимаются trap-сообщения.

Destination Port

Диапазон: 1–65535

По умолчанию: 162

Функция: настройка номера порта, который отправляет trap-сообщения.

4. Нажмите <Details>, чтобы просмотреть подробную конфигурацию ловушки, как показано ниже:

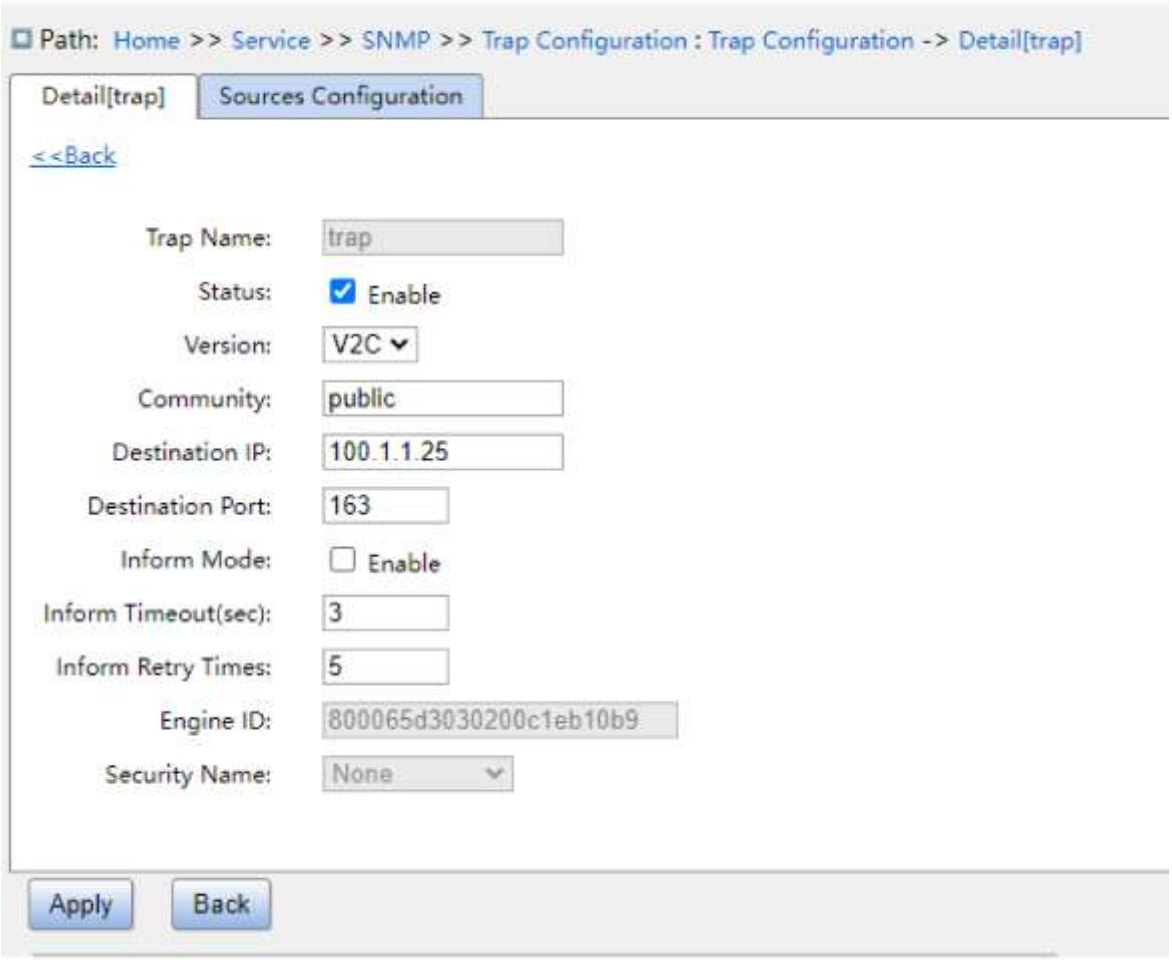


Рисунок 58 – Детальная конфигурация Trap

Community

Диапазон: 0–255 символов

По умолчанию: public

Функция: имя комьюнити, которое передается в отправляемом trap-сообщении.

Inform Mode

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправляет ли сервер ответ коммутатору после получения trap-сообщения.

Inform Timeout

Диапазон: 0–2147 с

По умолчанию: 3 с

Функция: настройка тайм-аута отправки повторного trap-сообщения в случае отсутствия ответа от сервера.

Inform retry Times

Диапазон: 0–255

По умолчанию: 5

Функция: указывает максимальное количество попыток отправки повторного trap-сообщения с тайм-аутом. После превышения заданного числа считается, что отправка trap-сообщения не удалась.

5. Ниже показана настройка событий, активирующих отправку trap-сообщений.

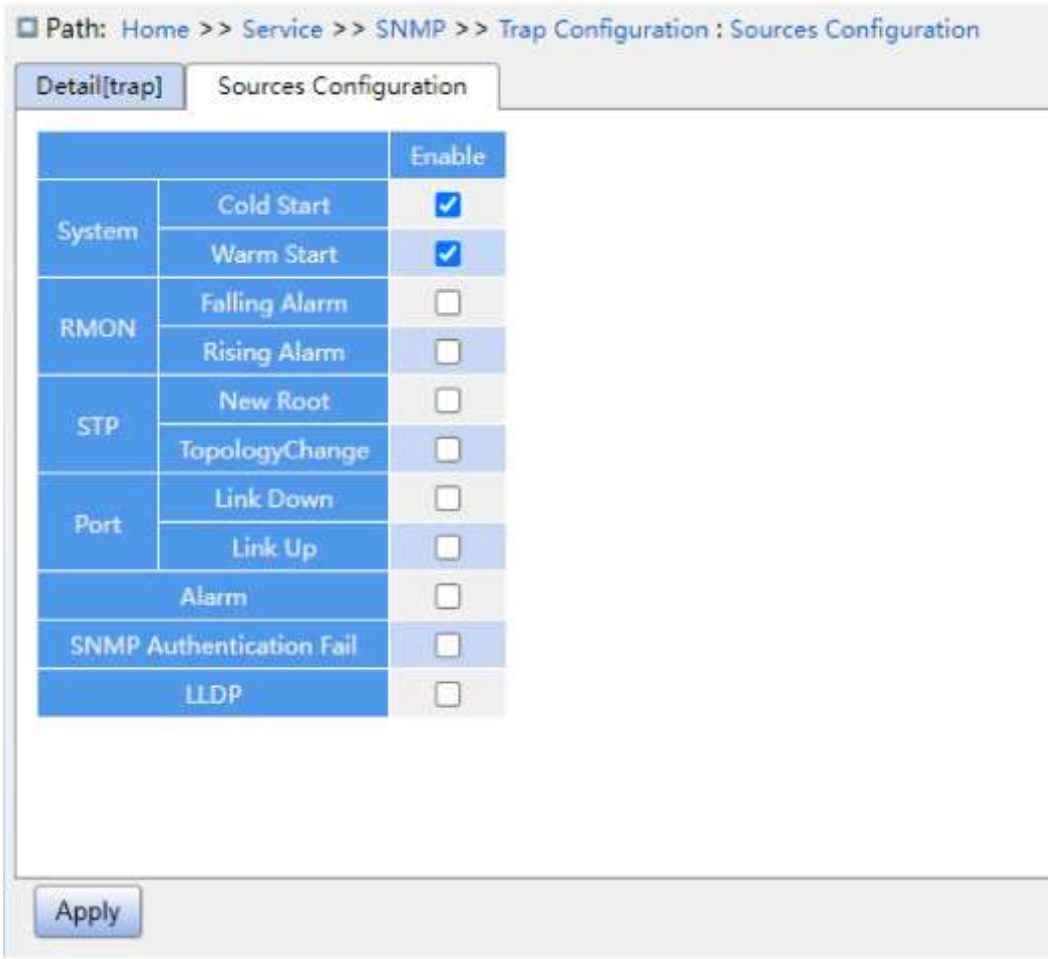


Рисунок 59 – События Trap

System Cold Start/ Warm Start

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при «холодном» и «теплом» старте системы.

RMON Falling Alarm / Rising Alarm

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение, когда RMON генерирует сигнализацию падения/превышения.

STP New Root / Topology Change

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при изменении состояния STP.

Port Link Down / Link Up

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при изменении состояния порта.

Alarm

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при наличии информации о тревожной ситуации.

SNMP Authentication Fail

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение, если аутентификация SNMP не удалась.

LLDP

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при изменении статуса LLDP-соседа.

5.2.6 Пример типовой настройки

Сервер управления SNMP подключен к коммутатору через Ethernet. IP-адрес сервера управления – 192.168.0.23, а коммутатора – 192.168.0.2, как показано на рисунке 60. NMS отслеживает и управляет агентом через SNMPv2c, а также считывает и записывает информацию MIB-узла агента. Когда агент неисправен, он сам отправляет trap-сообщения в NMS.

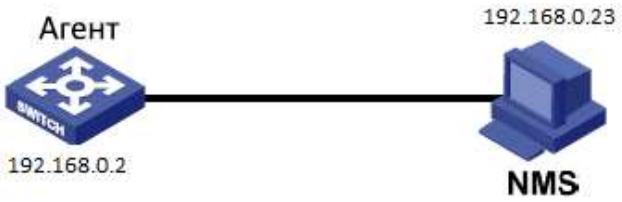


Рисунок 60 – Пример настройки SNMP

Настройка агента

1. Включите SNMP. Укажите версию V2C и настройте права доступа «Read Only» для комьюнити «public» и «Read And Write» для комьюнити «private», как показано на рисунках 55, 56.

2. Включите и настройте глобальную функцию Trap, как показано на рисунке 57.

3. Создайте запись Trap 111, отметьте статус «Enable»; выберите версию V2C, укажите IP-адрес назначения 192.168.0.23. Отметьте события о которых необходимо отправлять сообщения и примите настройки по умолчанию для других параметров, как показано на рисунках 58, 59.

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

5.3 SNMP v3

5.3.1 Введение

SNMP v3 предоставляет механизм аутентификации, относящийся к модели безопасности на основе пользователя (USM). Вы можете настроить функции аутентификации и шифрования. Аутентификация используется для проверки подлинности отправителя пакета, предотвращая доступ нелегитимных пользователей. Для защиты от перехвата применяется шифрования пакетов, передаваемых между NMS и агентом. Таким образом, повышается безопасность сети SNMP.

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

5.3.2 Реализация

Для SNMP v3 предоставляется четыре таблицы конфигурации. Каждая таблица может содержать 16 записей. Эти таблицы определяют, могут ли конкретные пользователи получать доступ к информации MIB.

В таблице пользователей можно создать несколько пользователей. Каждый из них использует разные политики безопасности для аутентификации и шифрования.

В таблице групп права доступа определяются на основе групп пользователей. Все пользователи группы имеют права группы.

Таблица представлений ссылается на информацию представления MIB, которая указывает, к каким данным могут получить доступ пользователи. Представление MIB может содержать все узлы определенного поддерева MIB (то есть пользователям разрешен доступ ко всем узлам поддерева MIB) или не содержать ни одного узла определенного поддерева MIB (то есть пользователям запрещен доступ к любому узлу поддерева MIB).

Вы можете определить права доступа к MIB в таблице доступа по имени группы, модели безопасности и уровню безопасности.

5.3.3 Настройка с помощью WEB-интерфейса

1. Включите SNMP, как показано ниже:

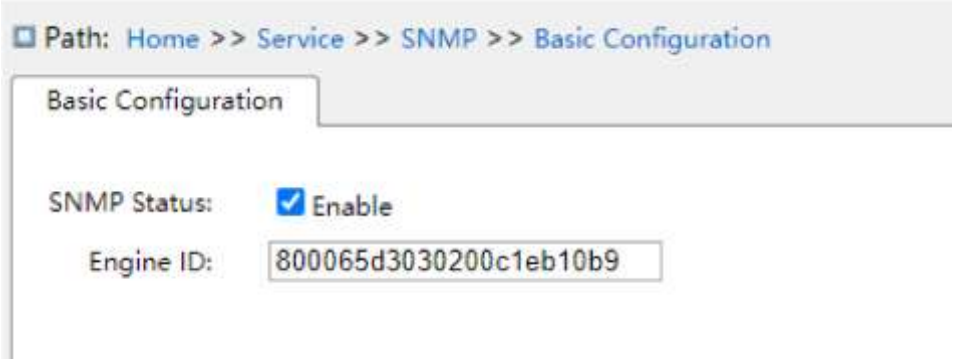


Рисунок 61 – Включение SNMP

SNMP Status

Варианты настройки: Enable/Disable

По умолчанию: Enable

Функция: включение или отключение SNMP.

Engine ID

Диапазон: четное шестнадцатеричное число в диапазоне от 10 до 64. Оно не может быть равно нулю (0) или F (в шестнадцатеричном представлении).

Функция: Engine ID используется для настройки идентификатора системы SNMP версии 3. При изменении Engine ID информация о пользователе, соответствующая идентификатору устройства в таблице пользователей, будет потеряна.

2. На рисунке 62 показана настройка функции Trap:

Рисунок 62 – Конфигурация Trap

Trap Name

Диапазон: 1–32 символа

Функция: настройка имени ловушки

Status

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: включение или отключение функции. Если выбрано «Enable», коммутатор будет отправлять соответствующие trap-сообщения на сервер.

Version

Варианты настройки: V1/V2C/V3

По умолчанию: V1

Функция: версия trap-сообщения, которое коммутатор отправляет на сервер.

Destination IP

Формат конфигурации: A.B.C.D

Функция: настройка адреса сервера, на котором принимаются trap-сообщения.

Destination Port

Диапазон: 1–65535

По умолчанию: 162

Функция: настройка номера порта, который отправляет trap-сообщения.

3. Нажмите <Details>, чтобы просмотреть подробную конфигурацию ловушки, как показано ниже:

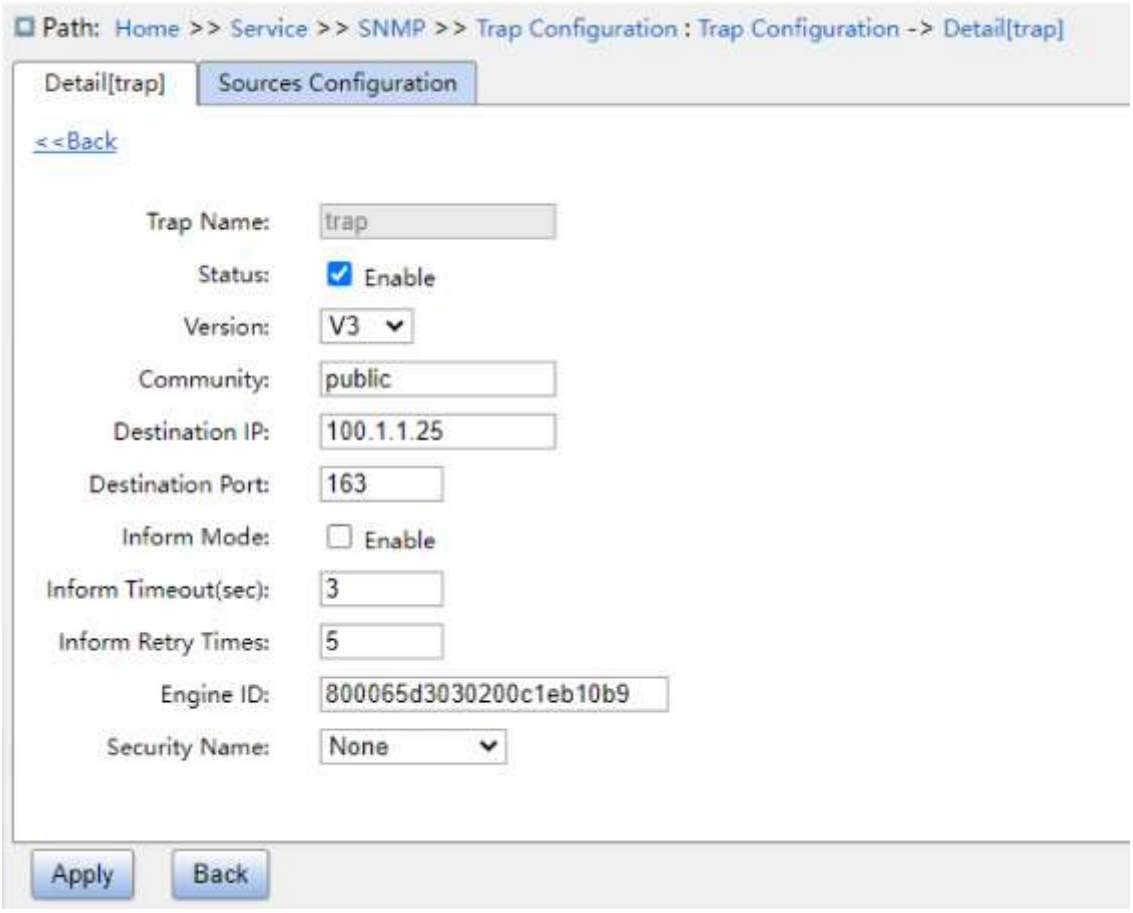


Рисунок 63 – Детальная конфигурация Trap

Community

Диапазон: 0–255 символов

По умолчанию: public

Функция: имя комьюнити, которое передается в отправляемом trap-сообщении.

Inform Mode

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправляет ли сервер ответ коммутатору после получения trap-сообщения.

Inform Timeout

Диапазон: 0–2147 с

По умолчанию: 3 с

Функция: настройка тайм-аута отправки повторного trap-сообщения в случае отсутствия ответа от сервера.

Inform retry Times

Диапазон: 0–255

По умолчанию: 5

Функция: указывает максимальное количество попыток отправки повторного trap-сообщения с тайм-аутом. После превышения заданного числа считается, что отправка trap-сообщения не удалась.

Engine ID

Диапазон: четное шестнадцатеричное число в диапазоне от 10 до 64. Оно не может быть равно нулю (0) или F (в шестнадцатеричном представлении).

Функция: настройка значения идентификатора модуля безопасности, которое передается в trap-сообщении SNMP v3.

4. Ниже показана настройка событий, активирующих отправку trap-сообщений.

Рисунок 64 – События Trap

System Cold Start/ Warm Start

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при «холодном» и «теплом» старте системы.

RMON Falling Alarm / Rising Alarm

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение, когда RMON генерирует сигнализацию падения/превышения.

STP New Root / Topology Change

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при изменении состояния STP.

Port Link Down / Link Up

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при изменении состояния порта.

Alarm

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при наличии информации о тревожной ситуации.

SNMP Authentication Fail

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение, если аутентификация SNMP не удалась.

LLDP

Варианты настройки: Enable / Disable

По умолчанию: Disable

Функция: указывает, отправлять ли trap-сообщение при изменении статуса LLDP-соседа.

5. На рисунке 65 показана настройка таблицы пользователей.

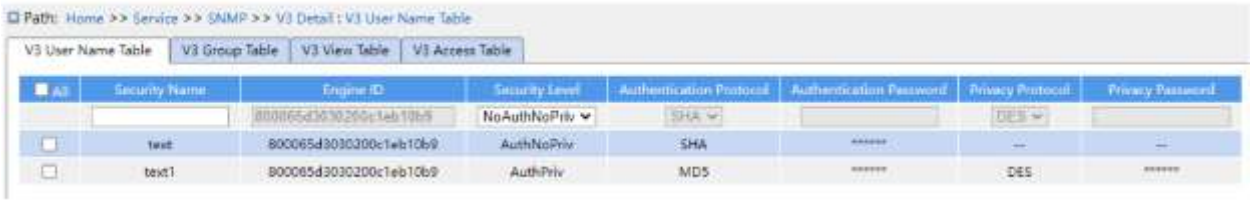


Рисунок 65 – Таблица пользователей SNMP v3

Security Name

Диапазон: 1–32 символа

Функция: создание имени пользователя.

Engine ID

Диапазон: четное шестнадцатеричное число в диапазоне от 10 до 64. Оно не может быть равно нулю (0) или F (в шестнадцатеричном представлении).

Функция: настройка значения идентификатора модуля безопасности, которое передается в trap-сообщении SNMP v3.

Security Level

Варианты настройки: NoAuthNoPriv / AuthNoPriv / AuthPriv

Функция: настройка уровня безопасности текущего пользователя.

Описание: NoAuthNoPriv – не требуется ни аутентификация, ни шифрование; AuthNoPriv – необходимо аутентифицировать, но не шифровать; AuthPriv – требуется как аутентификация, так и шифрование.

Authentication Protocol

Варианты настройки: MD5 / SHA

Функция: выбор протокола аутентификации. Если уровень безопасности пользователя AuthNoPriv или AuthPriv, необходимо настроить протокол и пароль аутентификации.

Authentication Password

Диапазон: 8–40 символов (протокол MD5) 8–32 символа (протокол SHA)

Функция: создание пароля аутентификации.

Privacy Protocol

Варианты настройки: DES / AES

Функция: выбор протокола конфиденциальности. Протокол и пароль конфиденциальности необходимо настроить на уровне безопасности AuthPriv.

Privacy Password

Диапазон: 8–32 символа

Функция: создание пароля конфиденциальности.

Всего в таблице можно настроить до 16 пользователей.

6. На рисунке 66 показана настройка таблицы групп.

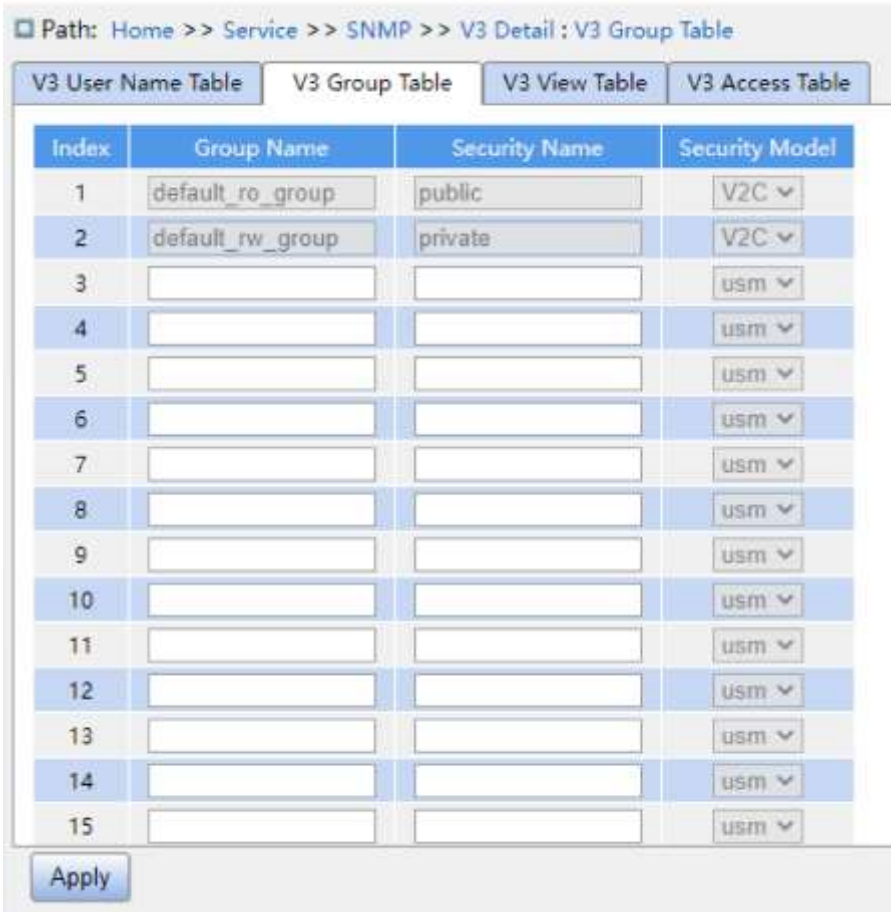


Рисунок 66 – Таблица групп

Group name

Диапазон: 1–32 символа

Функция: настройка имени группы. Пользователи с одинаковым именем группы принадлежат к одной группе.

Security model

По умолчанию: usm

Функция: указывает модель безопасности текущей группы (то есть номер версии SNMP). SNMP v3 использует технологию USM (модель безопасности на основе пользователя).

Security name

Диапазон: созданное имя пользователя, 1–32 символа

Функция: указывает имя безопасности, которое должно совпадать с именем пользователя в таблице пользователей. Пользователи с одинаковым именем группы принадлежат к одной группе.

7. На рисунке 67 показана настройка таблицы представлений.

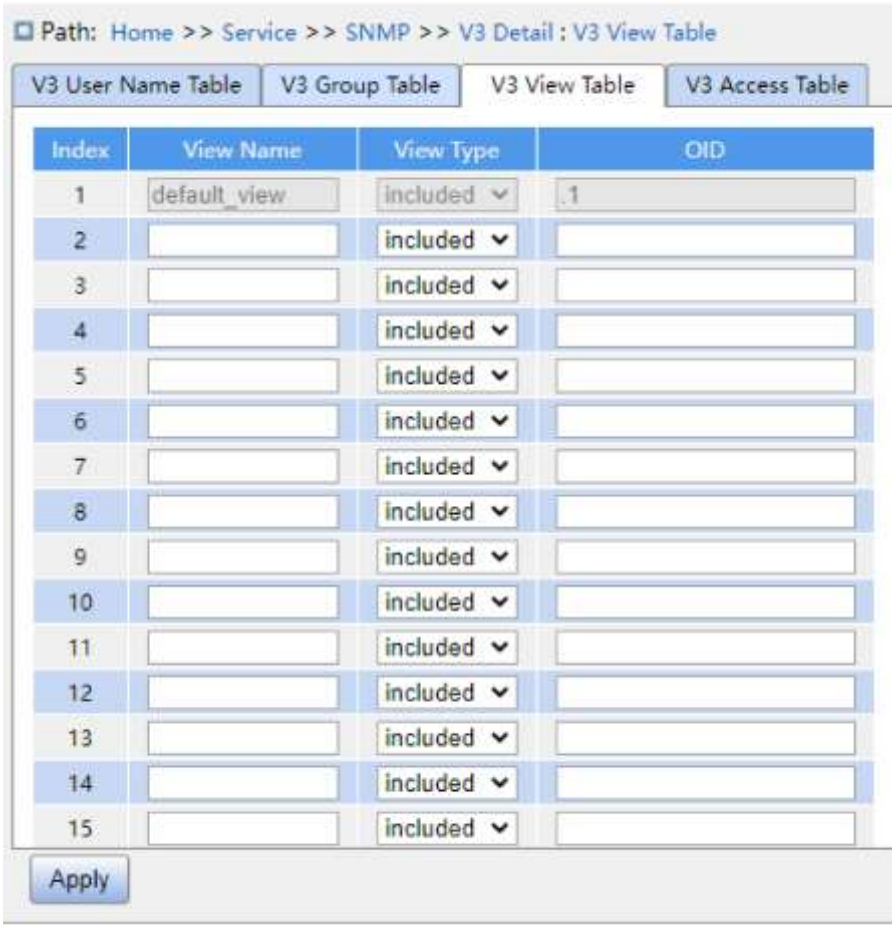


Рисунок 67 – Таблица представлений

View Name

Диапазон: 1–32 символа

Функция: указывает имя представления.

View Type

Варианты настройки: included / excluded

Функция: «included» указывает, что текущее представление включает все узлы поддерева MIB, «excluded» указывает, что текущее представление не включает ни одного узла поддерева MIB.

OID

Функция: указывает поддерево MIB, которое определяется с помощью OID корневого узла этого поддерева.

По умолчанию таблица представлений «default_view» включает все узлы поддерева.

8. На рисунке 68 показана настройка таблицы доступа.

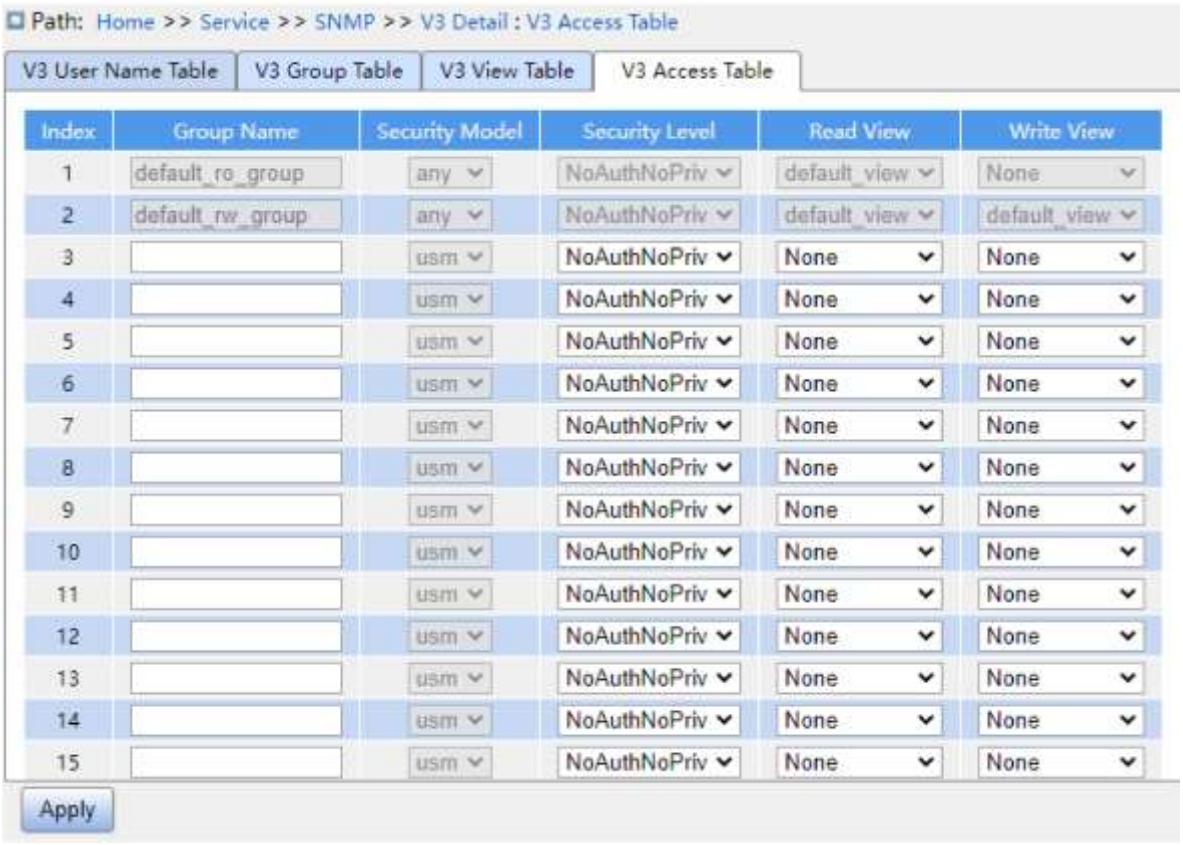


Рисунок 68 – Таблица доступа

Group Name

Диапазон: Созданное имя группы, 1–32 символа

Описание: все пользователи в группе имеют одинаковые права доступа.

Security Model

По умолчанию: any / v1 / v2 / usm

Функция: выбор модели безопасности для группового доступа (то есть номер версии SNMP). SNMP v3 использует технологию USM (модель безопасности на основе пользователя). «Any» означает использование любой модели безопасности. Имя группы, конфигурация модели безопасности должны соответствовать имени группы и модели безопасности в таблице групп.

Security Level

Варианты настройки: NoAuthNoPriv / AuthNoPriv / AuthPriv

Функция: настройка уровня безопасности текущей группы.

Описание: NoAuthNoPriv – не требуется ни аутентификация, ни шифрование; AuthNoPriv – необходимо аутентифицировать, но не шифровать; AuthPriv – требуется как аутентификация, так и шифрование. Если требуется шифрование, протокол аутентификации/шифрования, пароль аутентификации/шифрования на стороне NMS

должны соответствовать конфигурации таблицы пользователей, тогда к информации об узле коммутатора можно будет успешно получить доступ.

Уровень безопасности увеличивается в следующем порядке: NoAuthNoPriv, AuthNoPriv, AuthPriv. Низкий уровень безопасности позволяет получить доступ пользователям с более высоким уровнем безопасности. Если для группы настроен уровень безопасности как AuthNoPriv, пользователи с уровнем безопасности как AuthNoPriv, так и AuthPriv в этой группе могут успешно получить доступ к коммутатору. Однако, даже если и протокол, и пароль аутентификации/шифрования верны, пользователи с уровнем безопасности NoAuthNoPriv доступ получить уже не могут.

Read View

Варианты настройки: default_view / None / новое имя

Функция: выбор имени представления только для чтения.

Write View

Варианты настройки: default_view / None / новое имя

Функция: выбор имени представления для чтения и записи.

Таблицы доступа по умолчанию в коммутаторе {default_ro_group, any, NoAuth,NoPriv, default_view, None}, {default_rw_group, any, NoAuth,NoPriv, default_view, default_view}.

5.3.4 Пример типовой настройки

Сервер управления SNMP подключен к коммутатору через Ethernet. IP-адрес сервера управления – 192.168.0.23, а коммутатора – 192.168.0.2, как показано на рисунке 69. Пользователь 1111 и пользователь 2222 управляют агентом через SNMP v3. Уровень безопасности установлен на AuthNoPriv, и коммутатор может выполнять только операции чтения всей информации об узле агента. При возникновении тревоги агент самостоятельно отправляет trap-сообщения версии 3 в NMS

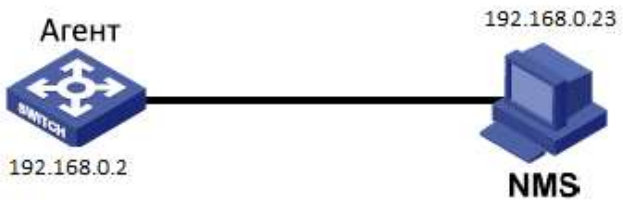


Рисунок 69 – Пример настройки SNMP v3

Настройка агента

1. Включите SNMP и укажите версию 3, как показано на рисунке 61.
2. Настройте таблицу пользователей SNMP v3

Создайте пользователя с именем 1111, укажите для него уровень безопасности AuthPriv, протокол аутентификации MD5, пароль аутентификации aaaaaaaa, протокол конфиденциальности DES и пароль конфиденциальности xxxxxxxx.

Создайте другого пользователя с именем 2222, укажите для него уровень безопасности AuthPriv, протокол аутентификации SHA, пароль аутентификации bbbbbbbb, протокол конфиденциальности AES и пароль конфиденциальности yyyyyyyy, как показано на рисунке 65.

3. Создайте группу, укажите для нее модель безопасности usm и добавьте пользователей 1111 и 2222 в группу, как показано на рисунке 66.

4. Настройте таблицу доступа SNMP v3

Укажите имя группы group, модель безопасности usm, уровень безопасности AuthNoPriv, представления только для чтения default_view и представления для чтения и записи None, как показано на рисунке 68.

5. Включите глобальную функцию Trap, как показано на рисунке 62.

6. Создайте запись Trap с именем 222, отметьте статус «Enable»; выберите версию V3, укажите IP-адрес назначения 192.168.0.23. Отметьте события о которых необходимо отправлять сообщения и примите настройки по умолчанию для других параметров, как показано на рисунках 63, 64.

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

5.4 SSH

5.4.1 Введение

SSH (Secure Shell) – сетевой протокол для безопасного удаленного входа. Он шифрует все передаваемые данные, чтобы предотвратить раскрытие информации. Когда данные зашифрованы SSH, для настройки коммутатора необходимо использовать командную строку. Коммутатор поддерживает функцию сервера SSH и позволяет подключать нескольких пользователей, которые заходят на коммутатор удаленно через SSH.

5.4.2 Реализация

Чтобы реализовать защищенное соединение SSH в процессе коммуникации, сервер и клиент проходят пять этапов, описанных ниже.

Этап согласования версии: в настоящее время SSH представлен двумя версиями: SSH1 и SSH2. Две стороны договариваются об используемой версии.

Этап согласования ключа и алгоритма: SSH поддерживает несколько типов алгоритмов шифрования. Две стороны договариваются об используемом алгоритме.

Этап аутентификации: клиент SSH отправляет запрос аутентификации на сервер, а сервер аутентифицирует клиента.

Этап запроса сеанса: клиент отправляет запрос сеанса на сервер после прохождения аутентификации.

Этап сеанса: клиент и сервер начинают взаимодействие после передачи запроса сеанса.

5.4.3 Настройка с помощью WEB-интерфейса

1. Включите протокол SSH, как показано ниже:

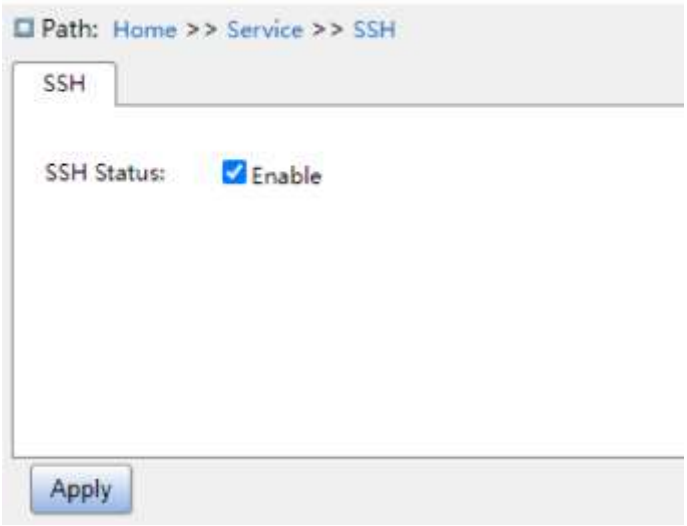


Рисунок 70 – Включение SSH

SSH Status

Варианты настройки: Enable/Disable

По умолчанию: Enable

Функция: включение или отключение протокола SSH. Если включено, коммутатор работает как SSH-сервер.

5.4.4 Пример типовой настройки

Хост работает как SSH-клиент для установления локального соединения с коммутатором, как показано на рисунке 71.

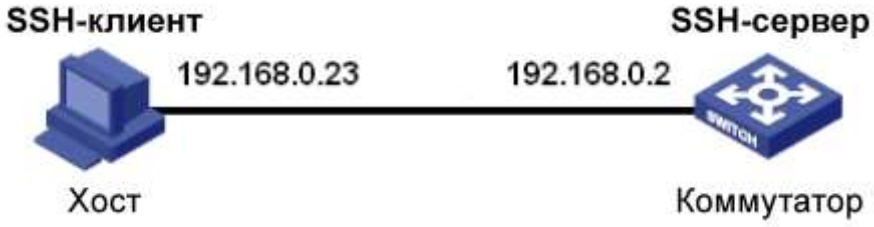


Рисунок 71 – Пример конфигурации SSH

1. Включите протокол SSH, как показано на рисунке 70.

2. Установите соединение с сервером SSH. Сначала запустите программное обеспечение PuTTY.exe, как показано на рисунке 72; введите IP-адрес SSH-сервера 192.168.0.2 в поле «Host Name (or IP address)».

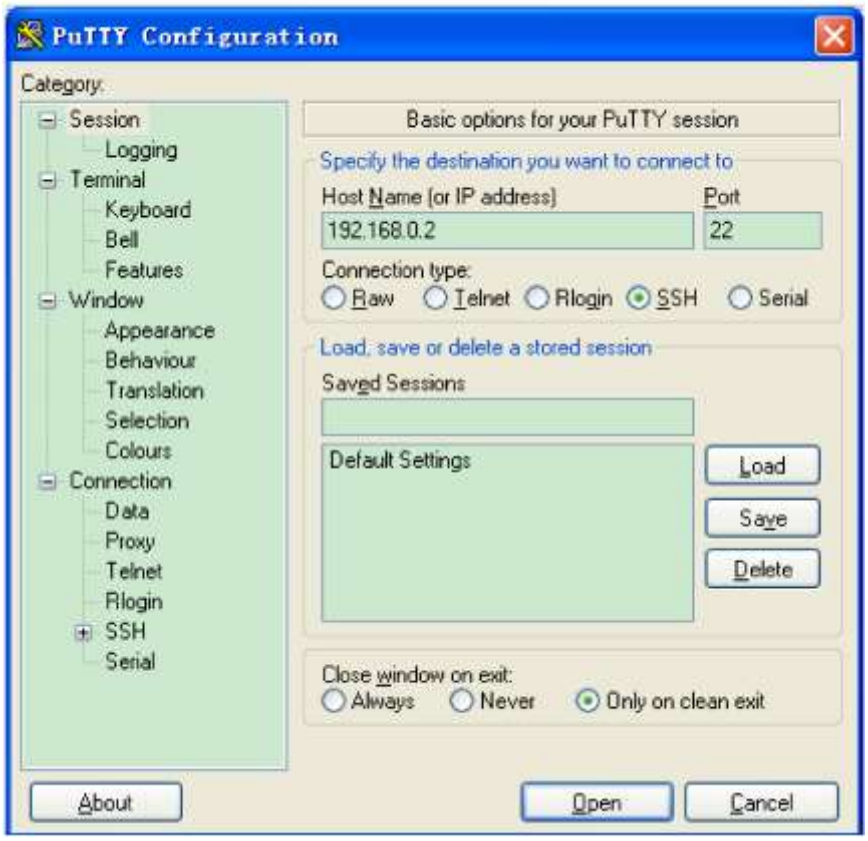


Рисунок 72 – Настройка SSH-клиента

3. Нажмите кнопку <Open>, и появится предупреждающее сообщение, показанное на рисунке 73. Нажмите кнопку <Yes>.

Рисунок 73 – Предупреждающее сообщение

4. Введите имя пользователя «admin» и пароль «123», чтобы войти в интерфейс конфигурации коммутатора, как показано на рисунке 74.

Рисунок 74 – Интерфейс входа в систему (аутентификация SSH)

5.5 TACACS+

5.5.1 Введение

TACACS+ (Terminal Access Controller Access Control System) – протокол аутентификации, авторизации и учета (AAA), который используется для централизованного управления доступом и контроля сетевых устройств. Это система, основанная на TCP. Для передачи данных между сервером сетевого доступа NAS (Network Access Server) и сервером TACACS+ она использует клиент-серверную архитектуру. Клиент функционирует на NAS, а пользовательская информация контролируется на централизованном сервере (см. рисунок 75). NAS является сервером для пользователей, но клиентом для сервера TACACS+.

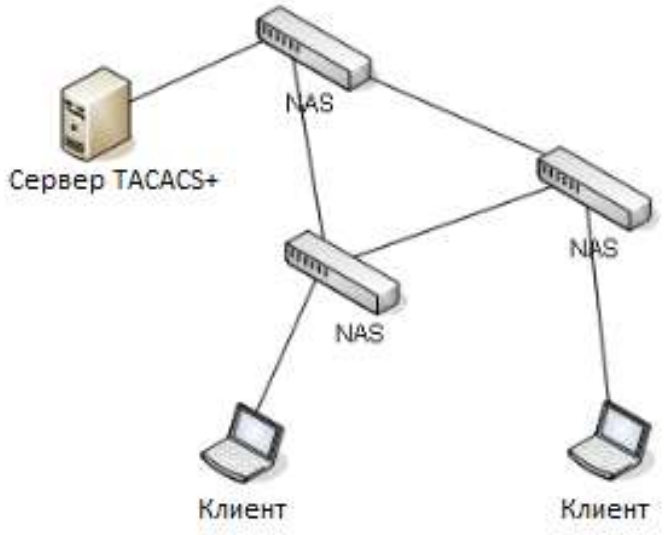


Рисунок 75 – Структура TACACS+

Протокол аутентифицирует, авторизует и управляет терминальными пользователями, которым необходимо заходить на сетевые устройства для каких-либо действий. Устройство работает как клиент TACACS+ и отправляет логин и пароль на сервер TACACS+ для аутентификации. Сервер получает запросы на TCP-соединение, отвечает на запросы аутентификации и проверяет легитимность пользователей. Если пользователь проходит аутентификацию, он может зайти на устройство.

5.5.2 Настройка с помощью WEB-интерфейса

На рисунке 76 показана настройка информации о сервере TACACS+.

Рисунок 76 – Настройка информации о сервере TACACS+

IP Address

Функция: настройка IP-адреса или имени хоста сервера TACACS+. Можно указать максимум 5 серверов TACACS+.

Port

Диапазон: 0–65535

По умолчанию: 49

Функция: настройка порта TCP сервера TACACS+ для аутентификации.

Timeout Period (sec)

Диапазон: 1–1000 с

Функция: настройка дополнительного времени для ответа от сервера TACACS+. После отправки пакета запроса, если устройство по-прежнему не получает ответа от сервера TACACS+ по истечении указанного времени, аутентификация не проходит, и устройство считает данный сервер недействительным.

Share Key

Диапазон: 0–63 символа

Функция: настройка ключа для повышения безопасности связи между клиентом и сервером TACACS+. Две стороны совместно используют ключ для проверки легитимности пакетов. Обе стороны могут получать пакеты друг от друга только тогда, когда ключи одинаковы. Поэтому убедитесь, что локально настроенный ключ совпадает с ключом на сервере TACACS+.

5.5.3 Пример типовой настройки

Как показано на рисунке 77, сервер TACACS+ может аутентифицировать и авторизовать пользователей с помощью коммутатора. IP-адрес сервера – 192.168.0.23, а общий ключ, используемый при обмене пакетами между коммутатором и сервером, – ааа.

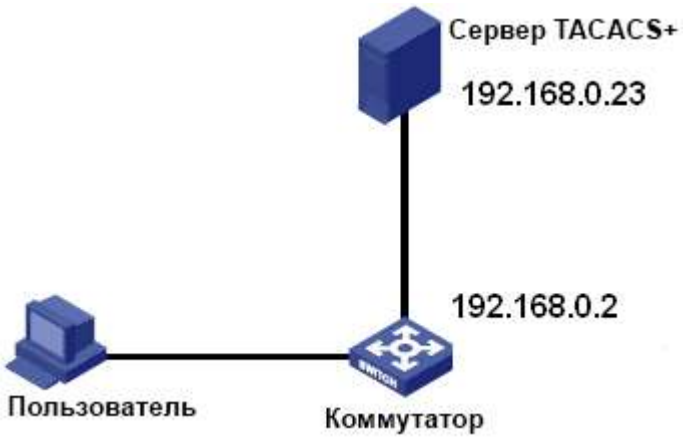


Рисунок 77 – Пример аутентификации TACACS+

1. Настройка сервера TACACS+. Укажите IP-адрес сервера 192.168.0.23 и ключ шифрования «ааа». Включите шифрование, как показано на рисунке 76.

2. При входе на коммутатор через веб-интерфейс выберите «Local», при входе через Telnet выберите «TACACS+», как показано на рисунке 13.

3. Настройте имя пользователя и пароль «bbb» и ключ шифрования «aaa» на сервере TACACS+.

4. При входе на коммутатор через веб-интерфейс введите имя пользователя «admin» и пароль «123», чтобы пройти локальную аутентификацию.

5. При входе на коммутатор через Telnet введите имя пользователя и пароль «bbb», чтобы пройти аутентификацию TACACS+.

5.6 RADIUS

5.6.1 Введение

RADIUS (Remote Authentication Dial-In User Service) – это распределенный протокол обмена информацией. Он определяет формат кадра RADIUS на основе UDP и механизм передачи информации, защищая сети от несанкционированного доступа. RADIUS обычно используется в сетях, требующих высокой безопасности и удаленного доступа пользователей. RADIUS использует режим клиент/сервер для обеспечения связи между NAS (сервером сетевого доступа) и сервером RADIUS. Клиент RADIUS работает на NAS. Сервер RADIUS обеспечивает централизованное управление информацией о пользователях. NAS является сервером для пользователей, но клиентом для сервера RADIUS. На рисунке 78 показана типовая структура.

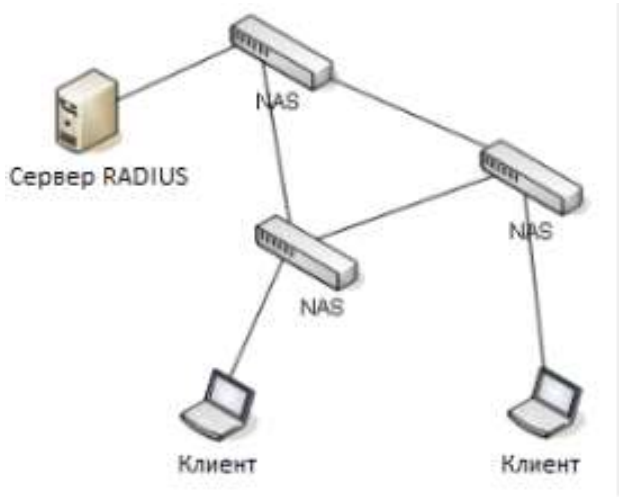


Рисунок 78 – Структура сети RADIUS

Протокол проводит аутентификацию конечных пользователей, которым необходимо авторизоваться в системе устройства для работы. Выступая в качестве клиента RADIUS, устройство отправляет информацию о пользователе на сервер RADIUS для аутентификации и разрешает или запрещает пользователям вход в соответствии с результатами аутентификации.

5.6.2 Настройка с помощью WEB-интерфейса

1. Ниже показана настройка информации о сервере RADIUS.

Рисунок 79 – Настройка информации о сервере RADIUS

IP Address

Функция: настройка IP-адреса или имени хоста сервера RADIUS. Можно указать максимум 5 серверов RADIUS.

Authentication Port

Диапазон: 0–65535

По умолчанию: 1812

Функция: настройка UDP-порта сервера RADIUS для аутентификации.

Accounting Port

Диапазон: 0–65535

По умолчанию: 1813

Функция: настройка UDP-порта сервера RADIUS для учета. Для сообщений аутентификации и учета RADIUS использует разные порты UDP.

Timeout Period (sec)

Диапазон: 1–1000 с

Функция: установка дополнительного времени для ответа от сервера RADIUS. Если по истечении указанного времени после отправки запроса серверу RADIUS от него не будет получен ответ, устройство повторно отправит запрос.

Retransmission Times

Диапазон: 1–1000

Функция: установка максимального количества попыток повторной передачи для пакетов запроса RADIUS. Если устройство по-прежнему не получает ответа от сервера после максимального количества попыток повторной передачи, аутентификация не происходит, и устройство считает сервер RADIUS недействительным.

Secret Key

Диапазон: 0–63 символа

Функция: настройка ключа для повышения безопасности связи между клиентом и сервером RADIUS. Две стороны совместно используют ключ для проверки легитимности

пакетов. Обе стороны могут получать пакеты друг от друга, только если ключи одинаковы. Поэтому убедитесь, что настроенный ключ совпадает с ключом на сервере RADIUS.

Приоритет параметров «Timeout Period», «Retransmission Times» и «Secret Key» в конфигурации сервера RADIUS выше, чем в глобальной конфигурации.

2. Ниже показана глобальная конфигурация RADIUS.

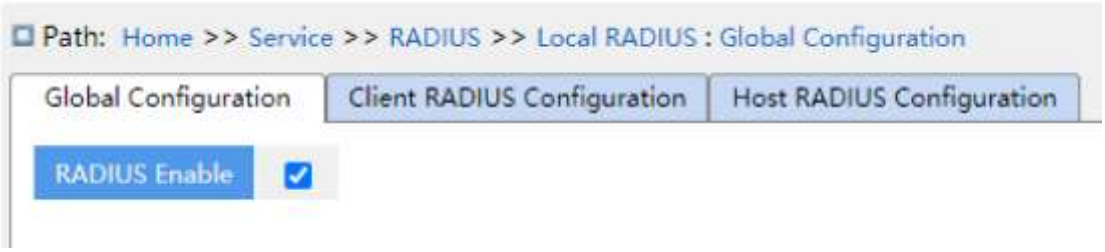


Рисунок 80 – Глобальная конфигурация RADIUS

RADIUS Enable

Варианты настройки: Enable/Disable

По умолчанию: Enable

Функция: указывает, разрешить ли использовать локальный RADIUS другими устройствами в качестве RADIUS-сервера.

3. Ниже показана настройка клиента RADIUS.

Рисунок 81 – Конфигурация клиента RADIUS

NAS-IP

Функция: настройка IP-адреса или диапазона адресов клиента RADIUS.

Mask

Диапазон: 1–32

Функция: настройка сетевого сегмента клиента RADIUS. Для IP-адресов из одного сетевого сегмента следует настраивать только один этот сегмент.

Secret key

Диапазон: 1–63 символа

Функция: настройка общего ключа для проверки подлинности сообщений между устройством и клиентом RADIUS. Сообщения будут приняты и обработаны только в том случае, если ключи совпадают. Поэтому общий ключ, настроенный на устройстве, должен совпадать с ключом, установленным на клиенте RADIUS.

4. Ниже показана настройка хоста RADIUS.

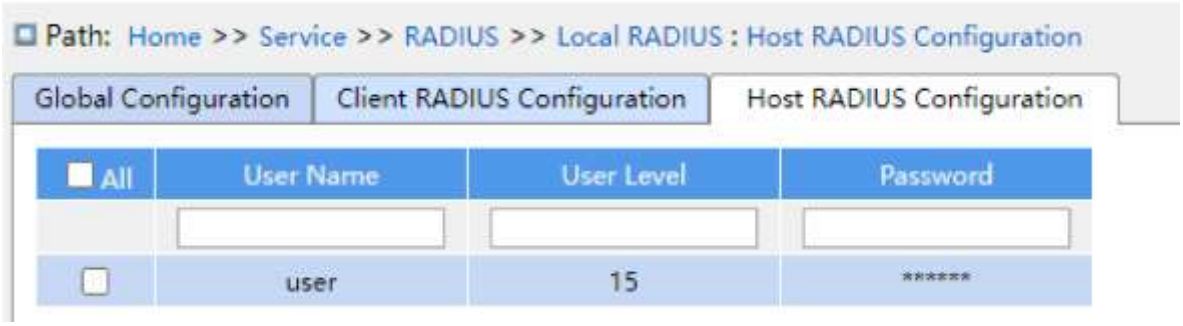


Рисунок 82 – Настройка хоста RADIUS

User Name

Диапазон: 1–31 символ

Функция: настройка имени пользователя RADIUS.

User Level

Диапазон: 1–15

Функция: настройка уровня авторизации пользователя. Пользователи с разными уровнями имеют разные полномочия доступа.

Password

Диапазон: 1–31 символ

Функция: настройка пароля пользователя для входа.

5.6.3 Пример типовой настройки

Как показано на рисунке 83, на порту 1 коммутатора включена работа протокола стандарта IEEE 802.1X. Соответственно, пользователи могут зайти на коммутатор через порт 1 после прохождения аутентификации на сервере RADIUS. IP-адрес сервера 192.168.0.23. Ключ для обмена пакетами между коммутатором и сервером – aaa.

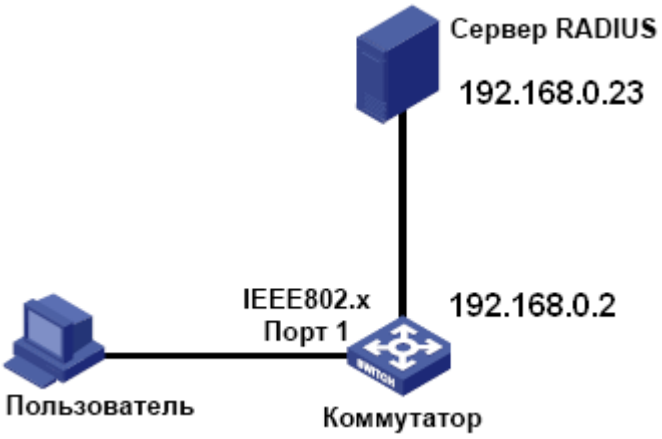


Рисунок 83 – Пример аутентификации RADIUS

1. Установите для IP-адреса сервера аутентификации значение 192.168.0.23 и пароль «aaa», как показано на рисунке 79.

2. Настройки IEEE 802.1X: включите IEEE 802.1X глобально, как показано на рисунке 220.

Выберите административное состояние порта 1 «Port-Based» (см. рисунок 221), оставьте настройки по умолчанию для других параметров.

3. Настройте имя пользователя и пароль на сервере RADIUS «ccc», ключ шифрования – «aaa».

4. Установите и запустите клиентское программное обеспечение 802.1X на ПК. Введите «ccc» в качестве имени пользователя и пароля. После этого пользователь может пройти аутентификацию и получить доступ к коммутатору через порт 1.

5.7 DNS

5.7.1 Введение

DNS (Domain Name System) – это распределенная база данных для приложений TCP/IP, которая обеспечивает преобразование между доменными именами и IP-адресами. С помощью системы доменных имен пользователи могут использовать легко запоминаемые и значимые доменные имена, которые DNS-сервер в сети преобразует в соответствующие IP-адреса.

Разрешение доменных имен делится на статическое и динамическое. В первом случае используется статическая таблица разрешения доменных имен. Система сначала ищет соответствие в этой таблице. Статическое разрешение подразумевает ручное установление соответствия между доменным именем и IP-адресом. Когда пользователь использует доменное имя в приложениях (например, в Telnet), система обращается к статической таблице и получает IP-адрес для указанного доменного имени. Если статическое разрешение не увенчалось успехом, система переходит к динамическому разрешению доменных имен.

5.7.2 Настройка с помощью WEB-интерфейса

1. Включите DNS-прокси, настройте доменное имя.

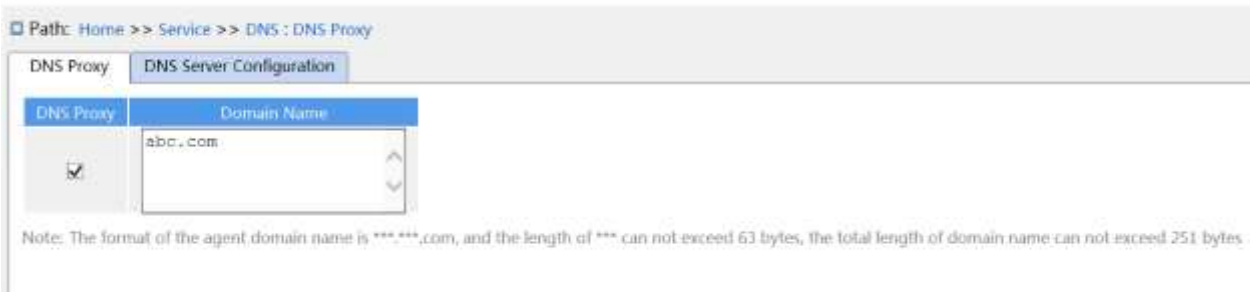


Рисунок 84 – Настройка доменного имени

DNS Proxy

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение DNS-прокси.

Domain Name

Диапазон: формат домена ***.***.com, где длина *** меньше 63 символов, общая длина меньше 251 символа.

По умолчанию: не задано

Функция: если клиент запрашивает доменное имя у сервера и разрешение адреса не удалось, доменное имя с добавленным суффиксом будет повторно отправлено на DNS-сервер для разрешения.

2. Настройка DNS-сервера:

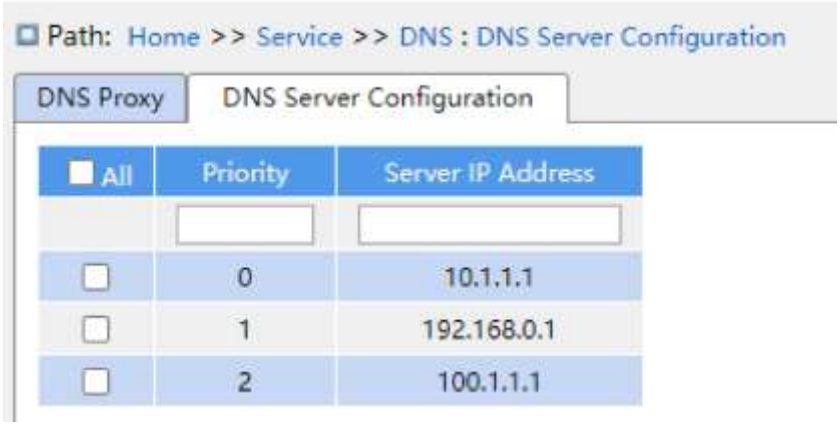


Рисунок 85 – Настройка DNS-сервера

Priority

Диапазон: 0, 1, 2

По умолчанию: не задано

Функция: устройство прокси разрешает адрес, обращаясь к указанным DNS-серверам в порядке приоритета, пока разрешение не будет успешным.

Server IP Address

Формат конфигурации: A.B.C.D

Функция: ручная настройка IP-адреса DNS-сервера.

5.7.3 Пример типовой настройки

Иногда DNS-клиент не может или не должен быть напрямую настроен с адресом DNS-сервера. В этом случае адрес DNS-клиента можно установить напрямую на адрес DNS-прокси, настроив его на коммутаторе. После настройки списка суффиксов доменных имен DNS-прокси автоматически добавит указанный суффикс к доменному имени при повторной отправке запроса на разрешение DNS после неудачного запроса.

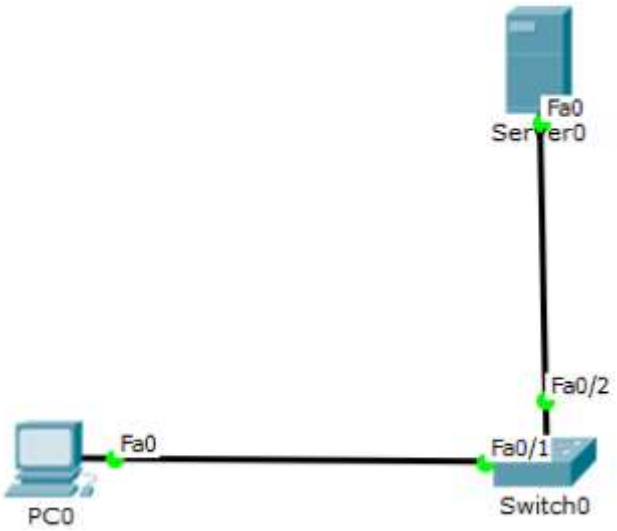


Рисунок 86 – Пример конфигурации DNS-прокси

1. Настройте IP-адрес DNS-сервера на 192.168.0.254/24.
2. Настройте IP-адрес PC0 на 192.168.1.2/24, DNS-сервер — на 192.168.1.1.
3. Настройте интерфейс Fa1/1 на Switch0 в режиме доступа для подключения к VLAN 1, настройте IP-адрес L3 интерфейса на 192.168.1.1/24; интерфейс Fa1/2 также в режиме доступа для подключения к VLAN 2, настройте IP-адрес L3 интерфейса на 192.168.0.1/24.
4. Включите DNS-прокси на Switch0, настройте IP-адрес DNS-сервера на 192.168.0.254, настройте суффикс домена на abc.com. Таким образом, будет реализован DNS-прокси-сервер для разрешения доменных имен.

5.8 RMON

5.8.1 Введение

Основанный на архитектуре SNMP, удаленный мониторинг сети RMON позволяет устройствам управления сетью активно отслеживать управляемые устройства и управлять ими. Сеть RMON обычно включает в себя станцию сетевого управления (NMS) и агентов. NMS управляет агентами, а они собирают статистику по различным типам трафика на своих портах.

RMON в основном выполняет функции сбора статистики и функции сигнализации. С помощью функции статистики агенты могут периодически собирать данные по различным типам трафика на портах, например, количество пакетов, полученных из определенного сегмента сети за определенный период. Функция сигнализации заключается в том, что агенты могут отслеживать значения указанных переменных MIB. Когда значение достигает порога тревоги (например, количество пакетов превышает указанное значение), агент может автоматически записывать тревожное событие в журнал RMON или отправлять trap-сообщение на устройство управления.

5.8.2 Группы RMON

Согласно RFC2819 определяется несколько групп RMON. Устройства данной серии поддерживают группу статистики, группу истории, группу событий и группу сигналов тревоги в общедоступной базе MIB.

- Группа статистики

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

- Группа истории

Группа истории требует, чтобы система периодически производила выборку всех видов трафика на портах и сохраняет значения выборки в таблице записей истории для дальнейшего запроса устройством управления. Группа истории подсчитывает статистические значения всех видов данных в интервале выборки.

- Группа событий

Группа событий используется для определения индексов событий и методов обработки событий. События, определенные в группе, используются для настройки элемента группы сигналов тревоги. Событие инициируется, когда контролируемое устройство достигает установленного состояния тревоги. Система обрабатывает события следующими способами:

Log: регистрирует событие и связанную с ним информацию в таблице журнала событий.

Trap: отправляет trap-сообщение в NMS и информирует NMS о событии.

Log-Trap: регистрирует событие и отправляет trap-сообщение в NMS.

None: никакие действия не выполняются.

- Группа сигналов тревоги

Управление сигнализацией RMON может отслеживать указанные переменные сигналов тревоги. После определения записей сигналов тревоги система получит значения контролируемых переменных этих сигналов за определенный период. Когда значение переменной больше или равно верхнему пределу, срабатывает тревожное событие превышения контролируемого значения. Когда значение тревожной переменной меньше или равно нижнему пределу, срабатывает сигнал о падении значения. Тревоги будут обрабатываться в соответствии с определением события.

Если выборочное значение тревожной переменной несколько раз превышает пороговое значение в одном и том же направлении, то тревожное событие инициируется только в первый раз. Поэтому сигнализация повышения и понижения контролируемого значения генерируется попеременно.

5.8.3 Настройка с помощью WEB-интерфейса

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

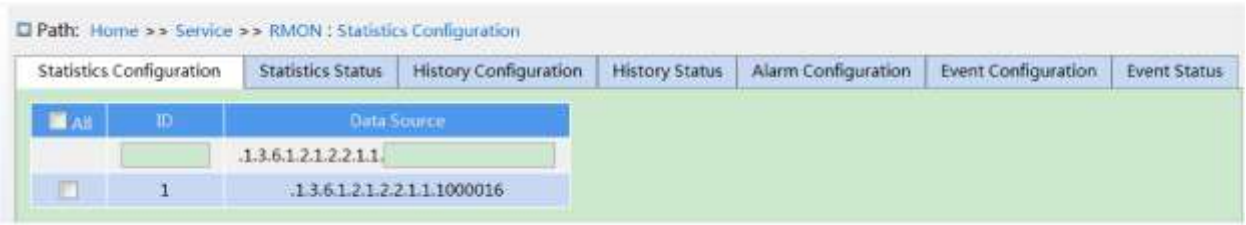


Рисунок 87 – Таблица статистики RMON

ID

Диапазон: 1–65535

Функция: настройка номера записи статистики. Группа статистики может содержать до 128 записей.

Data Source

Варианты настройки: 10000PortID

Функция: выбор порта, статистику которого нужно собирать.

2. На следующем рисунке показано отображение состояния группы статистики.

Рисунок 88 – Статус группы статистики

Drop: количество пакетов, отброшенных портом.

Octets: количество байтов, полученных портом.

Pkts: количество пакетов, полученных портом.

Broadcast: количество широковещательных пакетов, полученных портом.

Multicast: количество многоадресных пакетов, полученных портом.

CRC Errors: количество пакетов с ошибками CRC длиной от 64 до 9600 байт, полученных портом.

Undersize: количество пакетов длиной менее 64 байт, полученных портом.

Oversize: количество пакетов длиной более 9600 байт, полученных портом.

Frag.: количество пакетов с ошибками CRC длиной менее 64 байт, полученных портом.

Jabb.: количество пакетов с ошибками CRC длиной более 9600 байт, полученных портом.

Coll.: количество коллизий, полученных портом в полудуплексном режиме.

64 Bytes: количество пакетов длиной 64 байта, полученных портом.

65~127: количество пакетов длиной от 65 до 127 байт, полученных портом.

128~255: количество пакетов длиной от 128 до 255 байт, полученных портом.

256~511: количество пакетов длиной от 256 до 511 байт, полученных портом.

512~1023: количество пакетов длиной от 512 до 1023 байт, полученных портом.

1024~1588: количество пакетов длиной от 1024 до 1588 байт, полученных портом.

Превышение размера зависит от настройки максимального размера кадра в конфигурации порта (см. раздел 7.1). В приведенном выше примере это значение составляет 9600 байт.

---

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

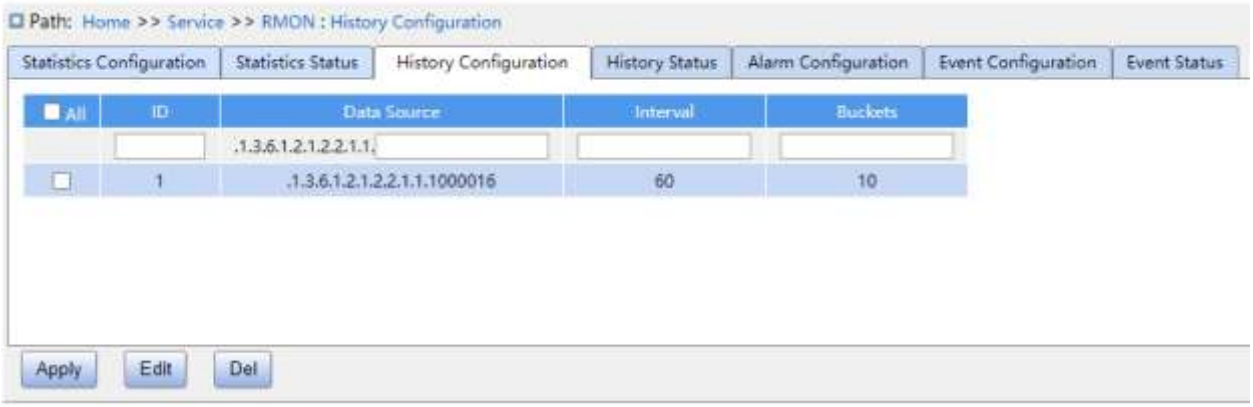


Рисунок 89 – Таблица истории RMON

ID

Диапазон: 1–65535

Функция: настройка номера записи истории. Группа истории может содержать до 256 записей.

Data Source

Параметры конфигурации 10000PortID

Функция: выбор порта, историю которого нужно собирать.

Interval

Диапазон: 1–3600 с

По умолчанию: 1800 с

Функция: настройка периода выборки для порта.

Buckets

Диапазон: 1–65535

По умолчанию: 50

Функция: указывает количество последних значений информационных выборок порта, хранящихся в RMON.

4. На следующем рисунке показано отображение состояния группы истории.

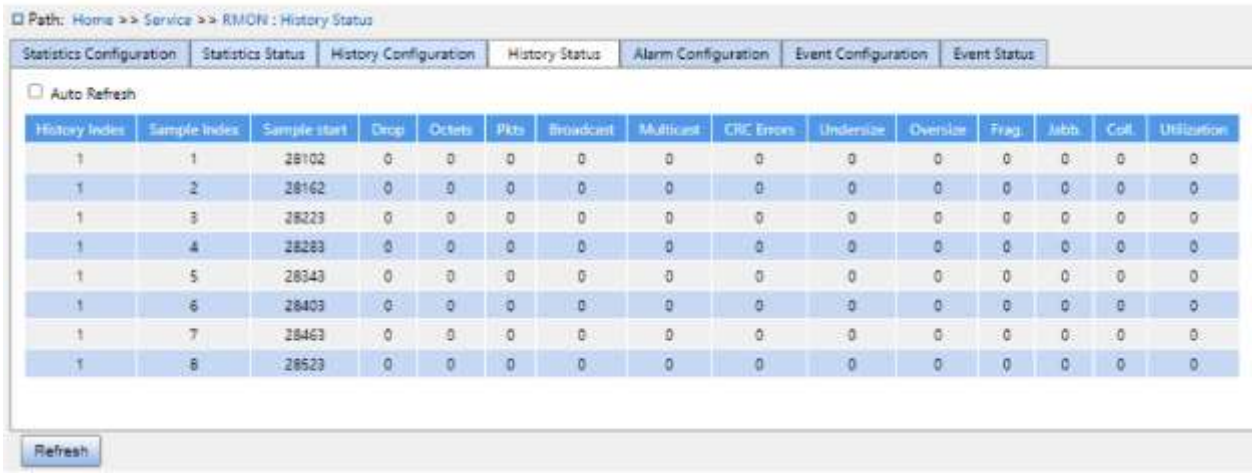


Рисунок 90 – Статус группы истории

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

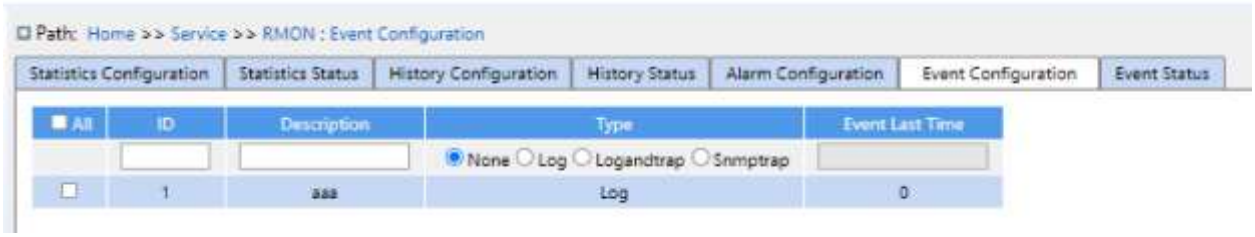


Рисунок 91 – Таблица событий RMON

ID

Диапазон: 1–65535

Функция: настройка номера записи события. Группа истории может содержать до 128 записей.

Description

Диапазон: 1–127 символов

Функция: описание события.

Type

Варианты настройки: None/Log/ Logandtrap /Snmp-Trap

По умолчанию: None

Функция: настройка типа события для сигнализации, то есть режима обработки тревожных событий.

Event Description

Диапазон: 1–127 символов.

Функция: описание события.

Event Last Time

Функция: отображает значение sysUpTime в момент последнего срабатывания определенного события.

6. На следующем рисунке показано отображение состояния группы событий.

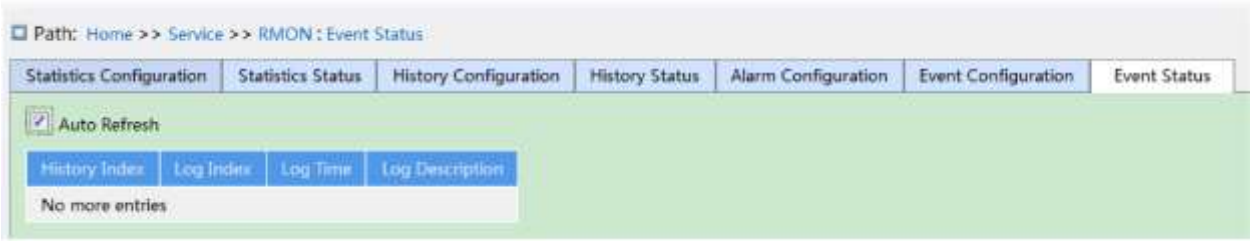


Рисунок 92 – Статус группы событий

7. Настройте таблицу сигналов тревоги, как показано на следующем рисунке.

Рисунок 93 – Таблица сигналов тревоги RMON

ID

Диапазон: 1–65535

Функция: настройка номера записи тревоги. Группа сигналов тревоги может содержать до 256 записей.

Interval

Диапазон: 1–2147483647 с

По умолчанию: 30 с

Функция: настройка периода выборки.

Переменная

Формат конфигурации: A.100000PortID

Диапазон: A=10–21

Функция: выбор информации MIB порта для мониторинга.

InOctets: A=10, количество байтов, полученных портом.

InUcastPkts: A=11, количество одноадресных пакетов, полученных портом.

InNUcastPkts: A=12, количество широковещательных и многоадресных пакетов, полученных портом.

InDiscards: A=13, количество пакетов, отброшенных портом.

InErrors: A=14, количество пакетов с ошибками, полученных портом.

InUnknownProtos: A=15, количество неизвестных пакетов, полученных портом.

OutOctets: A=16, количество байтов, отправленных портом.

OutUcastPkts: A=17, количество одноадресных пакетов, отправленных портом.

OutNUcastPkts: A=18, количество широковещательных и многоадресных пакетов, отправленных портом.

OutDiscards: A=19, количество отброшенных портом исходящих пакетов.

OutErrors: A=20, количество пакетов с ошибками, отправленных портом.

OutQLen: A=21, длина пакетов в выходной очереди порта.

Sample Type

Варианты настройки: Absolute / Delta

По умолчанию: Delta

Функция: выбор метода сравнения значения выборки и порогового значения.

Описание: Absolute: непосредственное сравнение каждого значения выборки с пороговым значением. Delta: значение выборки минус предыдущее значение выборки, затем использование полученной разности для сравнения с пороговым значением.

Startup Alarm

Варианты настройки: Rising / Falling / RisingOrFalling

По умолчанию: RisingOrFalling

Функция: выбор типа сигнала тревоги.

Rising Threshold

Диапазон: 1–2147483647

Функция: настройка верхнего порога. Когда значение выборки превышает пороговое значение и тип сигнала тревоги установлен на Rising или RisingOrFalling, генерируется сигнал тревоги и запускается Rising Index.

Rising Index

Диапазон: 1–65535

Функция: настройка индекса нарастающего события, то есть режима обработки сигналов тревоги переднего фронта.

Falling Threshold

Диапазон: 1–2147483647

настройка нижнего порога. Когда значение выборки опускается ниже порогового значения и тип сигнала тревоги установлен на Falling или RisingOrFalling, генерируется сигнал тревоги и запускается Falling Index.

Falling Index

Диапазон: 1–65535

Функция: настройка индекса спадающего события, то есть режима обработки сигналов тревоги заднего фронта.

6. Тревожная сигнализация

6.1 Введение

Коммутаторы данной серии поддерживают следующие типы сигналов тревоги:

Power Alarm – сигнализация электропитания. Если включена данная функция, сигнализация будет срабатывать в случае проблем с источником питания;

IP/MAC Conflict Alarm – сигнализация конфликта IP- и MAC-адресов. Если функция включена, то при конфликте IP/MAC будет генерироваться сигнал тревоги.

CPU/Memory Availability Alarm – сигнализация использования ЦП/памяти. Если эта функция включена, сигнализация генерируется, когда использование ресурсов процессора или памяти превышает указанный порог.

Port Alarm – сигнализация порта. Если эта функция включена, сигнал срабатывает, когда на порту пропадает связь.

Alarm about PortRate – сигнализация трафика порта. Если эта функция включена, сигнализация генерируется, когда скорость входящего/исходящего трафика порта превышает указанный порог.

Alarm about CRC/Pkt Loss – сигнализация ошибок CRC/потери пакетов. Если эта функция включена, сигнализация генерируется, когда количество ошибок CRC или потерянных пакетов на порту превышает указанный порог.

Alarm about Ring – сигнализация кольцевой сети. Если эта функция включена, сигнализация срабатывает, когда кольцо разомкнуто.

6.2 Настройка с помощью WEB-интерфейса

1. На следующем рисунке показана базовая конфигурация сигнализации.

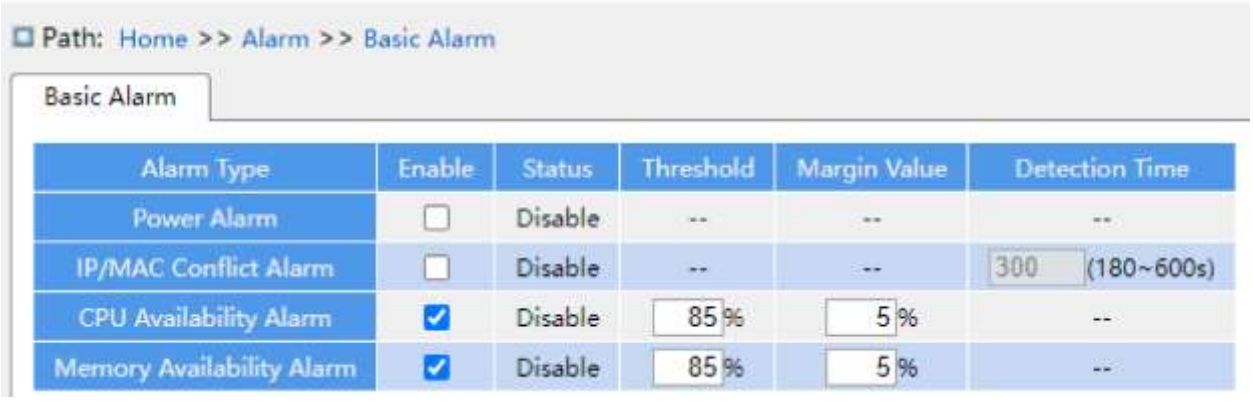


Рисунок 94 – Базовая конфигурация сигнализации

Power Alarm

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение сигнализации по питанию.

Status

Варианты настройки: Normal/Alarm

Функция: отображение состояния сигнализации питания.

Alarm: для устройств с резервным питанием тревога срабатывает в случае, если один из модулей питания выходит из строя или работает ненормально.

Normal: модуль питания или оба модуля (для устройств с резервным питанием) работают нормально.

IP/MAC Conflict Alarm

Варианты настройки: Enable/Disable

По умолчанию: Enable

Функция: включение/отключение сигнализации конфликта IP/MAC.

Status

Варианты настройки: Conflict/No Conflict

Описание: при возникновении конфликта IP/MAC отображается «Conflict»; в противном случае отображается «No Conflict».

Check Time

Диапазон: 180–600 с

По умолчанию: 300 с

Функция: настройка интервала для обнаружения конфликтов IP/MAC.

CPU/Memory Availability Alarm

Варианты настройки: Enable/Disable

По умолчанию: Enable

Функция: включение/отключение сигнализации загрузки процессора/памяти.

Threshold

Диапазон: 50–100%

По умолчанию: 85%

Функция: настройка порогового значения использования процессора/памяти в процентах. Когда загрузка превышает пороговое значение, генерируется сигнал тревоги.

Margin Value

Диапазон: 1–20%

По умолчанию: 5%

Функция: установка значение предела загрузки для процессора/памяти.

Описание: если загрузка процессора или памяти колеблется вокруг установленного порога, могут возникать повторяющиеся срабатывания и сбросы тревог. Чтобы предотвратить эту ситуацию, вы можете задать значение предела (по умолчанию 5%). Тревога будет сброшена только в случае, если загрузка процессора или памяти ниже порога на величину, равную или превышающую заданное значение предела. Например, если порог загрузки памяти установлен на 60%, а значение предела составляет 5%, то тревога не будет срабатывать, если загрузка памяти не превышает 60%. Тревога сработает, если загрузка памяти превысит 60%, и будет сброшена только в том случае, если загрузка станет равной или ниже 55%.

2. Настройка и отображение сигнализации о состоянии связи портов показаны ниже.

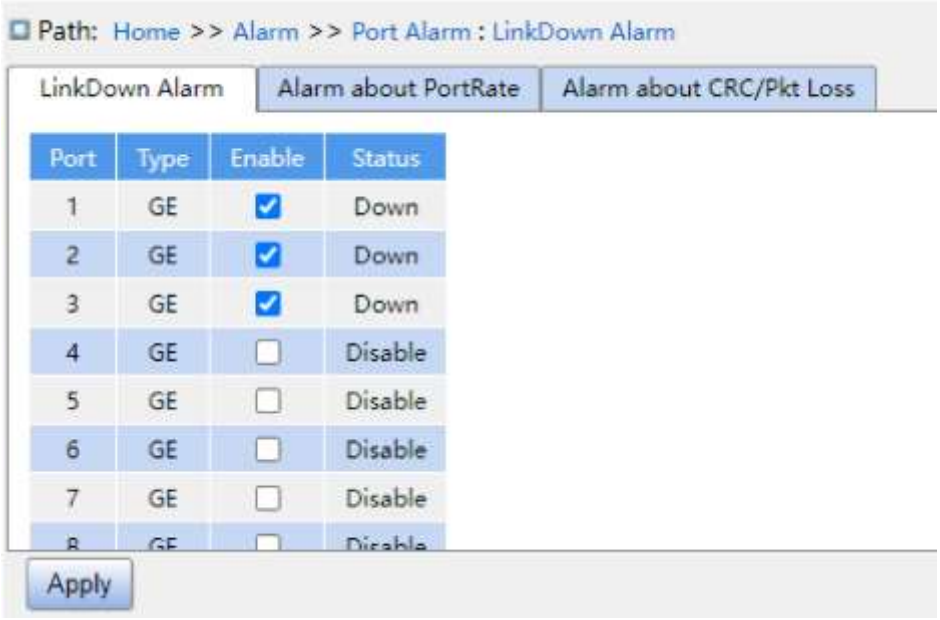


Рисунок 95 – Сигнализация состояния связи

LinkDown Alarm

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение сигнализации состояния связи порта.

Status

Варианты настройки: Up/Down

Описание: «Up» означает, что порт находится в подключенном состоянии и поддерживает нормальную связь.

«Down» означает, что порт отключен или находится в ненормальном состоянии (сбой связи).

3. Настройка и отображение сигнализации о состоянии трафика портов показаны ниже.

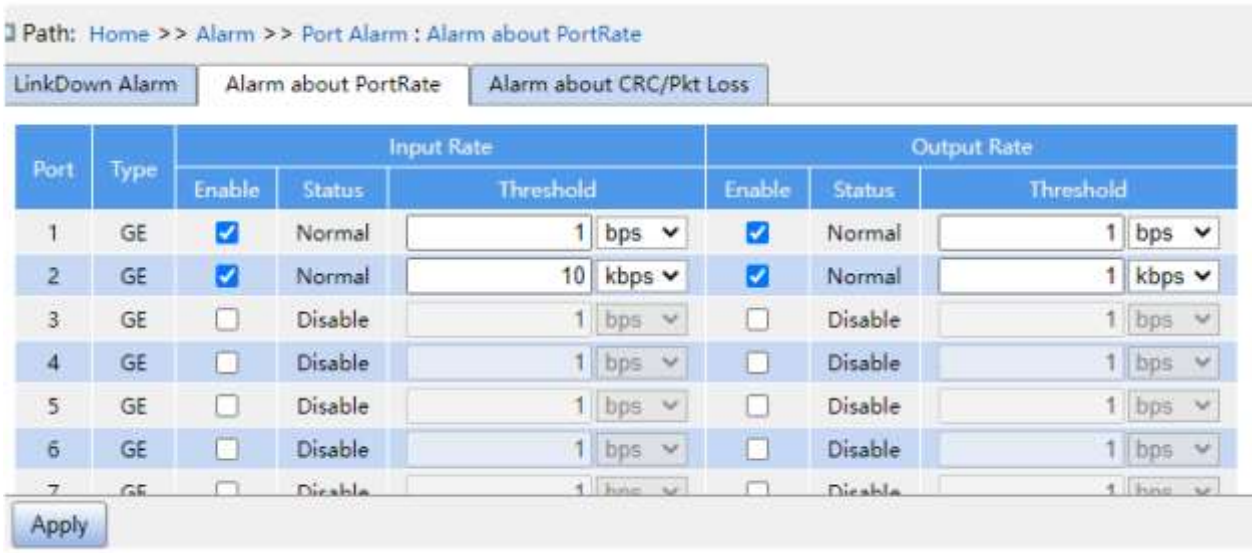


Рисунок 96 – Сигнализация состояния трафика

Input Rate / Output Rate

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение сигнализации состояния входящего/исходящего трафика порта.

Threshold

Диапазон: от 1 до 1000000000 бит/с или от 1 до 1000000 кбит/с.

Функция: настройка порогового значения для трафика порта.

Status

Варианты настройки: Disable/Alarm/Normal

Функция: отображение состояния трафика порта. «Alarm» означает, что скорость входящего/исходящего трафика превышает установленное пороговое значение и вызывает сигнал тревоги.

4. Настройка и отображение сигнализации об ошибках CRC и потере пакетов показаны ниже.

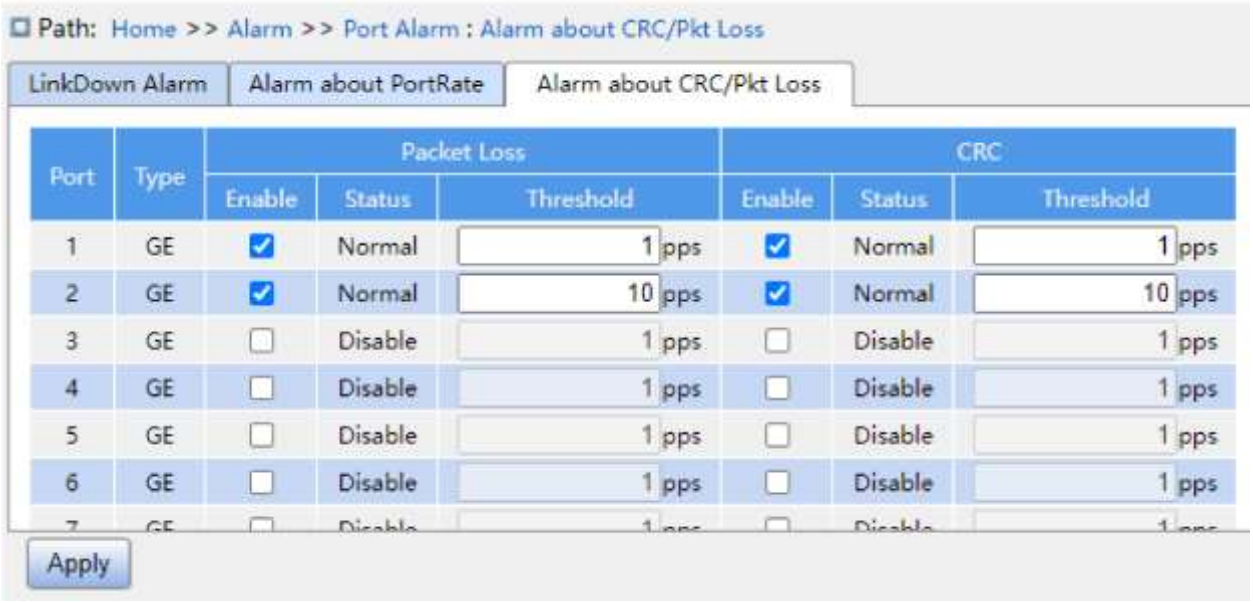


Рисунок 97 – Сигнализации об ошибках CRC и потере пакетов

Packet Loss / CRC

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение сигнализации о потере пакетов или ошибках CRC.

Threshold

Диапазон: от 1 до 1000000 пакетов в секунду

Функция: настройка порогового значения для сигнализации о потере пакетов или ошибках CRC.

Status

Варианты настройки: Disable/Alarm/Normal

Функция: просмотр статуса сигнализации. «Alarm» означает, что количество потерянных пакетов или пакетов с ошибками CRC на порту превышает установленное пороговое значение и вызывает срабатывание тревожной сигнализации.

5. Настройка и отображение сигнализации о неисправностях кольцевой топологии показаны ниже.

Рисунок 98 – Сигнализация кольцевой сети

Alarm About Sy2-RP

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение сигнализации Sy2-RP.

Status

Варианты настройки: Disable/Alarm/---

Функция: просмотр статуса Sy2-RP. «---» означает, что кольцо Sy2-RP замкнуто. «Alarm» означает, что кольцо разомкнуто или работает ненормально.

6. Ниже показаны конфигурация тревожной сигнализации и отображение информации, передаваемой программой измерения входящей оптической мощности на порту SFP.

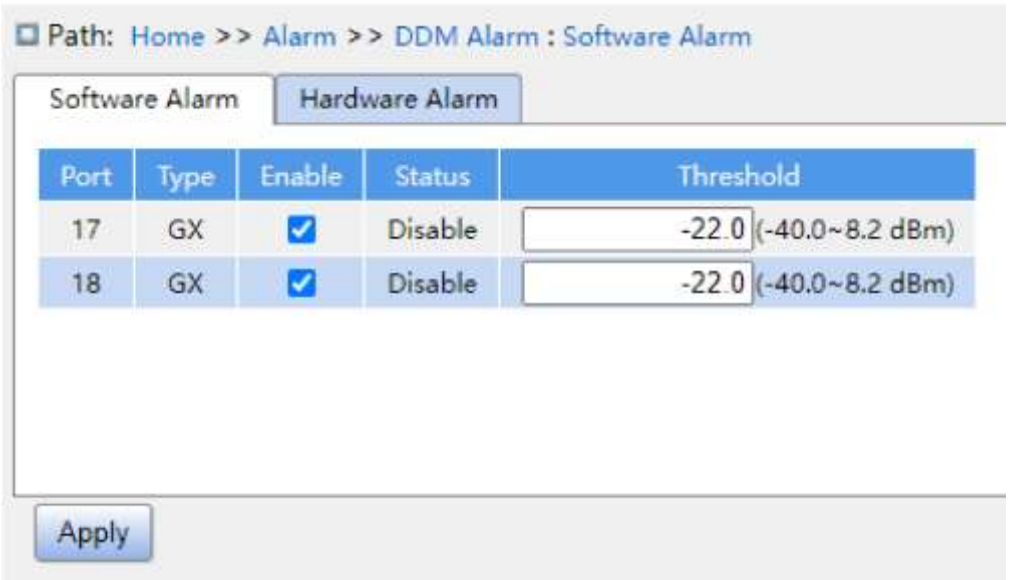


Рисунок 99 – Сигнализация оптической мощности на приемнике SFP

Software Alarm

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение сигнализации об уровне оптического сигнала на приемнике SFP.

Threshold

Диапазон: -400~82 (единица: 0,1 дБм)

По умолчанию: -220 (-22,0 дБм)

Функция: настройка порога для сигнала тревоги об уровне оптического сигнала на приемнике SFP.

Status

Варианты настройки: Disable/Alarm/Normal

Функция: просмотр статуса сигнализации. «Alarm» означает, мощность входного оптического сигнала на порту SFP меньше установленного порога и активирован сигнал тревоги.

7. Настройка и отображение сигнализации о состоянии трансиверов на портах SFP показаны ниже.

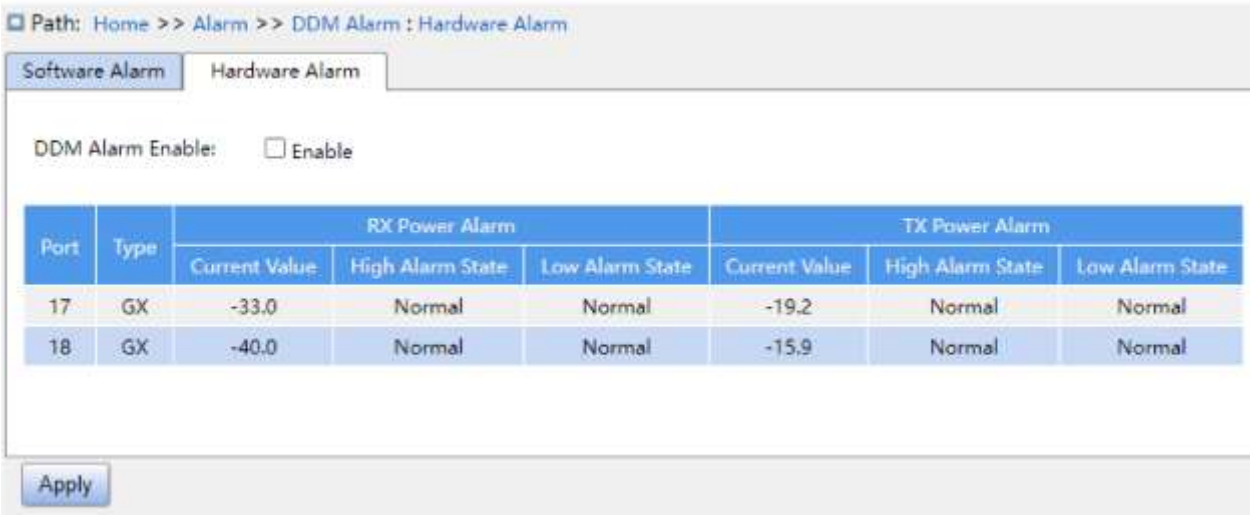


Рисунок 100 – Сигнализация трансиверов

Hardware Alarm

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение сигнализации об уровне оптического сигнала трансивера SFP-порта. Сигнализация спадающего события генерируется, когда контролируемое значение оптической мощности на порту SFP меньше порогового значения низкой оптической мощности; сигнализация нарастающего события

генерируется, когда контролируемое значение оптической мощности на порту SFP превышает пороговое значение высокой оптической мощности.

Пороги низкой и высокой оптической мощности зависят от аппаратного обеспечения и не могут быть настроены программно.

7. Управление функциями

7.1 Настройка портов

1. Ниже показана конфигурация портов, включая состояние, скорость, управление потоком и т. д.

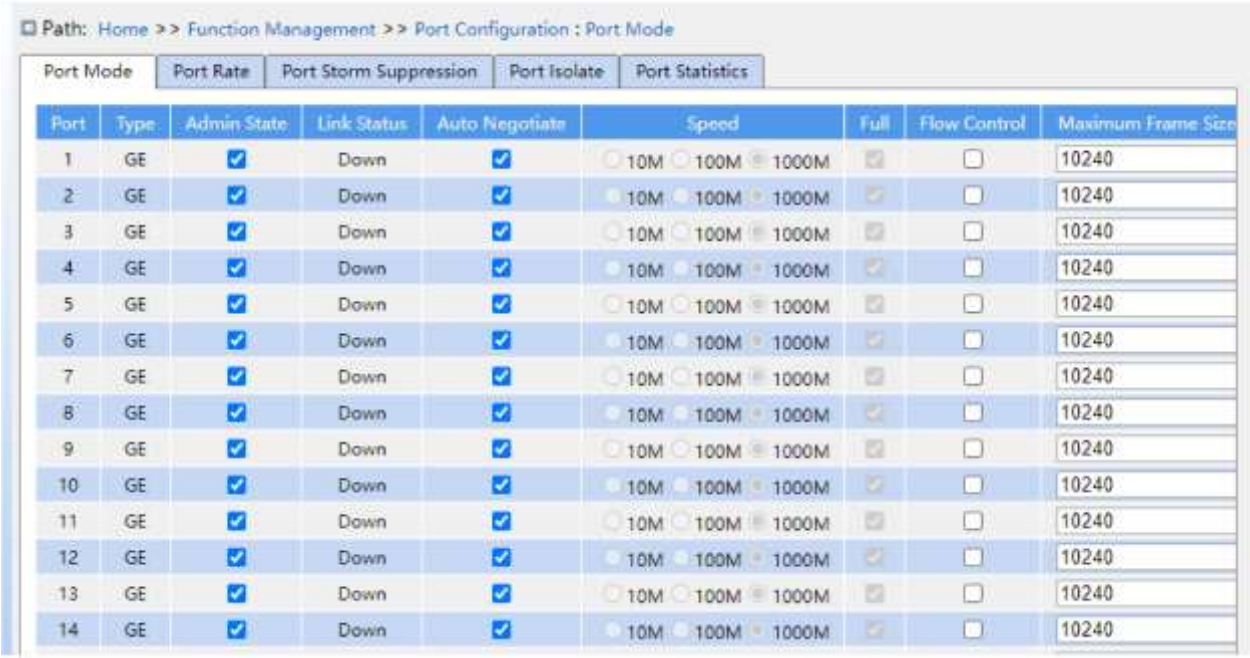


Рисунок 101 – Конфигурация портов

Administration Status

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: указывает, разрешено ли порту передавать данные.

Описание: если включено, порт открыт для передачи данных; если выключено, порт закрыт и данные не передаются. Этот параметр напрямую влияет на аппаратное состояние порта и активирует информацию о событиях для тревожной сигнализации.

Link Status

Варианты настройки: Up/Down

Описание: «Up» означает, что порт находится в подключенном состоянии и поддерживает нормальную связь.

«Down» означает, что порт отключен или находится в ненормальном состоянии (сбой связи).

Auto Negotiate

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: настройка автоматического режима выбора скорости и дуплекса для порта.

Описание: скорость и режим передачи данных для порта поддерживают как автоматическое определение, так и ручную настройку. Если установлен автоматический режим, скорость и режим передачи данных будут определены в соответствии с типом подключения. Рекомендуется включать этот параметр во избежание проблем, возникающих при несовпадении настроек портов с двух сторон соединения. Если вы устанавливаете скорость или duplex-режим на одном из портов соединения вручную, убедитесь, что на другом конце соединения порт имеет те же настройки.

- Гигабитный электрический порт может быть настроен на автосогласование, 10M полный дуплекс, 10M полудуплекс, 100M и 1000M полный дуплекс.
- Оптический порт 10 Gigabit может быть настроен как полнодуплексный 1000M, полнодуплексный 2.5G и полнодуплексный 10G.

Speed

Варианты настройки: 100M/1000M или 10M/100M/1000M или 2.5G или 10G

Функция: настройка автоматически согласуемой скорости порта.

Описание: при включенном автоматическом согласовании скорость порта определяется по умолчанию через процесс согласования с устройством на другом конце соединения. Достигнутая скорость может быть любой из доступных в диапазоне, указанном в параметрах конфигурации. Если вы вручную настроите скорость порта, он сможет согласовывать только выбранную скорость, что позволяет контролировать процесс согласования.

Ручная настройка скорости и дуплексного режима возможна только при отключенной функции «Auto Negotiate».

Full

Варианты настройки: включено/выключено

Функция: настройка режима согласования дуплекса порта.

Описание: полный дуплекс означает, что порт может принимать данные во время отправки данных; полудуплексный порт может либо отправлять, либо получать данные в отдельный момент времени. При включенном автоматическом согласовании режим дуплекса порта определяется по умолчанию через процесс согласования с устройством на другом конце соединения. Достигнутый режим может быть либо полным, либо половинным дуплексом. Если вы вручную настроите режим дуплекса, порт будет согласовывать только выбранный режим, что позволяет контролировать процесс согласования.

Flow Control

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение управления потоком

Описание: после включения управления потоком, если порт получает больше трафика, чем может обработать его кэш, он сообщает отправляющему устройству замедлить скорость передачи данных. Это делается для предотвращения потери пакетов.

Различия в реализации управления потоком:

В режиме полного дуплекса управление потоком осуществляется с помощью специального кадра данных, называемого «pause frame». Когда принимающая сторона решает, что не может обрабатывать больше данных, она отправляет этот кадр отправляющей стороне. После получения кадра «pause frame» отправляющая сторона останавливает передачу данных на время, указанное в кадре.

В режиме полудуплекса управление потоком реализуется по-другому – с использованием механизма «Backpressure». Принимающая сторона может намеренно создать коллизию или сигнал несущей, чтобы сообщить отправляющей стороне о необходимости остановить передачу. Когда отправляющая сторона обнаруживает коллизию или сигнал несущей, она применяет метод «Backoff», который задерживает передачу данных на некоторое время.

Maximum Frame Size

Варианты настройки: 1518–10240 байт

По умолчанию: 10240 байт

Функция: настройка максимально допустимого размера кадра для порта. Кадр, превышающий этот размер, будет отброшен.

2. Ниже показана настройка ограничения скорости портов.

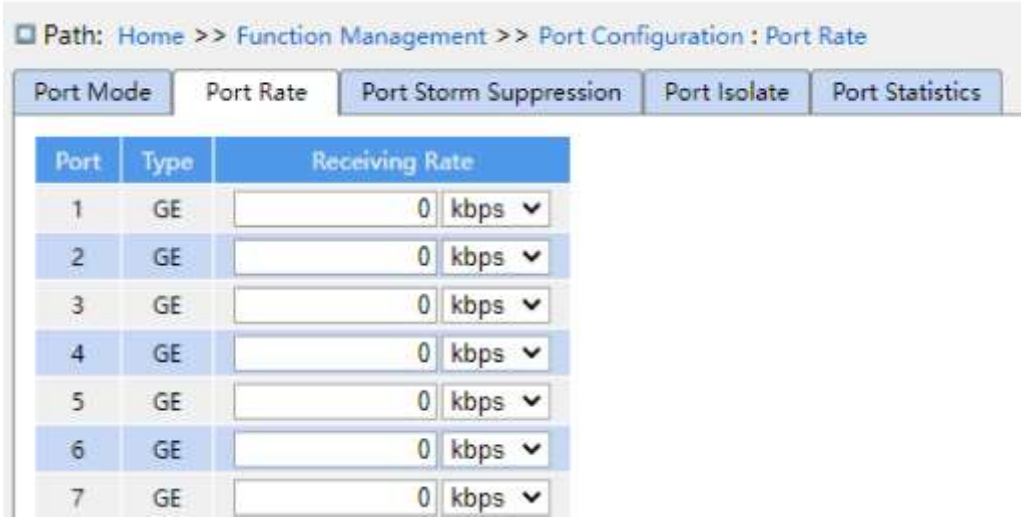


Рисунок 102 – Ограничение скорости портов

Receiving Rate

Параметры настройки: 10–13128147kbps/10–13128147fps/1–13128kfps/1–13128mbps

По умолчанию: 0 (ограничения отключены)

Функция: настройка порога ограничения скорости порта во время приема данных. Сообщения, превышающие указанный порог, будут отброшены.

3. Ниже показана настройка функции подавления штормов на порту.

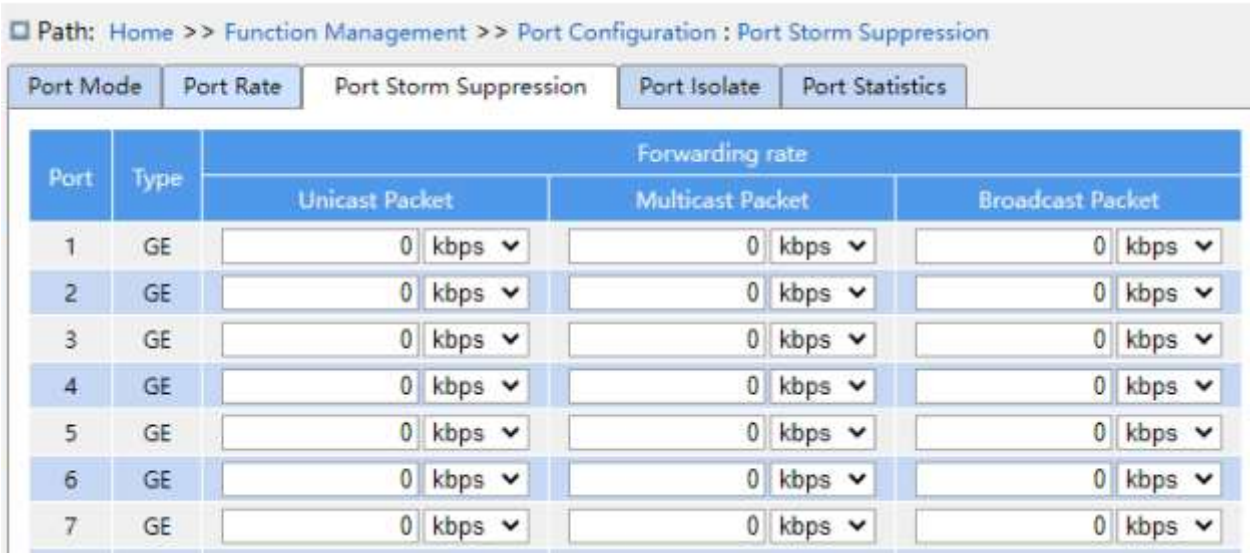


Рисунок 103 – Подавление штормов

Forwarding Rate

Параметры настройки: Unicast Packet/Multicast Packet/Broadcast Packet

Диапазон: 10–13128147kbps/10–13128147fps/1–13128kfps/1–13128mbps

По умолчанию: 0 (ограничения отключены)

Функция: настройка порога ограничения скорости передачи порта. Сообщения, относящиеся к выбранному типу данных и превышающие указанный порог, будут отброшены.

4. Ниже показана настройка функции изоляции портов.

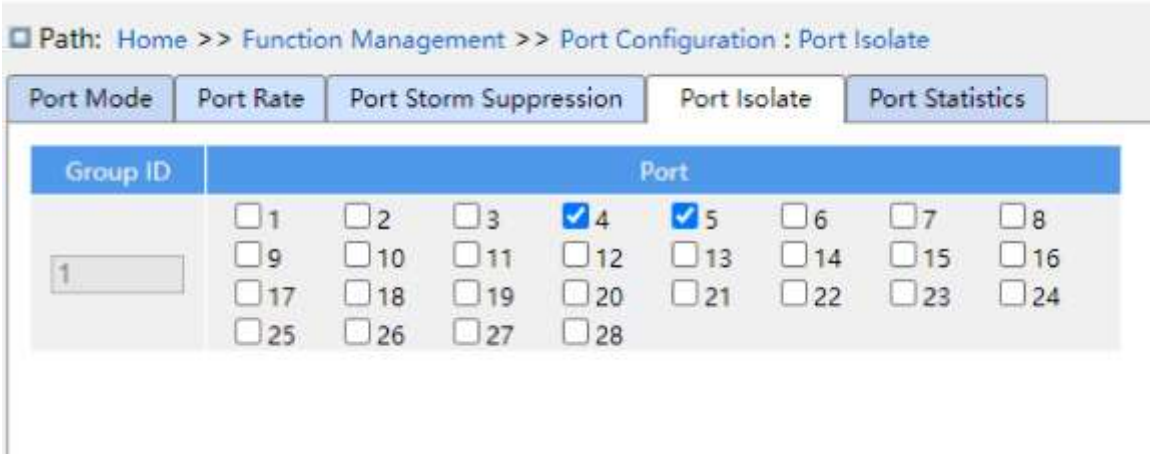


Рисунок 104 – Изоляция портов

Port Isolate

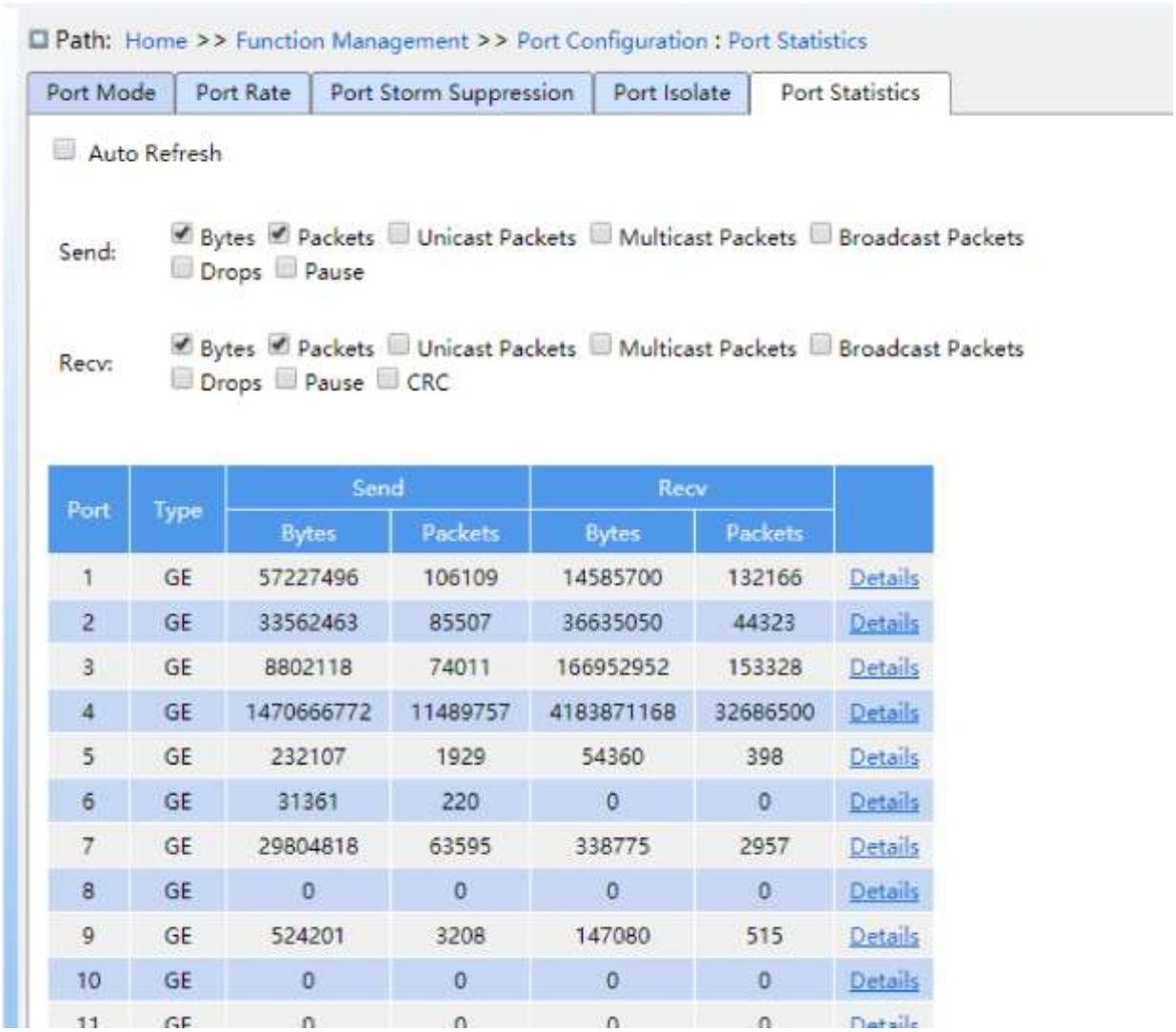
Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение или отключение функции изоляции для выбранного порта.

Примечание: у коммутаторов данной серии существует только одна группа изоляции.

5. Ниже показано отображение статистики портов.



Port	Type	Send		Recv		
		Bytes	Packets	Bytes	Packets	
1	GE	57227496	106109	14585700	132166	Details
2	GE	33562463	85507	36635050	44323	Details
3	GE	8802118	74011	166952952	153328	Details
4	GE	1470666772	11489757	4183871168	32686500	Details
5	GE	232107	1929	54360	398	Details
6	GE	31361	220	0	0	Details
7	GE	29804818	63595	338775	2957	Details
8	GE	0	0	0	0	Details
9	GE	524201	3208	147080	515	Details
10	GE	0	0	0	0	Details
11	GE	0	0	0	0	Details

Рисунок 105 – Статистика портов

Bytes

Подсчет количества полученных/отправленных байтов.

Packets

Подсчет количества полученных/отправленных пакетов.

Unicast Packets

Подсчет количества полученных/отправленных одноадресных пакетов.

Multicast Packets

Подсчет количества полученных/отправленных многоадресных пакетов.

Broadcast Packets

Подсчет количества полученных/отправленных широковещательных пакетов.

Drops

Подсчет количества сообщений, отброшенных из-за конфликтов приема/передачи.

Pause

Подсчет количества полученных/отправленных кадров паузы (pause frame).

CRC

Подсчет количества полученных/отправленных сообщений CRC.

Нажмите «Details» напротив выбранного порта, чтобы войти в интерфейс подробной статистической информации о нем:

Statistics			
Send	Packets		106111
	Bytes		57227701
	Unicast Packets		90323
	Multicast Packets		13897
	Broadcast Packets		1891
	Drops		0
	Pause		0
	Late/Exc.Coll		0
	Length Statistics	64 Bytes	15248
		65~127 Bytes	33153
		128~255 Bytes	10315
		256~511 Bytes	1446
		512~1023 Bytes	24031
		1024~1518 Bytes	21918
		≥1519 Bytes	0
	Queue Statistics	Q0	103194
		Q1	0
		Q2	0
		Q3	0
		Q4	0
		Q5	0
		Q6	0
		Q7	2917
	Packets		132166
	Bytes		14585700
	Unicast Packets		117599
	Multicast Packets		6540
	Broadcast Packets		8027
	Drops		0

Рисунок 106 – Детальная статистика порта

7.2 VLAN

7.2.1 Конфигурация VLAN

7.2.1.1 Введение

Любая локальная сеть (LAN) может быть разделена на несколько логических виртуальных локальных сетей (VLAN). Устройство при этом может обмениваться данными только с устройствами, находящимися с ним в одной VLAN. В результате широковещательные пакеты ограничиваются своей VLAN, а также оптимизируется безопасность локальной сети. Разделение на VLAN не ограничено физическим расположением устройств. Каждая VLAN рассматривается как логическая сеть. Если хосту в одной VLAN необходимо отправить пакеты данных на хост в другой VLAN, должен быть задействован маршрутизатор или коммутатор 3-го уровня.

7.2.1.2 Принцип работы

Чтобы сетевые устройства могли различать пакеты из разных VLAN, в пакеты необходимо добавить поля для идентификации VLAN. В настоящее время наиболее часто используемым протоколом для идентификации VLAN является IEEE802.1Q. В таблице 2 показана структура кадра 802.1Q.

Таблица 2 – Структура кадра 802.1Q

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

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

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

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

CFI: 1 бит. Указывает, инкапсулирован ли MAC-адрес в стандартный формат в различных средах передачи. Значение «0» говорит о том, что MAC-адрес инкапсулирован в стандартный формат, а значение «1» указывает на нестандартный формат.

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

- VLAN 1 – это VLAN по умолчанию, ее нельзя создать или удалить.
- VLAN с зарезервированными номерами нужны для системных функций и также не могут быть созданы или удалены.

Кадр, содержащий заголовок 802.1Q является тегированным; не содержащий – соответственно, нетегированным. В коммутаторе все пакеты несут заголовок 802.1Q.

7.2.1.3 VLAN на основе портов

Разделение на сети VLAN может быть на основе портов или MAC-адресов. Данная серия коммутаторов поддерживает разделение на основе портов. Устройства, принадлежащие определенным VLAN, распознаются в соответствии с портами коммутатора. После добавления порта в указанную VLAN, он может передавать ее тегированные пакеты.

1. Режим порта.

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

Порт доступа (access): в режиме доступа порт может быть добавлен только к одной VLAN. По умолчанию все порты коммутатора являются портами доступа и принадлежат VLAN1. Пакеты, пересылаемые портом доступа, не имеют тегов VLAN. Порты доступа обычно используются для подключения к терминалам, которые не поддерживают 802.1Q.

Магистральный, или транковый порт (trunk): в этом режиме порт может быть добавлен ко многим VLAN. Для него можно указать, требуется ли добавлять тег при отправке пакетов PVID. При отправке других пакетов теги переносятся в обязательном порядке. Такие порты обычно используются для подключения к магистрали сетевых устройств передачи данных, таких как коммутаторы и маршрутизаторы.

Гибридный порт (hybrid): в гибридном режиме порт может быть добавлен ко многим VLAN. Вы можете указать тип пакетов, которые будет получать гибридный порт, и будет ли передаваться тег при отправке пакетов этим портом. Гибридный порт может использоваться для подключения как сетевых, так и пользовательских устройств.

Разница между гибридным и транковым портом заключается в следующем: гибридный порт не передает тег при отправке пакетов из нескольких VLAN, а транковый – только при отправке пакетов PVID.

2. PVID.

Каждый порт имеет PVID (идентификатор VLAN по умолчанию для порта). При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID. По умолчанию PVID всех портов – 1.

- При конфигурации PVID для порта необходимо выбрать один из идентификаторов VLAN, которые разрешены для этого порта. Если не выбрать допустимый VLAN ID, порт может не суметь правильно пересылать пакеты, что приведет к проблемам с передачей данных.
- Когда PVID добавляется к нетегированным пакетам, это позволяет системе идентифицировать, к какой VLAN относится пакет. Важно учитывать настройки PCP (Priority Code Point) и DEI (Drop Eligible Indicator), которые определяют значения по умолчанию для приоритета (PRI) и CFI (Canonical

Format Indicator) порта. Эти параметры помогают управлять приоритетом и форматом пакетов в сети (см. раздел 7.18).

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

Таблица 3 – Различные режимы обработки пакетов

Обработка входящих пакетов		**Обработка исходящих пакетов**	
Нетегированные пакеты	**Тегированные пакеты**	**Режим порта**	**Обработка пакетов**
Добавление тегов PVID к пакетам: ➢ Если PVID есть в списке разрешенных VLAN, пакет принимается ➢ Если PVID отсутствует в списке разрешенных VLAN, пакет отклоняется	➢ Если VLAN ID пакета есть в списке разрешенных VLAN, пакет принимается ➢ Если VLAN ID пакета отсутствует в списке разрешенных VLAN, пакет отклоняется	Access	Пакет пересылается после удаления тега
		Trunk	Пересылка пакетов в соответствии с настройкой «Egress Tagging»: ➢ Untag Port VLAN – если VLAN ID пакета совпадает с PVID и находится в списке разрешенных VLAN, пакет пересылается после удаления тега. Если VLAN ID в пакете отличается от PVID и находится в списке разрешенных VLAN, тег сохраняется и пакет пересылается ➢ Tag All – если VLAN ID пакета находится в списке разрешенных VLAN, тег сохраняется и пакет пересылается
		Hybrid	Пересылка пакетов в соответствии с настройкой «Egress Tagging»: ➢ Untag Port VLAN – аналогично режиму trunk ➢ Tag All – аналогично режиму trunk ➢ Untag All – если VLAN ID

			пакета находится в списке разрешенных VLAN, пакет пересылается после удаления тега

7.2.1.4 Настройка с помощью WEB-интерфейса

1. Ниже показана настройка режима портов.

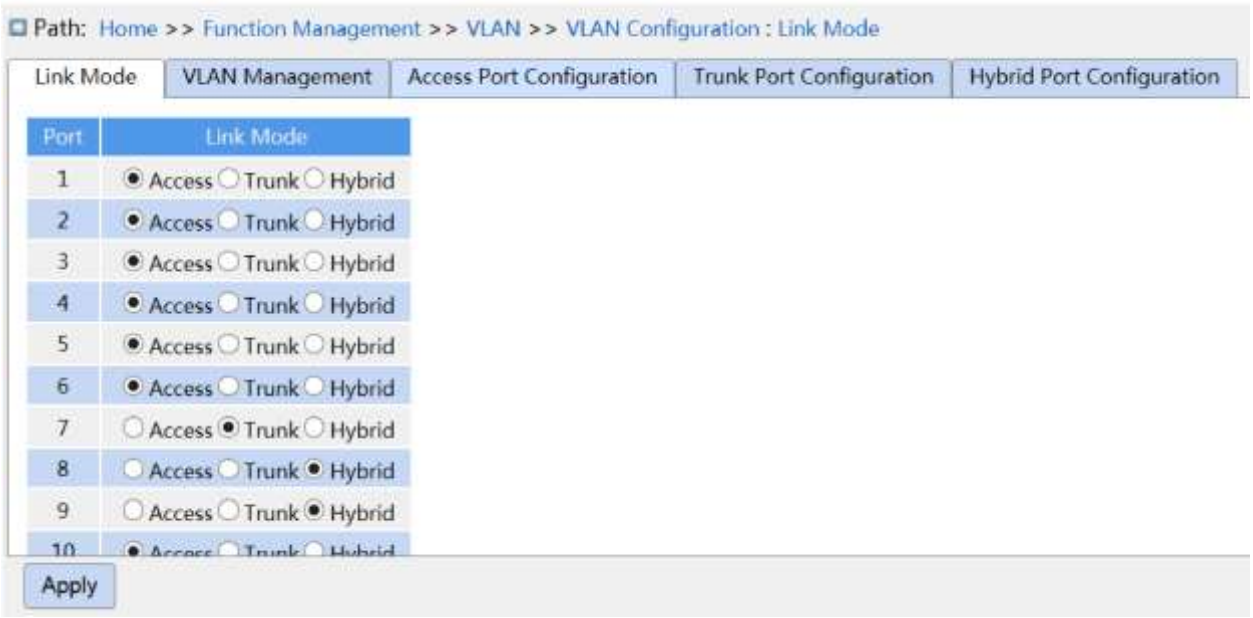


Рисунок 107 – Настройка режима связи

Link Mode

Варианты настройки: Access/Trunk/Hybrid

По умолчанию: Access

Функция: настройка режима обработки тегов для указанного порта.

2. Ниже показано управление VLAN

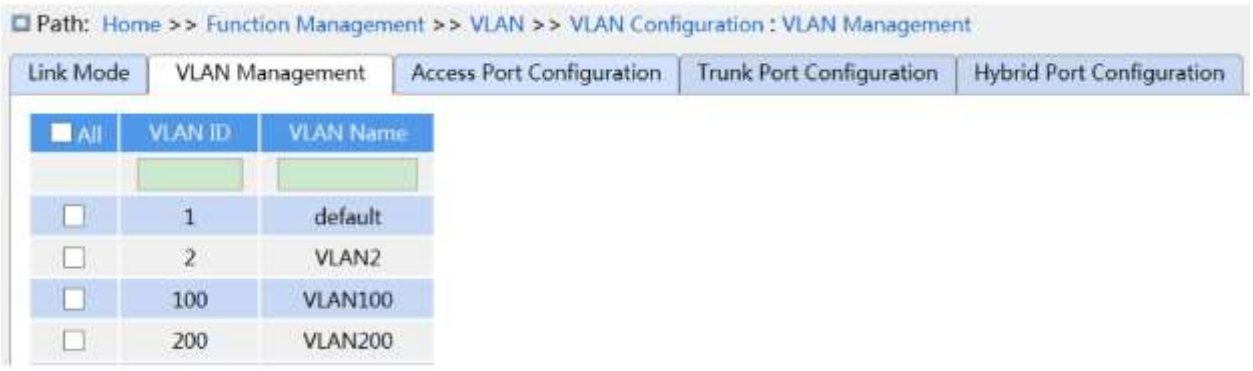


Рисунок 108 – Управление VLAN

VLAN ID

Диапазон: 1–4094

По умолчанию: 1

Функция: создание VLAN.

VLAN Name

Диапазон: 1–32 символа, включая заглавные буквы, строчные буквы, цифры и подчеркивания.

Функция: настройка имени VLAN.

3. Ниже показана настройка порта доступа.

Рисунок 109 – Настройка порта доступа

PVID

Диапазон: 1–4094

По умолчанию: 1

Функция: настройка VLAN по умолчанию для порта доступа.

VLAN необходимо создать до настройки VLAN ID порта доступа. Это правило относится и к портам других типов.

---

3. Ниже показана настройка магистрального порта.

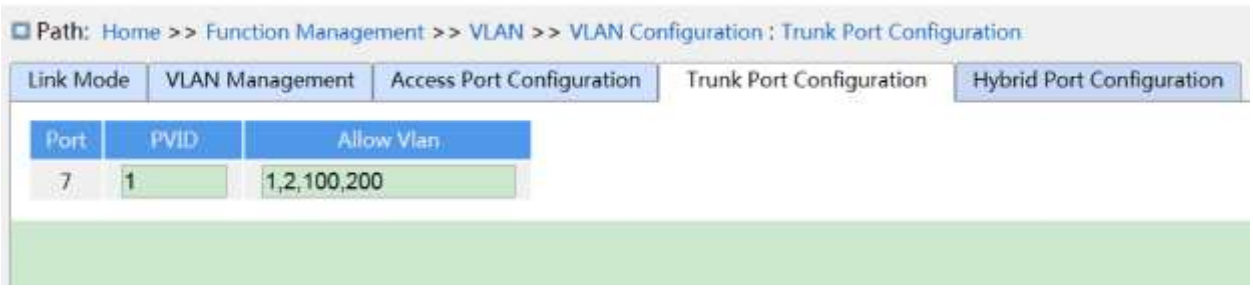


Рисунок 110 – Настройка магистрального порта

PVID

Диапазон: 1–4094

По умолчанию: 1

Функция: настройка VLAN по умолчанию для транкового порта.

Allow VLAN

Диапазон: 1–4094, разделенные запятой «,» и дефисом «-» (M-N, M должно быть меньше N), например: 2, 33, 34-77.

По умолчанию: 1

Функция: настройка разрешенных VLAN для транкового порта.

4. Ниже показана настройка гибридного порта.

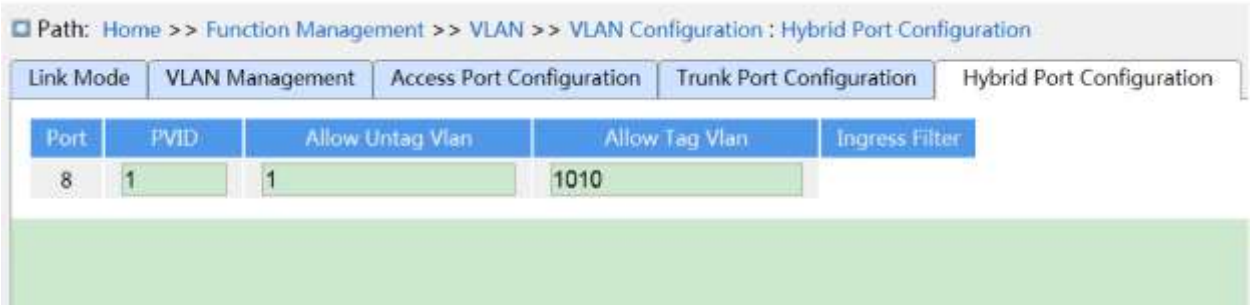


Рисунок 111 – Настройка гибридного порта

PVID

Диапазон: 1–4094

По умолчанию: 1

Функция: настройка VLAN по умолчанию для гибридного порта.

Allow Untag VLAN

Диапазон: 1–4094, разделенные запятой «,» и дефисом «-» (M-N, M должно быть меньше N), например: 2, 33, 34-77.

По умолчанию: 1

Функция: настройка разрешенных нетегированных VLAN для гибридного порта.

Allow Tag VLAN

Диапазон: 1–4094, разделенные запятой «,» и дефисом «-» (M-N, M должно быть меньше N), например: 2, 33, 34-77.

По умолчанию: не задано

Функция: настройка разрешенных тегированных VLAN для гибридного порта.

7.2.1.5 Пример типовой настройки

Как показано на рисунке 112, вся локальная сеть разделена на 3 VLAN: VLAN2, VLAN100 и VLAN200. Требуется, чтобы устройства в одной VLAN могли взаимодействовать друг с другом, но разные VLAN были изолированы. Конечные ПК не могут различать тегированные пакеты, поэтому порты, соединяющие коммутатор А и коммутатор В с ПК, настроены в режиме «Access». Пакеты VLAN2, VLAN100 и VLAN200 должны передаваться между коммутаторами А и В, поэтому порты, соединяющие коммутаторы, должны быть настроены в режиме «Trunk», что позволит пропускать пакеты VLAN 2, VLAN 100 и VLAN 200. В таблице 4 показана соответствующая конфигурация.

Таблица 4 – Настройка VLAN

VLAN	**Настройка**
VLAN2	Порты 1 и 2 коммутаторов А и В в режиме Access, а порт 7 в режиме Trunk
VLAN100	Порты 3 и 4 коммутаторов А и В в режиме Access, а порт 7 в режиме Trunk
VLAN200	Порты 5 и 6 коммутаторов А и В в режиме Access, а порт 7 в режиме Trunk

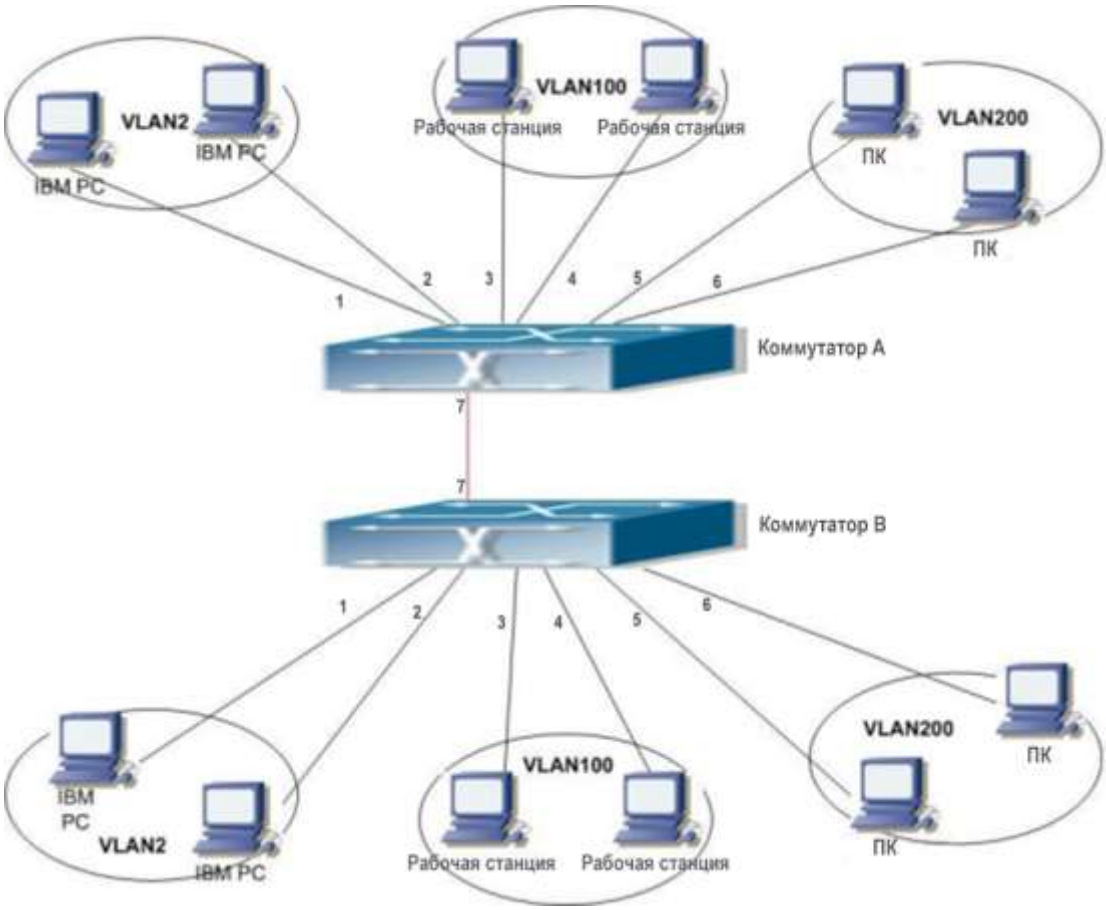


Рисунок 112 – Схема VLAN

Настройка коммутаторов A и B

1. Настройте разрешенные VLAN доступа на 1,2,100,200, как показано на рисунке 108.

2. Настройте порты 1, 2 как порты доступа, укажите PVID 2. Настройте порты 3, 4 как порты доступа, укажите PVID 100. Настройте порты 5, 6 как порты доступа, укажите PVID 200, как показано на рисунке 109. Настройте порт 7 как транковый, укажите PVID 1, разрешенные VLAN как 1,2,100,200, как показано на рисунке 110.

3. Для остальных параметров оставьте значения по умолчанию.

7.2.2 GMRP

7.2.2.1 Протокол GARP

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

Благодаря GARP, информация о настройках коммутатора может быть передана по всей локальной сети. Объекты GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путем отправки соответствующих Join и Leave-сообщений.

GARP предусматривает три типа сообщений: Join, Leave и LeaveAll.

- Когда объект GARP хочет передать свои настройки другим коммутаторам, он отсылает Join-сообщение. Join-сообщения бывают двух типов: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для зарегистрированного свойства, в то время как JoinEmpty – для свойства, которое еще не было зарегистрировано.
- Когда объект GARP хочет удалить свои настройки с других коммутаторов, он отправляет сообщение Leave.
- После запуска объекта GARP, он начинает отсчитывать период LeaveAll. Когда период заканчивается, объект отсылает сообщение LeaveAll.

Объект GARP означает порт, на котором включен протокол GARP.

Для работы GARP использует таймеры Hold, Join, Leave и LeaveAll.

Таймер Hold. При получении сообщения о регистрации настроек, объект GARP не отправляет сообщение Join сразу, а запускает таймер Hold. Когда таймер заканчивает отсчет, объект отправляет все сообщения о настройках, полученные за этот период в одном Join-сообщении, что уменьшает количество передаваемых по сети данных.

Таймер Join. Для того, чтобы убедиться, что Join-сообщения получены другими объектами, после отправки сообщения Join объект GARP запускает таймер Join. Если за период до истечения установленного срока в ответ не получено JoinIn-сообщение, объект отправляет Join-сообщение снова. В противном случае, сообщение Join не отправляется.

Таймер Leave. Если объект GARP хочет удалить информацию об атрибуте, он отсылает Leave-сообщение. Объект, получивший это сообщение, запускает таймер Leave. Если он не получает ни одного Join-сообщения до истечения таймера, он удаляет информацию о данном атрибуте.

Таймер LeaveAll. При старте объекта GARP, запускается таймер LeaveAll. По его истечении, объект отправляет LeaveAll-сообщение для того, чтобы другие объекты GARP перерегистрировали все атрибуты. После этого объект запускает таймер LeaveAll заново.

7.2.2.2 Описание GVRP

GVRP (GARP VLAN Registration Protocol) является приложением GARP и основан на механизме работы GARP для поддержания динамической информации о регистрации VLAN на устройстве и распространения этой информации на другие устройства.

Устройство с включенным GVRP может получать информацию о регистрации VLAN от других устройств и динамически обновлять локальную информацию о регистрации VLAN. Кроме того, устройство может распространять локальную информацию о регистрации VLAN на другие устройства, обеспечивая согласованность информации о VLAN на всех устройствах в одной локальной сети. Информация о регистрации VLAN, распространяемая с помощью GVRP, включает как статическую информацию о регистрации, настроенную вручную, так и динамическую информацию о регистрации от других устройств.

GVRP и Port Chanel являются взаимоисключающими. На порту агрегации нельзя включать GVRP, а порт GVRP нельзя добавлять в группу агрегации.

7.2.2.3 Настройка с помощью WEB-интерфейса

1. Включите глобально протокол GVRP и настройте таймер, как показано ниже.

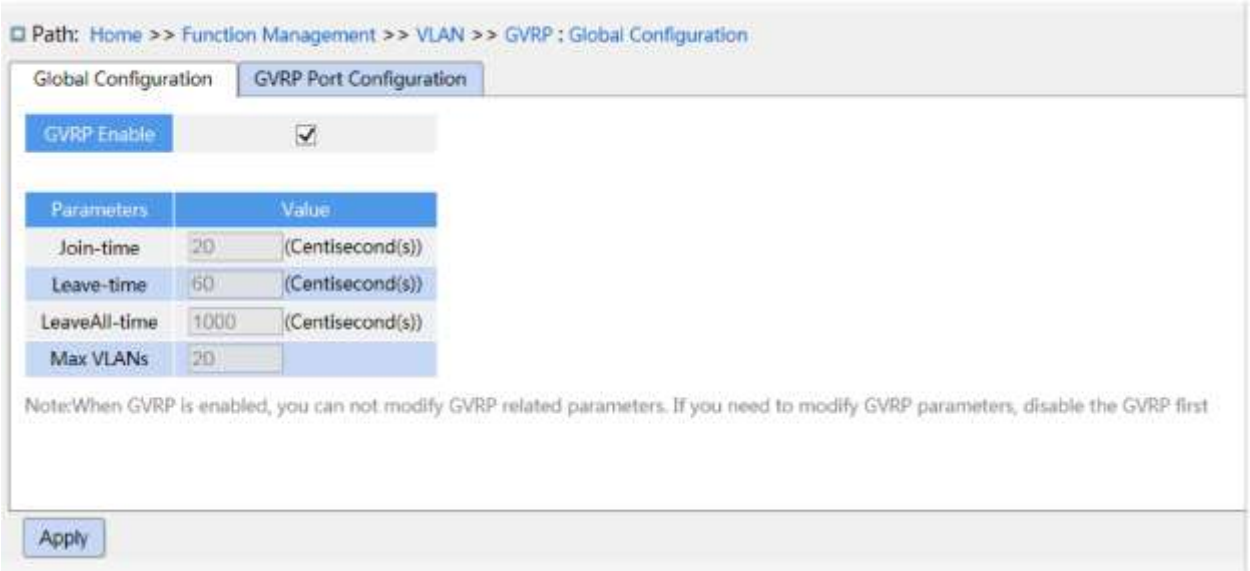


Рисунок 113 – Глобальная настройка GVRP

GVRP enable

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение протокола GVRP.

Join-time

Варианты настройки: 1–20 сантисекунд

По умолчанию: 20 сантисекунд

Функция: настройка значения таймера Join.

Leave-time

Варианты настройки: 60–300 сантисекунд

По умолчанию: 60 сантисекунд

Функция: настройка значения таймера Leave.

LeaveAll-time

Варианты настройки: 1000–5000 сантисекунд

По умолчанию: 1000 сантисекунд

Функция: настройка значения таймера LeaveAll.

Описание: таймер LeaveAll используется для управления временем, в течение которого устройство ожидает перед отправкой LeaveAll-сообщений. Если таймер LeaveAll истекает одновременно на нескольких устройствах, это может привести к одновременному отправлению нескольких LeaveAll-сообщений, что увеличивает количество ненужных сообщений в сети. Чтобы избежать этой ситуации, фактическое значение таймера LeaveAll устанавливается случайным образом в пределах до 1.5 раз от установленного значения LeaveAll. Это помогает распределить время отправки LeaveAll сообщений между устройствами, снижая вероятность их одновременной отправки и тем самым уменьшая нагрузку на сеть.

Max VLANs

Диапазон: 1–4094

По умолчанию: 20

Функция: настройка максимального количества VLAN, которые порт GVRP может зарегистрировать динамически.

Отключите GVRP перед настройкой таймера и максимального количества VLAN.

---

2. Ниже показана настройка портов GVRP

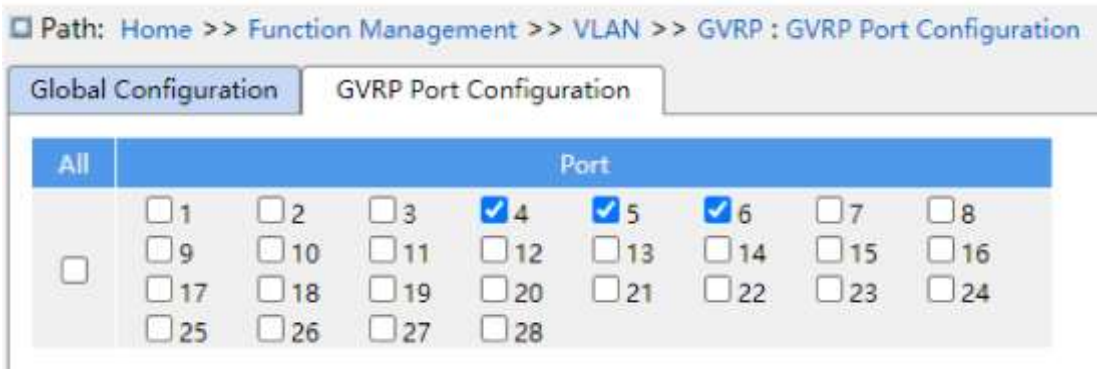


Рисунок 114 – Выбор портов GVRP

Port

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение/отключение протокола GVRP на портах.

7.2.2.4 Пример типовой настройки

Как показано на рисунке 115, GVRP необходимо включить на устройствах, чтобы информация VLAN динамически регистрировалась и обновлялась между коммутатором A и коммутатором B.

Рисунок 115 – Схема подключения устройств GVRP

Настройка коммутатора A:

1. Настройте порт 1 как транковый, в поле «Allow VLAN» укажите 1.
2. Включите глобальный GVRP, как показано на рисунке 113.
3. Включите GVRP на порту 1, как показано на рисунке 114.

Настройка коммутатора B:

1. Настройте порт 4 как транковый, в поле «Allow VLAN» укажите 1; настройте порт 5 как порт доступа, в поле «PVID» укажите 5; настройте порт 6 как транковый, в поле «Allow VLAN» укажите 1,6.
2. Включите глобальный GVRP, как показано на рисунке 113.
3. Включите GVRP на портах 4, 5, 6, как показано на рисунке 114.

Порт 1 коммутатора A может регистрировать ту же информацию VLAN, что и порты 5 и 6 коммутатора B.

7.2.3 PVLAN

7.2.3.1 Введение

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

Верхняя VLAN – это VLAN общего домена, в которой порты являются портами восходящей линии связи. Нижние сети VLAN представляют собой изолированные домены, в которых порты являются портами нисходящей линии связи. Порты нисходящей линии связи могут быть назначены разным изолированным доменам, и они могут одновременно взаимодействовать с портом восходящей линии связи. Изолированные домены не могут взаимодействовать друг с другом.

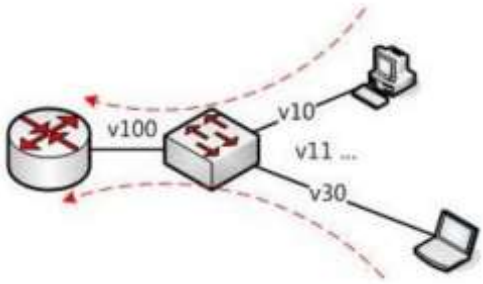


Рисунок 116 – Схема PVLAN

Как показано на рисунке 116, общим доменом является VLAN 100, а изолированными доменами – 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 VLAN 100, но устройства в изолированных доменах не могут устанавливать соединение друг с другом, например, VLAN 10 не может связываться с VLAN 30.

7.2.3.2 Пояснение

Функция PVLAN может быть реализована посредством специальной настройки портов.

- PVID портов восходящей линии связи совпадает с VLAN ID домена общего пользования; PVID портов нисходящей линии связи совпадает с VLAN ID их собственного изолированного домена.
- Порты восходящей линии связи настроены на гибридный режим и назначены VLAN домена общего пользования и всем доменам изоляции; порты нисходящей линии связи настроены на гибридный режим и назначены VLAN общего домена и собственному изолированному домену.
- Пакеты, отправляемые портами-участниками PVLAN, являются немаркированными.

7.2.3.3 Настройка с помощью WEB-интерфейса

1. Ниже показана настройка портов восходящей связи.

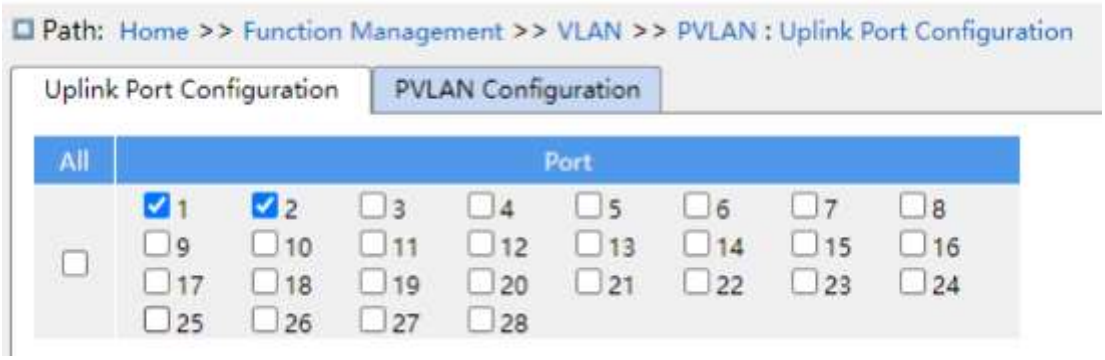


Рисунок 117 – Выбор uplink-портов

Port

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: выбор портов восходящей линии.

2. Ниже показана настройка PVLAN.

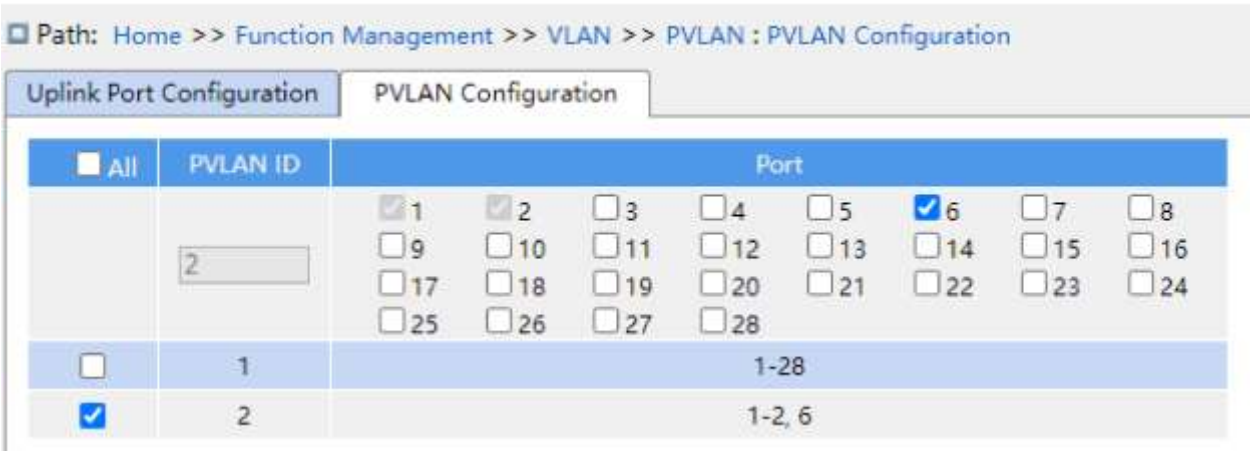


Рисунок 118 – Настройка PVLAN

PVLAN ID

Варианты настройки: 1–4094

По умолчанию: 1

Функция: настройка PVLAN ID для портов.

Port

Варианты настройки: включено/выключено

По умолчанию: 1-28

Функция: выбор портов PVLAN.

7.2.3.4 Пример типовой настройки

На рисунке 119 показан пример настройки PVLAN. VLAN 300 является общим доменом, а порт 1 и порт 2 – портами восходящей линии связи. VLAN 100 и VLAN 200 являются изолированными доменами, а порты 3, 4, 5 и 6 – портами нисходящей линии связи.

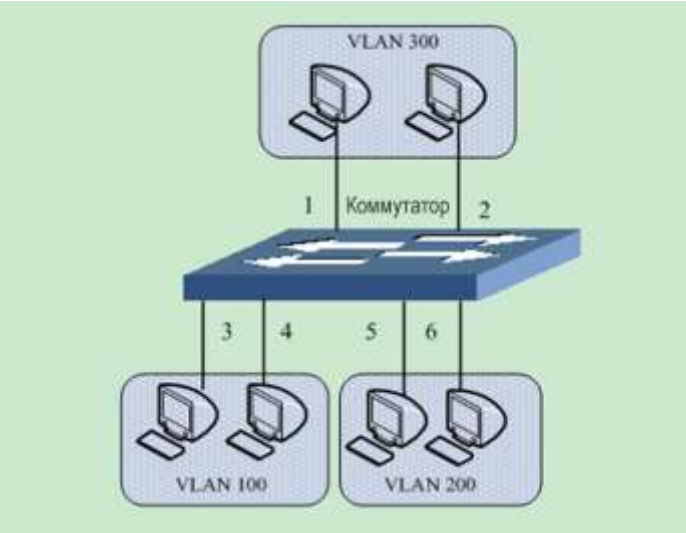


Рисунок 119 – Пример настройки PVLAN

Настройка коммутатора:

1. Настройте порты 1, 2 как гибридные порты, укажите PVID 300, установите маркировку исходящего трафика на «Untag All», разрешенные VLAN на 100,200,300.

2. Настройте порты 3, 4 как гибридные порты, укажите PVID 100, установите маркировку исходящего трафика на «Untag All», разрешенные VLAN на 100,300.

3. Настройте порты 5, 6 как гибридные порты, укажите PVID 200, установите маркировку исходящего трафика на «Untag All», разрешенные VLAN на 200,300.

4. Оставьте все остальные параметры по умолчанию.

7.2.3.5 Статус VLAN

Проверьте состояние портов VLAN, как показано ниже.

Рисунок 120 – Статус VLAN

7.3 Конфигурация IP

7.3.1 Настройка IP-адреса

1. Просмотр IP-адреса коммутатора через консольный порт

Войдите в CLI коммутатора через консольный порт. Выполните команду **show interface vlan 1** в привилегированном режиме, чтобы просмотреть IP-адрес коммутатора, как показано на рисунке 121.

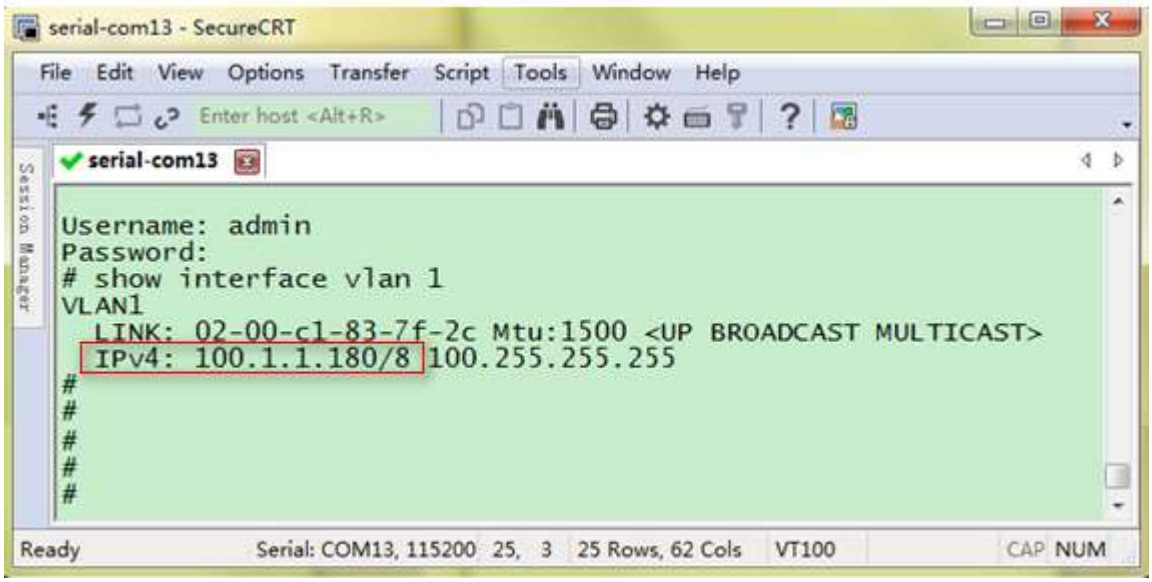


Рисунок 121 – Отображение IP-адреса

2. Создание IP-интерфейса

Устройства в разных VLAN не могут напрямую общаться друг с другом. Для передачи их коммуникационных пакетов требуется маршрутизатор или коммутатор уровня 3, который будет использовать IP-интерфейс.

Эта серия коммутаторов поддерживает IP-интерфейсы, которые представляют собой виртуальные интерфейсы уровня 3, используемые для связи между VLAN. Вы можете создать один IP-интерфейс для каждой VLAN. Этот интерфейс предназначен для пересылки пакетов уровня 3, поступающих с портов данной VLAN.

3. Настройка основного IP-адреса

Основной IP-адрес коммутатора можно получить путем ручной настройки и автоматически, как показано ниже.

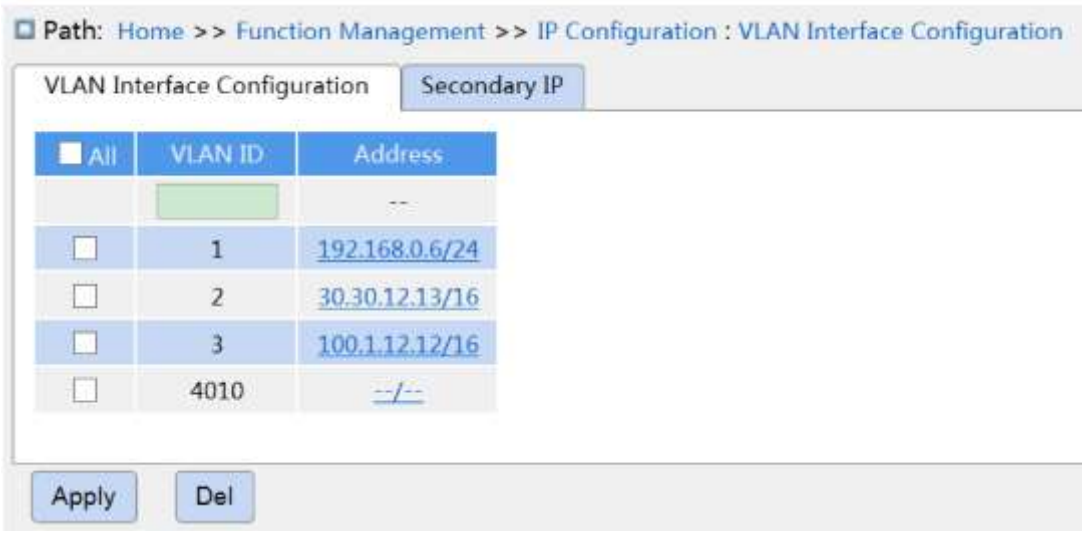


Рисунок 122 – Настройка интерфейса VLAN

VLAN ID

Функция: только порт-участник соответствующей VLAN сможет получить доступ к текущему IP-интерфейсу.

Address

Функция: IP-адрес и маска, полученные интерфейсом VLAN.

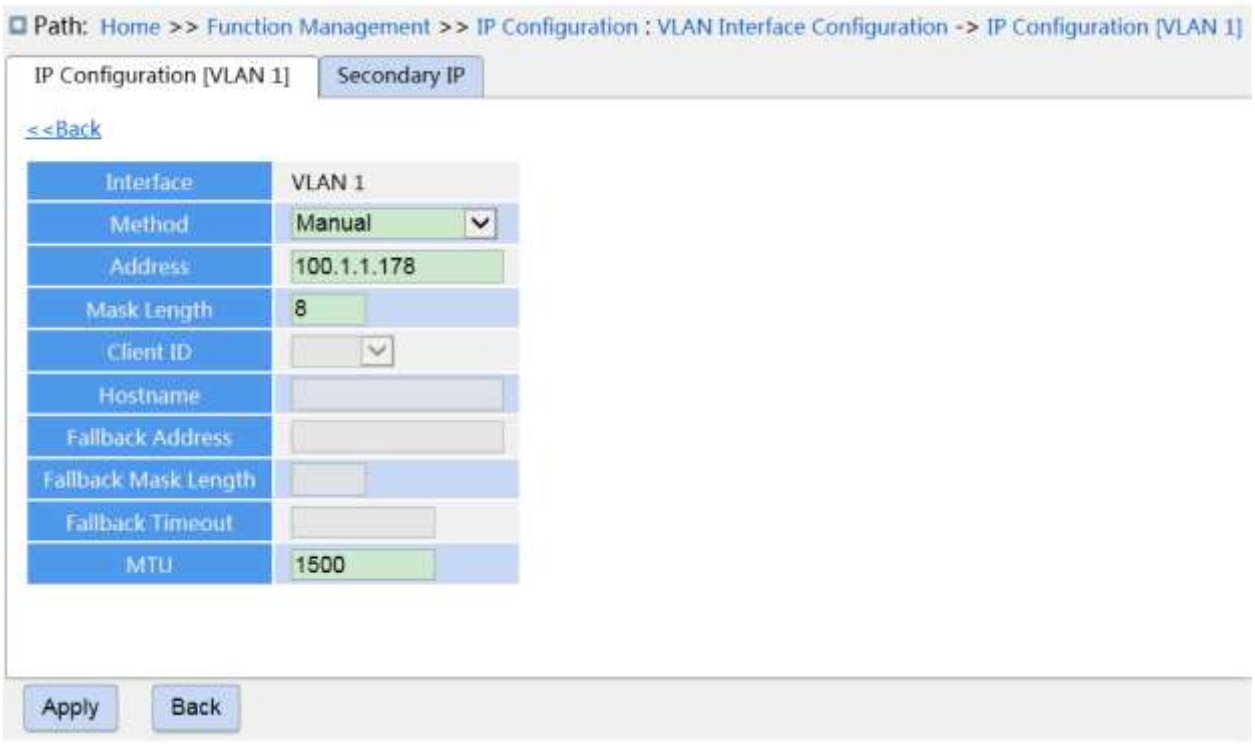


Рисунок 123 – Настройка IP-адреса

Method

Варианты настройки: None/DHCP/Manual

Функция: при выборе «Manual» вам необходимо вручную настроить IP-адрес и маску подсети. Если выбрать «DHCP», коммутатор автоматически получит IP-адрес через протокол DHCP как DHCP-клиент. В этом случае в сети должен присутствовать DHCP-сервер для назначения IP-адреса и маски подсети клиенту.

Address

Формат конфигурации: A.B.C.D

Функция: IP-адрес интерфейса VLAN.

Mask Length

Функция: маска подсети – это 32-битное число, состоящее из последовательности единиц и нулей. Последовательности единиц обозначают поля сетевого номера и номера подсети, в то время как последовательности нулей соответствуют полю номера хоста. Длина маски определяется количеством единиц.

Client ID

Варианты настройки: Hex/ASCII/Port

Функция: Содержит детализированную информацию, заполненную в поле option 61, когда указанный IP-адрес отправляет запрос DHCP.

Hex: заполнение поля option 61 с типом 01 и MAC-адресом.

ASCII: заполнение поля option 61 с типом 00 и строкой.

Port: заполнение поля option 61 соответствующим MAC-адресом интерфейса.

Hostname

Диапазон: 0–63 символа

Функция: настройка имени хоста интерфейса VLAN.

Fallback Address

Формат конфигурации: A.B.C.D

Функция: после того как интерфейс VLAN получает через протокол DHCP IP-адрес с истекшим временем, этот адрес устанавливается в качестве резервного.

Fallback Mask Length

Функция: маска подсети – это 32-битное число, состоящее из последовательности единиц и нулей. Последовательности единиц обозначают поля сетевого номера и номера подсети, в то время как последовательности нулей соответствуют полю номера хоста. Длина маски определяется количеством единиц.

Fallback Timeout

Диапазон: 0–4294967295 с

Функция: если значение ненулевое, то коммутатор будет пытаться получить IP-адрес через протокол DHCP в течение заданного времени. В это время необходимо вручную настроить IP-адрес. После истечения времени попытки начинает действовать IP-адрес, настроенный вручную. Если значение равно нулю, коммутатор будет продолжать попытки получения IP-адреса через протокол DHCP до успешного завершения, и вручную настраивать IP-адрес не требуется.

MTU

Диапазон: 68–9600

По умолчанию: 1500

Функция: настройка максимальной длины пакета, который может пройти на уровне IP.

4. Настройка вторичного IP

Вручную настройте вторичный адрес IP-интерфейса коммутатора, как показано ниже.

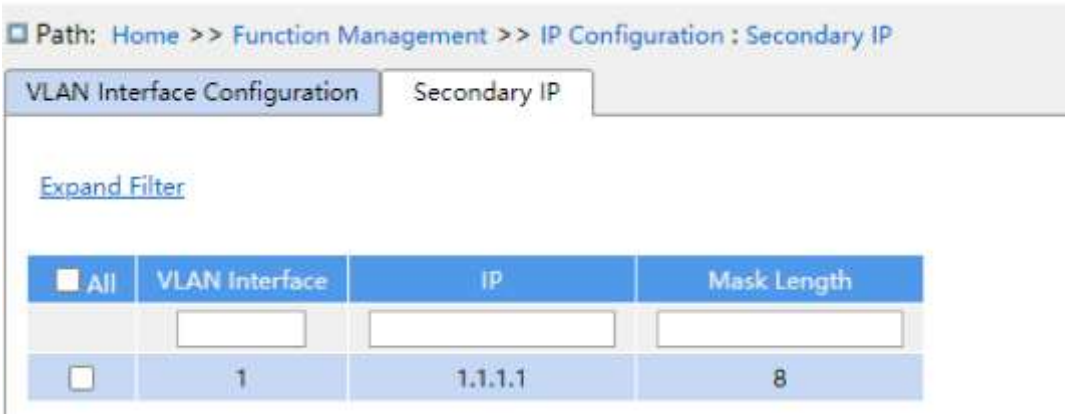


Рисунок 124 – Настройка вторичного IP-адреса

VLAN Interface

Функция: только порт-участник соответствующей VLAN сможет получить доступ к текущему IP-интерфейсу.

IP

Формат конфигурации: A.B.C.D

Функция: ручная настройка IP-адреса.

Mask Length

Функция: маска подсети – это 32-битное число, состоящее из последовательности единиц и нулей. Последовательности единиц обозначают поля сетевого номера и номера подсети, в то время как последовательности нулей соответствуют полю номера хоста. Длина маски определяется количеством единиц.

- Каждый IP-интерфейс соответствует первичному IP-адресу и может соответствовать нескольким вторичным IP-адресам.
- Различные IP-интерфейсы должны быть настроены с первичными и вторичными IP-адресами для различных сегментов сети.

7.4 Агрегация портов

7.4.1 Статическая агрегация

7.4.1.1 Введение

Технология агрегирования (Port Channel) предназначена для объединения группы физических портов с одинаковой конфигурацией в один логический порт для увеличения пропускной способности и повышения скорости передачи. Порты-участники одной группы совместно используют трафик и служат друг для друга динамическими резервными копиями, повышая надежность соединения.

7.4.1.2 Реализация

Как показано на рисунке 125, три порта на коммутаторах A и B объединяются, образуя один агрегированный канал Port Channel. Пропускная способность такого канала – это общая пропускная способность входящих в него трех портов.

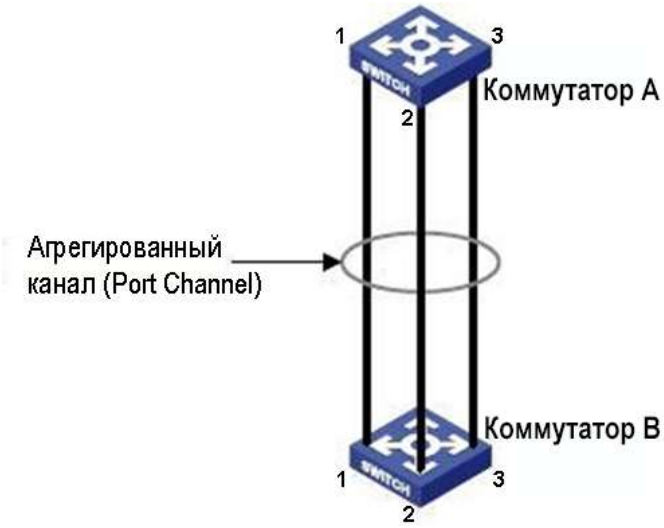


Рисунок 125 – Агрегированный канал

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

- Порт можно добавить только в одну группу.
- К агрегации могут присоединяться только полнодуплексные порты.
- На порту агрегированного канала нельзя включать LACP, а порт с включенным LACP не может быть добавлен в агрегацию.
- Port Channel и порт резервирования являются взаимоисключающими технологиями. Порт в агрегированном канале не может быть настроен как порт резервирования, а порт резервирования не может быть добавлен в агрегацию.
- Порт резервирования в этом документе подразумевает такие порты как порт Sy2-Ring, резервный порт Sy2-Ring, кольцевой порт Sy2-RP, резервный порт Sy2-RP, а также порты RSTP и MSTP.

7.4.1.3 Настройка с помощью WEB-интерфейса

1. Ниже показана статическая настройка агрегации.

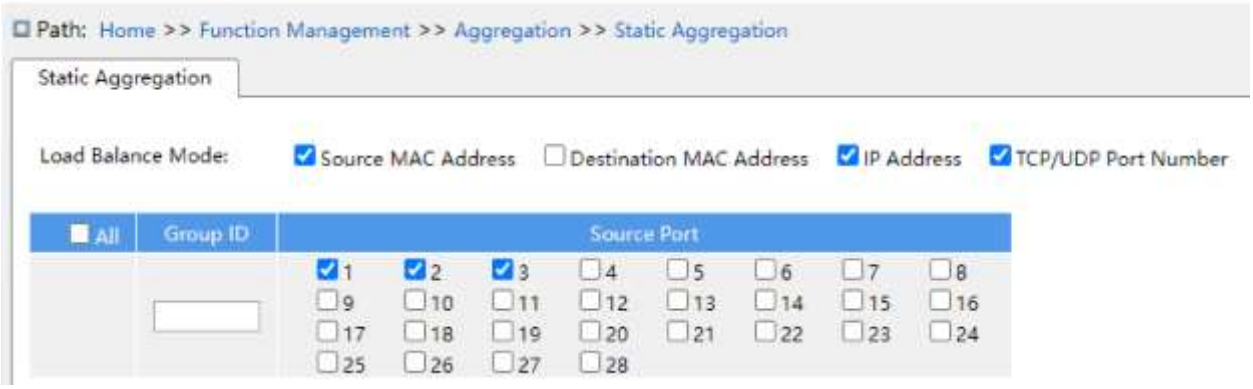


Рисунок 126 – Статическая настройка агрегации

Load Balance Mode

Варианты настройки: Source MAC Address / Destination MAC Address / IP Address / TCP/UDP Port Number

По умолчанию: Source MAC Address / IP Address / TCP/UDP Port Number

Функция: настройка режима балансировки нагрузки группы агрегации.

Описание: «Source MAC Address» балансирует трафик в соответствии с исходным MAC-адресом; «Destination MAC Address» балансирует трафик в соответствии с целевым MAC-адресом; «IP Address» балансирует трафик в соответствии с IP-адресом; «TCP/UDP Port Number» балансирует трафик в соответствии с номером порта TCP/UDP.

Group ID

Диапазон: 1–10

Функция: настройка идентификатора группы.

Описание: порты-участники одной и той же группы агрегации имеют одинаковые параметры. Количество групп агрегации зависит от портов устройства, а каждая группа поддерживает до 8 портов-участников.

Source Port

Варианты настройки: включено/выключено

Функция: выбор портов для присоединения к указанной группе агрегации.

7.4.1.4 Пример типовой настройки

Как показано на рисунке 125, добавьте в группу 1 три порта (порт 1, 2 и 3) коммутатора A и три порта (порт 1, 2 и 3) коммутатора B. Чтобы сформировать канал Port Channel соедините эти порты при помощи сетевых кабелей. Предполагается, что три порта на коммутаторах A и B имеют одинаковые атрибуты соответственно.

Настройка на коммутаторах:

1. Добавьте порт 1, 2 и 3 коммутатора A в группу 1, как показано на рисунке 126.
2. Добавьте порт 1, 2 и 3 коммутатора B в группу 1, как показано на рисунке 126.

7.4.2 LACP

7.4.2.1 Введение

Протокол управления агрегацией каналов LACP основан на стандарте IEEE802.3ad и предназначен для динамической агрегации портов. Протокол осуществляет обмен информацией между одноранговыми портами при помощи блоков данных LACPDU для выбора порта-участника в динамической группе агрегации.

7.4.2.2 Реализация

Порт, включенный в LACP, информирует соседний порт о своей приоритетности LACP, MAC-адресе устройства, приоритетности порта, номере порта и значении ключа, отправляя сообщение LACPDU. После получения сообщения LACPDU соседний порт ведет переговоры с локальным портом по следующему алгоритму:

1. Сравнение идентификаторов устройств

Идентификатор устройства определяется как комбинация приоритета LACP устройства и его MAC-адреса. Сначала сравниваются приоритеты LACP. Если приоритеты совпадают, сравниваются MAC-адреса. Устройство с меньшим идентификатором выбирается в качестве главного устройства.

2. Сравнение идентификаторов портов главного устройства

Идентификатор порта определяется как комбинация приоритета LACP порта и его номера. Сначала сравниваются приоритеты LACP портов. Если приоритеты совпадают, сравниваются номера портов. Порт с меньшим идентификатором выбирается в качестве эталонного порта.

3. Условия для добавления в группу агрегации

Если данный порт и эталонный порт имеют одинаковые значения ключей и одинаковые конфигурации атрибутов портов в состоянии «Up», а также если соседние порты данного порта и эталонного порта имеют одинаковые значения ключей и конфигурации атрибутов, данный порт может стать членом динамической группы агрегации.

7.4.2.3 Настройка с помощью WEB-интерфейса

1. Настройте приоритет LACP, как показано ниже.

Рисунок 127 – Настройка приоритета LACP

LACP

Диапазон: 1–65535

По умолчанию: 32768

Функция: настройка приоритета LACP, используемого для выбора основного устройства при согласовании LACP.

2. Ниже показана настройка портов LACP.

Рисунок 128 – Настройка портов LACP

LACP Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение протокола LACP для порта.

Key

Варианты настройки: Auto/Specific

Диапазон: 1–65535

По умолчанию: Auto

Функция: настройка значения ключа порта. Значение ключа определяется скоростью порта. если выбран режим «Auto», значение будет равно 1 (10 Мбит); 2 (100 Мбит); 3 (1000 Мбит). Порты с разными значениями ключа не могут быть добавлены в группы динамической агрегации.

Role

Варианты настройки: Active/Passive

По умолчанию: Active

Функция: выбор роли LACP. Активный порт будет активно отправлять сообщение LACPDU на соседний порт; пассивный порт принимает сообщения LACPDU от соседнего порта и отправляет свои сообщения только в ответ.

По крайней мере один из двух подключенных портов должен быть активен, в противном случае оба устройства не смогут обмениваться информацией.

Timeout

Варианты настройки: Fast/Slow

По умолчанию: Fast

Функция: настройка активного порта для отправки сообщения LACPDU с интервалом времени. Быстрый интервал (Fast) составляет 1 секунду, а медленный (Slow) – 30 секунд.

Priority

Диапазон: 1–65535

По умолчанию: 32768

Функция: настройка приоритета порта LACP, используется для выбора эталонных портов. Порты с низким приоритетом на главном устройстве выбираются в качестве эталонных.

3. Ниже показано состояние системы LACP.

Рисунок 129 – Состояние протокола LACP

4. Ниже показано состояние портов LACP.

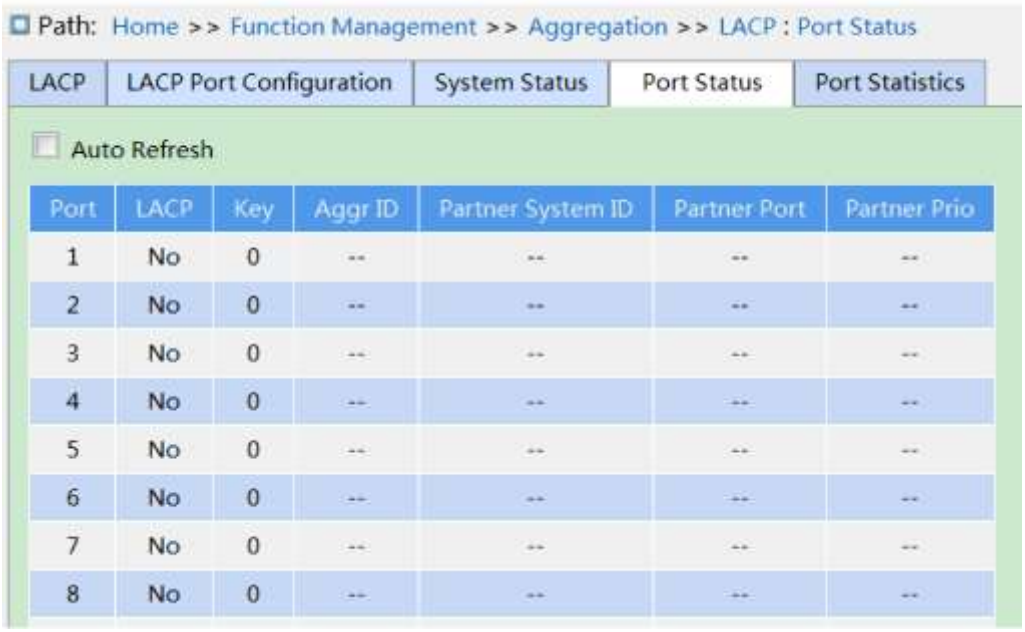


Рисунок 130 – Состояние портов LACP

LACP Status

Параметры отображения: Yes/No

Функция: отображение статуса LACP порта. «Yes» означает, что LACP включен, и порт работает. «No» означает, что LACP отключен, порт не работает.

5. Ниже показано отображение статистики портов LACP.

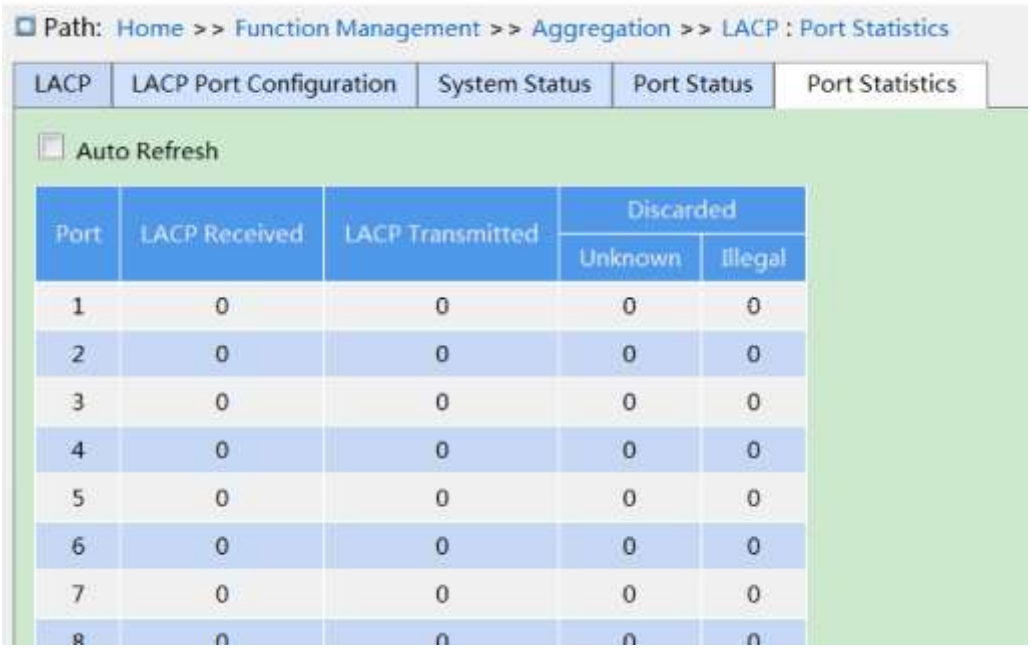


Рисунок 131 – Статистика портов LACP

7.4.2.4 Пример типовой настройки

Как показано на рисунке 125, добавьте в группу 1 три порта (порт 1, 2 и 3) коммутатора A и три порта (порт 1, 2 и 3) коммутатора B. Чтобы сформировать канал агрегации соедините эти порты при помощи сетевых кабелей. Предполагается, что три порта на коммутаторах A и B имеют одинаковые атрибуты соответственно.

Настройка на коммутаторах:

1. Включите LACP для портов 1, 2 и 3 коммутатора A, как показано на рисунке 128.
2. Включите LACP для портов 1, 2 и 3 коммутатора B, как показано на рисунке 128.

7.5 Резервирование

7.5.1 Sy2-Ring

7.5.1.1 Введение

Sy2-Ring и Sy2-Ring+ – проприетарные протоколы резервирования компании Symanitron. Они позволяют сети восстанавливаться менее чем за 50 мс при обрыве связи, обеспечивая надежную работу.

Sy2-Ring бывают двух типов: кольцо, основанное на портах (Sy2-Ring-Port), и кольцо, основанное на VLAN (Sy2-Ring-VLAN).

Sy2-Ring-Port: означает порт, через который необходимо передавать или блокировать данные.

Sy2-Ring-VLAN: означает порт определенной VLAN, через который необходимо передавать или блокировать данные. Это позволяет настраивать несколько колец, относящихся к разным VLAN, на одном порту.

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

7.5.1.2 Основные понятия

Мастер-узел. Одно кольцо может иметь только один мастер-узел. Мастер отправляет пакеты протокола Sy2-Ring и определяет состояние кольца. Когда кольцо замкнуто, два кольцевых порта на мастере находятся в состоянии пересылки и блокировки соответственно.

В состоянии пересылки находится порт, статус которого первым изменится на «Up». Второй кольцевой порт остается в состоянии блокировки.

Ведомый узел. Кольцо может иметь множество ведомых узлов. Ведомые узлы прослушивают сообщения Sy2-Ring и оповещают мастер-узел о неисправностях.

Резервный порт. Порт для связи между Sy2-кольцами называется резервным.

Резервный мастер-порт. Если в кольцевой топологии множество резервных портов, резервным мастер-портом среди них является порт, с бóльшим MAC-адресом. Он находится в состоянии пересылки данных.

Резервный ведомый порт. Если в кольцевой топологии множество резервных портов, все они, кроме резервного мастер-порта, будут ведомыми и будут находится в состоянии блокировки.

Состояние пересылки данных. Порт может получать и передавать данные.

Состояние блокировки. Порт может получать и передавать только пакеты Sy2-Ring, но не какие-либо другие данные.

7.5.1.3 Реализация

Sy2-Ring-Port

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

Рабочий процесс коммутаторов A, B, C и D:

1. Коммутатор A настроен как ведущий, а остальные коммутаторы – как ведомые.

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

3. Канал связи CD неисправен, как показано на рисунке 132.

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

б) Когда неисправность устранена, порты 6 и 7 ведомого устройства находятся в состоянии пересылки. Порт 2 на ведущем устройстве переходит в состояние блокировки. Происходит переключение каналов, и каналы восстанавливаются до состояния, предшествующего отказу канала CD.

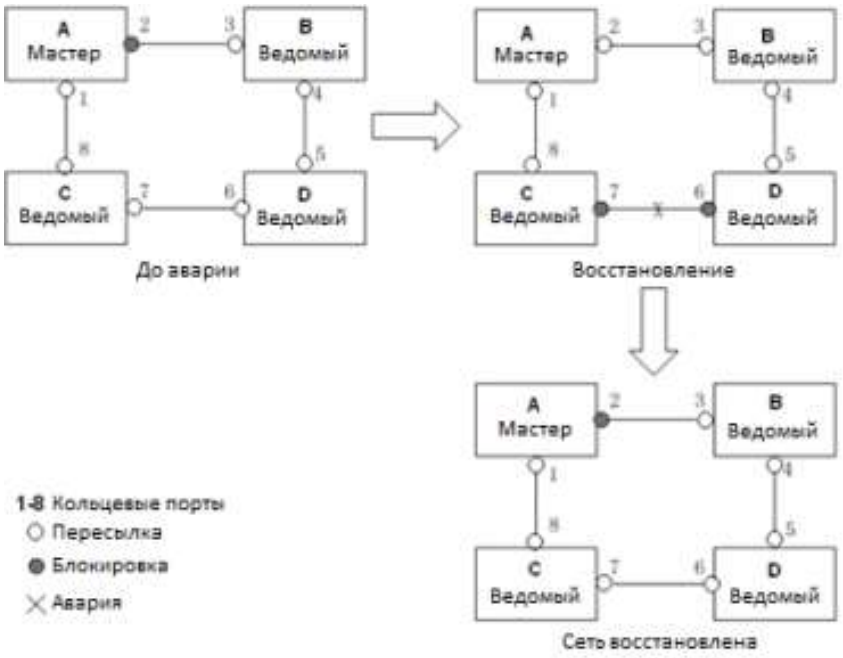


Рисунок 132 – Неисправность канала связи CD

4. Канал связи AC неисправен, как показано на рисунке 133.

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

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

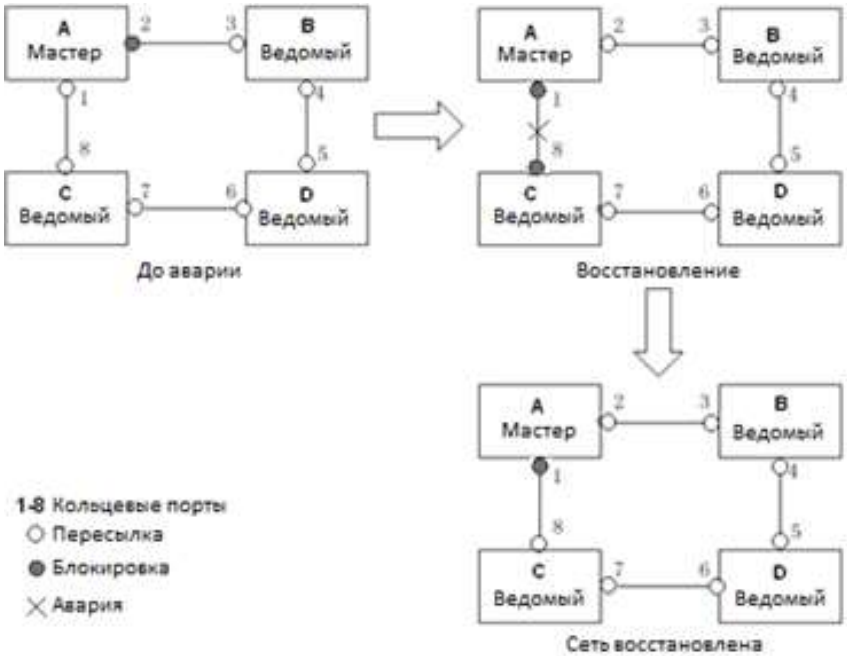


Рисунок 133 – Неисправность канала связи AC

Изменение состояния соединения влияет на состояние портов кольца.

Sy2-Ring-VLAN

Sy2-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям.

Каждый путь пересылки для VLAN образует Sy2-Ring-VLAN. У разных колец Sy2-Ring-VLAN могут быть разные мастер-узлы. Как показано на рисунке 134, настроены две Sy2-Ring-VLAN:

VLAN 10: AB-BC-CD-DE-EA.

VLAN 20: FB-BC-CD-DE-EF.

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

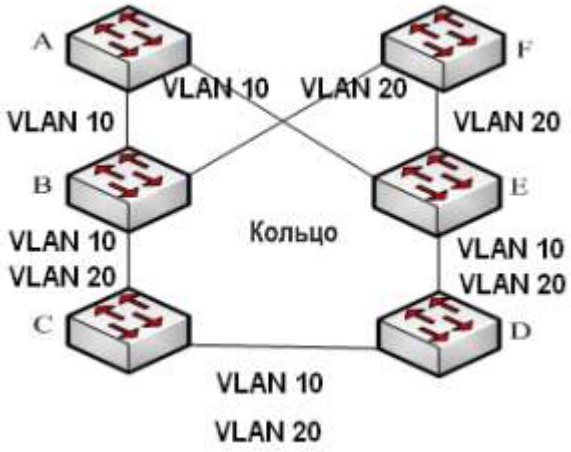


Рисунок 134 – Sy2-Ring-VLAN

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

Sy2-Ring+

Sy2-Ring+ может обеспечивать резервирование для двух колец SY2, как показано на рисунке 135. Один резервный порт настроен соответственно на коммутаторе C и коммутаторе D. Какой порт является резервным мастер-портом, зависит от MAC-адресов двух портов. Если главный резервный порт или его канал выходят из строя, ведомый резервный порт будет пересылать пакеты, предотвращая образование петель и обеспечивая нормальную связь между резервными кольцами.

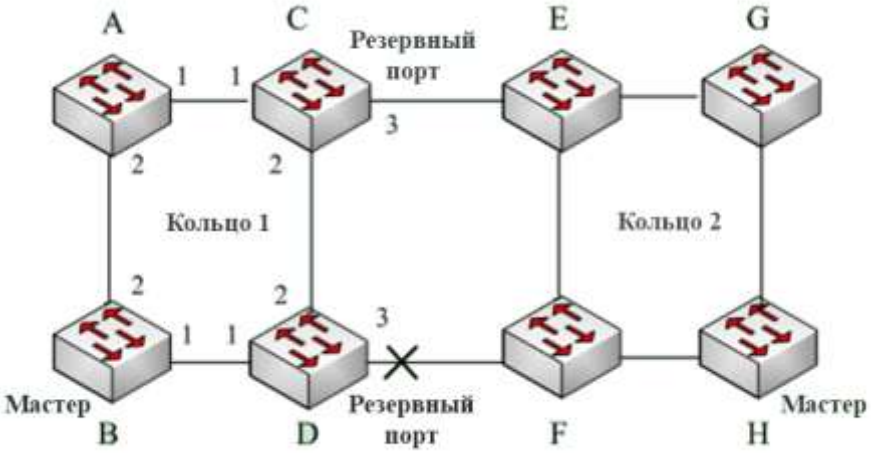


Рисунок 135 – Топология Sy2-Ring+

Изменение состояния соединения влияет на состояние резервных портов.

7.5.1.4 Пояснение

Конфигурации Sy2-Ring должны соответствовать следующим условиям:

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

7.5.1.5 Настройка с помощью WEB-интерфейса

1. Настройте режим кольцевого резервирования, как показано на рисунке 136.

Рисунок 136 – Выбор режима кольцевого резервирования

Redundancy Mode

Параметры: Port Based/Vlan Based

По умолчанию: Port Based

Функция: Выбор режима кольцевого резервирования Sy2-Ring.

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

---

2. Настройте Sy2-Ring-Port и Sy2-Ring-VLAN, как показано на рисунках 137 и 138.

Рисунок 137 – Настройка Sy2-Ring-Port

Рисунок 138 – Настройка Sy2-Ring-VLAN

Domain ID

Диапазон: 1–32

Функция: идентификатор домена, который используется для различения колец. Один коммутатор поддерживает максимум 16 колец на основе VLAN, количество колец на основе портов зависит от количества портов коммутатора.

Domain Name

Диапазон: 1–31 символ

Функция: настройка имени домена.

Station Type

Параметры: Master/Slave

По умолчанию: Master

Функция: выбор роли коммутатора в кольце. Master – ведущий, slave – ведомый.

Ring Port-1/Ring Port-2

Параметры: все порты коммутатора

Функция: выбор двух кольцевых портов.

- Порт кольца Sy2-Ring, а также резервные порты не могут быть добавлены в группу агрегации Port Channel. Порт, добавленный в группу агрегации не может быть портом кольца Sy2-Ring или резервным портом.
- Порты протоколов на основе портов RSTP, SY2-Ring-Port и SY-RP2-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт SY2-Ring-Port не могут быть настроены как порт RSTP, кольцевой порт SY-RP2-Port или резервный порт SY-RP2-Port; порт RSTP, кольцевой порт SY-RP2-Port и резервный порт SY-RP2-Port не могут быть настроены как кольцевой порт SY2-Ring-Port или резервный порт.
- Не рекомендуется настраивать порты в группе изоляции одновременно как порты Sy2-Ring и резервные порты, а порты Sy2-Ring и резервные порты нельзя добавлять в группу изоляции.

Sy2-Ring+

Параметры: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение Sy2-Ring+.

Backup Port

Параметры: все порты коммутатора

Функция: выбор порта в качестве резервного.

Пояснение: перед настройкой резервного порта включите Sy2-Ring+.

Не настраивайте кольцевой порт в качестве резервного.

VLAN List

Параметры: все созданные VLAN

Функция: выбор VLAN для кольцевого порта. Если есть несколько VLAN, вы можете разделить VLAN запятой (,) и дефисом (-), где дефис используется для указания диапазона последовательных идентификаторов VLAN, а запятая – для разделения двух непоследовательных идентификаторов.

3. Просмотрите и измените конфигурацию Sy2-Ring, как показано на рисунке 139.

Рисунок 139 – Конфигурация Sy2-Ring

Выберите запись Sy2-Ring, нажмите <Edit>, чтобы изменить конфигурацию записи или <Del>, чтобы удалить ее.

4. Нажмите <Details> напротив записи, чтобы отобразить состояние кольца и портов Sy2-Ring, как показано на рисунке 140.

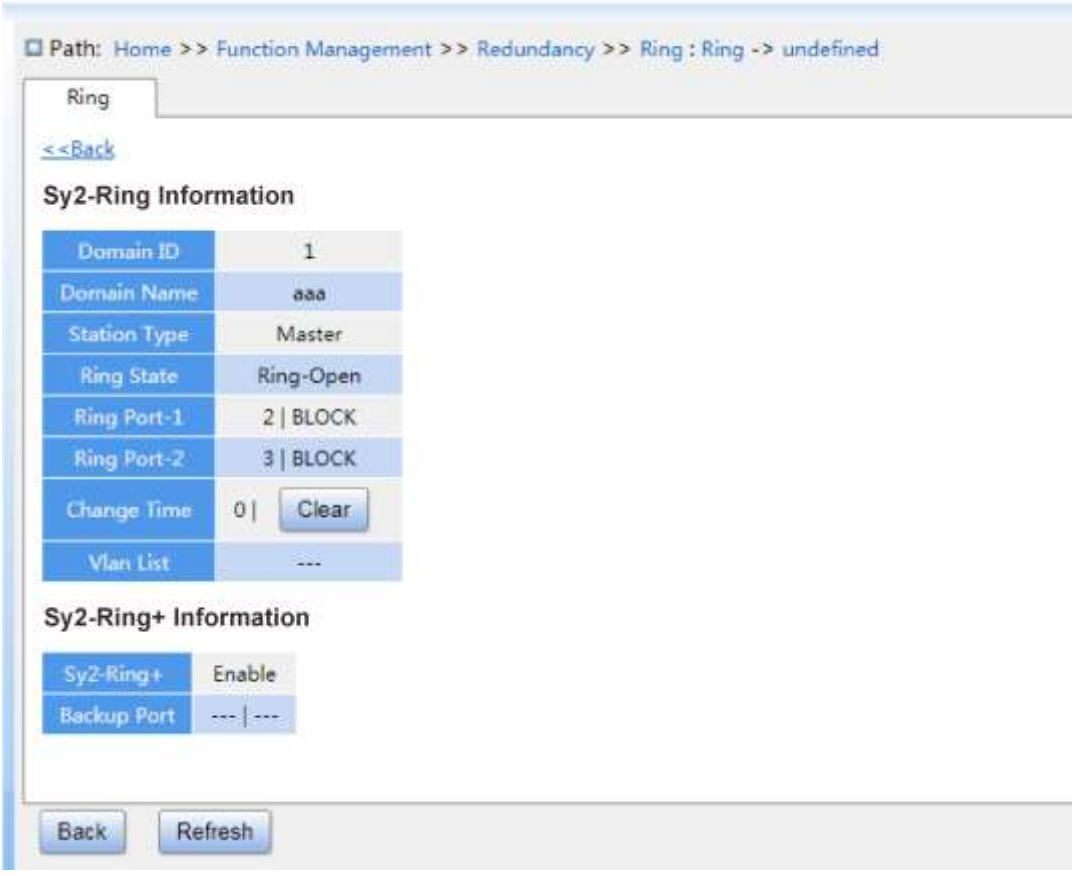


Рисунок 140 – Статус Sy2-Ring

7.5.1.6 Пример типовой настройки

Как показано на рисунке 135, коммутаторы A, B, C и D образуют кольцо 1; коммутаторы E, F, G и H образуют кольцо 2. Каналы CE и DF являются резервными соединениями между кольцом 1 и кольцом 2.

Конфигурация коммутатора A:

1. Domain ID: 1; Domain Name: a; Ring Port: 1, 2; Station Type: Slave; Sy2-Ring+: Disable; Backup Port: не назначен (см. рисунок 137).

Конфигурация коммутатора B:

2. Domain ID: 1; Domain Name: a; Ring Port: 1, 2; Station Type: Master; Sy2-Ring+: Disable; Backup Port: не назначен (см. рисунок 137).

Конфигурация коммутаторов C и D:

3. Domain ID: 1; Domain Name: a; Ring Port: 1, 2; Station Type: Slave; Sy2-Ring+: Enable; Backup Port: 3 (см. рисунок 137).

Конфигурация коммутаторов E, F и G:

4. Domain ID: 2; Domain Name: b; Ring Port: 1, 2; Station Type: Slave; Sy2-Ring+: Disable; Backup Port: не назначен (см. рисунок 137).

Конфигурация коммутатора H:

5. Domain ID: 2; Domain Name: b; Ring Port: 1, 2; Station Type: Master; Sy2-Ring+: Disable; Backup Port: не назначен (см. рисунок 137).

7.5.2 Sy2-RP

7.5.2.1 Введение

Протокол Sy2-RP (Symanitron Redundancy Protocol) разработан для передачи данных в кольцевых сетях. Он может предотвращать широковещательные штормы в кольцевых топологиях. Если канал или узел выходят из строя, вместо них задействуется резервная связь, обеспечивающая бесперебойную передачу данных.

Совместимый со стандартом IEC 62439-6, протокол Sy2-RP использует механизм выбора мастера без привязки к определенному узлу. Sy2-RP предоставляет следующие возможности:

- Время восстановление, не зависящее от размеров сети.

Sy2-RP обеспечивает время восстановления, не зависящее от размера сети, за счет оптимизации механизма определения передачи данных по кольцу. Sy2-RP позволяет сетям восстанавливаться менее, чем за 20 мс, благодаря функции оповещения реального времени, обеспечивающей надежную передачу данных. Эта функция позволяет коммутаторам обеспечивать максимальную надежность приложений в энергетике, железнодорожном транспорте и многих других отраслях, где требуется управление в реальном времени.

➢ Функция диверсифицированного определения сбоя соединения.

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

➢ Применимость к различным сетевым топологиям.

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

➢ Функции диагностики и поддержки

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

7.5.2.2 Основные понятия

1. Режимы Sy2-RP

Sy2-RP имеет два режима: Sy2-RP-Port-Based и Sy2-RP-VLAN-Based.

Sy2-RP-Port-Based: пересылает или блокирует данные на основе определенных портов.

Sy2-RP-VLAN-Based: пересылает или блокирует пакеты на основе VLAN. Если порт находится в состоянии блокировки, блокируются только пакеты данных указанной VLAN. Таким образом, на общих портах пересекающихся колец можно настроить несколько VLAN. Порт может принадлежать разным кольцам Sy2-RP в соответствии с конфигурациями VLAN.

2. Статус порта Sy2-RP

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

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

Основной порт: указывает кольцевой порт корневого устройства, статус которого принудительно настроен пользователем на передачу данных при замыкании кольца.

➢ Если на корневом устройстве не настроен основной порт, первый порт, состояние связи которого меняется на «Up» при замыкании кольца, будет пересылать данные. Другой кольцевой порт остается в состоянии блокировки.

- Порт на корневом устройстве, находящийся в состоянии блокировки, может активно отправлять пакеты Sy2-RP.

---

3. Роли Sy2-RP

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

INIT: обозначает устройство, на котором Sy2-RP включен и оба его кольцевых порта находятся в состоянии «Link Down».

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

Резервный корневой (B-Root): обозначает устройство, на котором Sy2-RP включен, один порт активен, а второй неактивен или в режиме деградации CRC; приоритет не ниже 200. B-Root сравнивает и передает пакеты Announce. Если вектор полученного пакета Announce меньше, чем вектор собственного пакета, B-Root меняет свою роль на Root, в противном случае он передает полученный пакет и не меняет собственной роли. Статус кольцевых портов: один кольцевой порт в состоянии пересылки.

Обычный (Normal): обозначает устройство, на котором Sy2-RP включен и оба порта активны без CRC-деградации; приоритет больше 200. Обычные коммутаторы только передают пакеты Announce, без проверки содержимого. Статус кольцевых портов: оба порта в состоянии пересылки.

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

7.5.2.3 Реализация

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

Вектор пакета Announce содержит следующую информацию для назначения роли:

Таблица 5 – Вектор пакета Announce

Статус соединения	Деградация CRC		Ролевой приоритет	IP-адрес устройства	MAC-адрес устройства
	Статус деградации CRC	Скорость деградации CRC			

Статус соединения: значение устанавливается равным 1, если один кольцевой порт находится в состоянии «Link Down», и устанавливается в 0, если оба кольцевых порта находятся в состоянии «Link Up».

Статус деградации CRC: если на одном из портов присутствует деградация CRC, значение равно 1. Если ни на одном порту ее нет, значение равно 0.

Скорость деградации CRC: отношение количества пакетов CRC к пороговому значению за 15 минут.

Ролевой приоритет: значение можно установить через веб-интерфейс.

Параметры вектора из таблицы 5 сравниваются следующим образом:

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

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

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

4. Устройство с бóльшим вектором выбирается корневым.

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

➢ Реализация режима Sy2-RP на основе портов

Роль коммутатора определяется следующим образом:

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

2. Коммутатор с наибольшим вектором Announce выбирается корневым. Его кольцевой порт, перешедший в активное состояние первым, начинает пересылать данные, а второй порт переходит в режим блокировки. Среди остальных коммутаторов тот, у которого один

из портов в неактивном состоянии или в режиме CRC-деградации, переходит в режим B-Root. Коммутаторы с двумя активными кольцевыми портами, не имеющими деградации CRC, получают статус Normal.

Процедура устранения неисправности показана на рисунке 141:

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

2. Когда связь CD обрывается, Sy2-RP изменяет статусы портов 6 и 7 на блокировку. В результате C и D становятся корневыми. Поскольку A, C и D в данный момент являются корневыми, все они отправляют пакеты Announce. Векторы C и D больше, чем векторы A, потому что порты 7 и 6 находятся в состоянии «Link Down». В этом случае, если вектор D больше, чем вектор C, D выбирается в качестве Root, а C становится B-Root. При получении пакета Announce от D, A обнаруживает, что вектор D больше, чем его собственный вектор, и оба его кольцевых порта находятся в состоянии «Link Up». Таким образом, A становится обычным (Normal) и изменяет статус порта 2 на пересылку данных.

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

Если на D не настроен основной порт, порт 7 все еще находится в состоянии блокировки, а порт 8 – в состоянии пересылки.

Если порт 7 на D настроен как основной, порт 7 переходит в состояние пересылки, а порт 8 – в состояние блокировки.

Sy2-RP изменяет статус порта 6 на передачу данных. В результате C возвращается к роли Normal. Таким образом, роли коммутаторов не меняются при восстановлении канала связи.

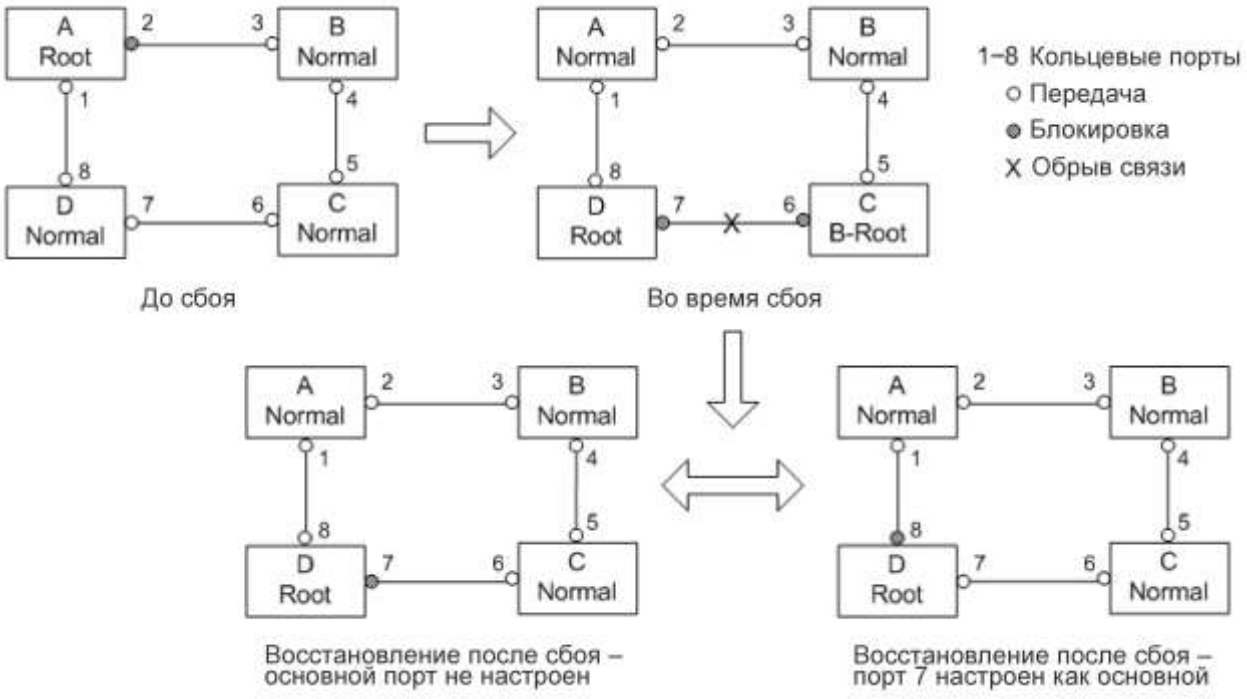


Рисунок 141 – Сбой связи Sy2-RP

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

➢ Реализация режима Sy2-RP на основе VLAN

Кольцо Sy2-RP-VLAN-Based позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует Sy2-RP-VLAN-Based. Различные кольца Sy2-RP на основе VLAN могут иметь разные корни. Как показано на следующем рисунке, на основе VLAN настроены два кольца Sy2-RP.

Кольцевые связи Sy2-RP на основе VLAN10/20: AB-BC-CD-DE-EA.

Кольцевые связи Sy2-RP на основе VLAN30: FB-BC-CD-DE-EF.

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

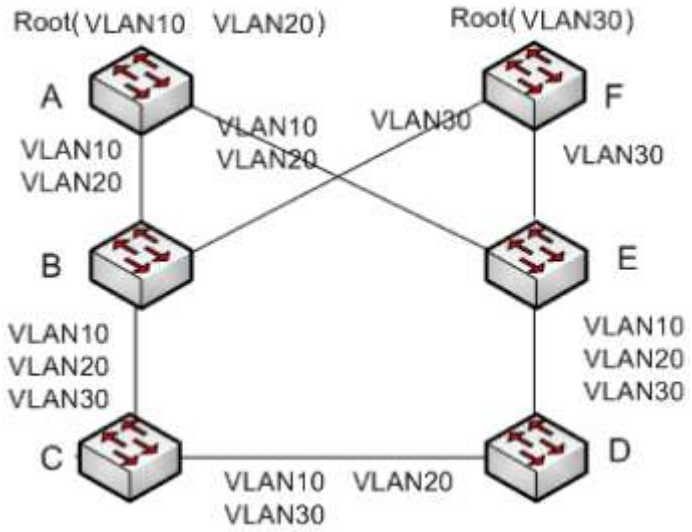


Рисунок 142 – Sy2-RP-VLAN-Based

Статусы портов и распределение ролей в каждом кольце Sy2-RP-VLAN-Based такие же, как и в кольце Sy2-RP-Port-Based.

➢ Резервирование Sy2-RP

Sy2-RP также может обеспечивать резервируемое соединение между двумя кольцами, обеспечивая для них надежную связь и предотвращая появление петель.
Резервный порт: обозначает порт связи между кольцами Sy2-RP. Можно назначать множество резервных портов, однако все они должны быть в одном кольце. Первый активный порт становится главным (резервным мастер-портом) и переходит в режим

пересылки данных. Все остальные резервные порты становятся ведомыми и переходят в режим блокировки.

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

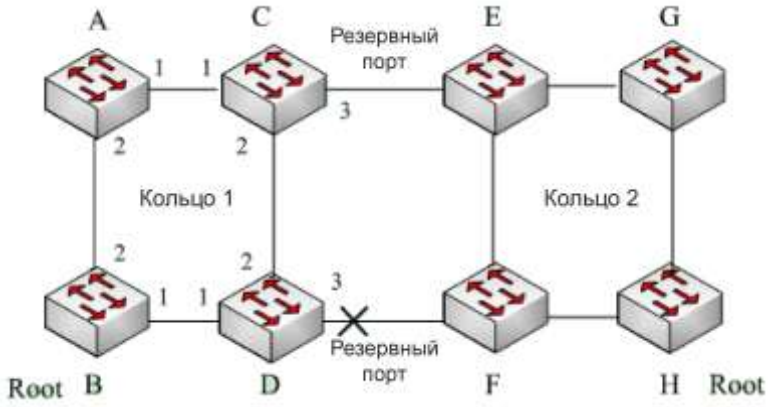


Рисунок 143 – Резервирование Sy2-RP

Изменение состояния соединения влияет на статус резервных портов.

7.5.3 DHP

7.5.3.1 Введение

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

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

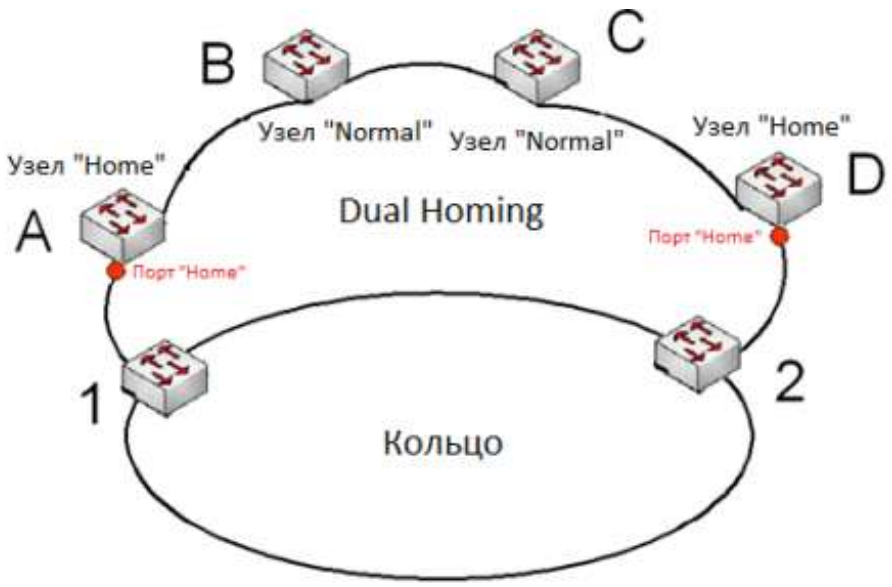


Рисунок 144 – Реализация протокола Dual Homing

7.5.3.2 Основные понятия

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

- Отправку ответных пакетов корневому коммутатору при получении от него пакетов Announce. Если корневой коммутатор получает ответные пакеты, он считает, что кольцо замкнуто. В противном случае кольцо считается разомкнутым.
- Блокировку пакетов Sy2-RP внешних сетей и изоляцию канала Dual Homing от внешних сетей.
- Отправку пакетов очистки записей подключенным устройствам во внешних сетях при изменении топологии канала Dual Homing.

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

7.5.3.3 Реализация

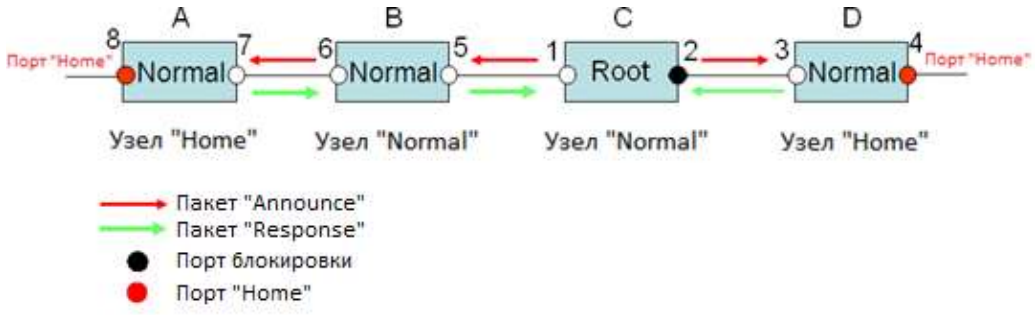


Рисунок 145 – Конфигурация Dual Homing

Как показано на рисунке 145, настройки коммутаторов A, B, C и D следующие:

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

Реализация:

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

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

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

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

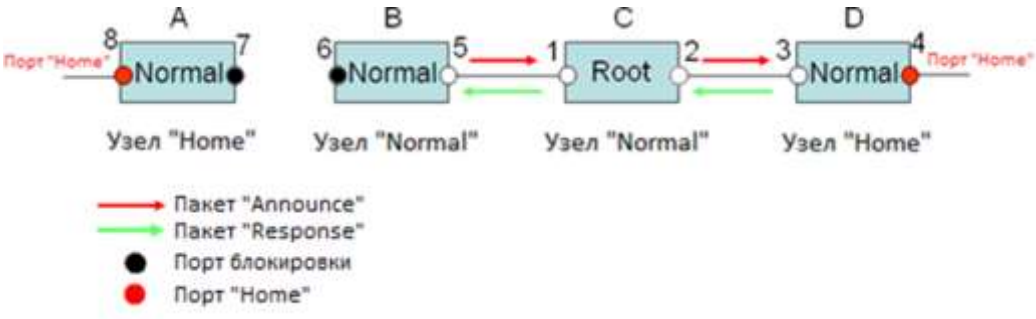


Рисунок 146 – Восстановление связи Dual Homing

7.5.3.4 Пояснение

Конфигурации Sy2-RP должны соответствовать следующим требованиям:

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

7.5.3.5 Настройка с помощью WEB-интерфейса

1. Настройте режим кольцевого резервирования, как показано на рисунке 147.

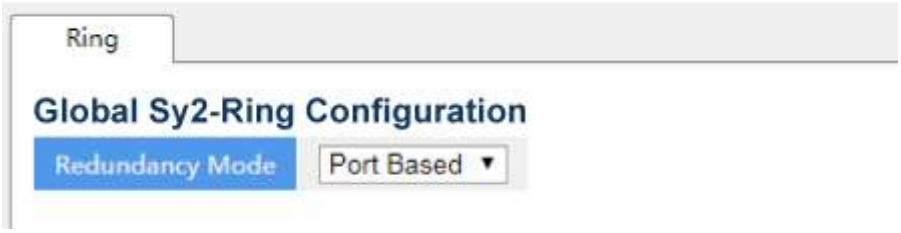


Рисунок 147 – Выбор режима кольцевого резервирования

Redundancy Mode

Параметры: Port Based/Vlan Based

По умолчанию: Port Based

Функция: Выбор режима кольцевого резервирования Sy2-Ring.

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

---

2. Настройте Sy2-RP-Port и Sy2-RP-VLAN, как показано на рисунках 148 и 149.

Рисунок 148 – Настройка Sy2-RP-Port

Рисунок 149 – Настройка Sy2-RP-VLAN

Domain ID

Диапазон: 1–32

Функция: идентификатор домена, который используется для различения колец. Один коммутатор поддерживает максимум 8 колец на основе VLAN, количество колец на основе портов зависит от количества портов коммутатора.

Domain Name

Диапазон: 1–31 символ

Функция: настройка имени домена.

Ring Port-1/Ring Port-2

Параметры: все порты коммутатора

Функция: выбор двух кольцевых портов.

- Порт кольца Sy2-RP, а также резервные порты не могут быть добавлены в группу агрегации Port Channel. Порт, добавленный в группу агрегации не может быть портом кольца Sy2-RP или резервным портом.
- Порты протоколов на основе портов RSTP, SY2-Ring-Port и SY-RP2-Port являются взаимоисключающими, то есть кольцевой и резервный порт SY2-RP не могут быть настроены как порт RSTP; порт RSTP не может быть настроен как кольцевой или резервный порт SY2-RP.

Primary Port

Варианты настройки: --/Ring Port-1/Ring Port-2

По умолчанию: --

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

DHP Mode

Варианты настройки: Disable/Normal-Node/Home-Node

По умолчанию: Disable

Функция: отключение или выбор режима DHP.

DHP Home Port

Варианты настройки: Ring-Port-1/Ring-Port-2/Ring-Port-1-2

Функция: настройка порта Home для DHP-узла Home.

Описание: если в топологии DHP задействовано только одно устройство, оба кольцевых порта Home-узла должны быть настроены как Home-порт.

CRC Threshold

Диапазон: 25–65535

По умолчанию: 100

Функция: настройка порога CRC.

Описание: этот параметр используется при выборе корневого коммутатора. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет деградацию CRC. В результате значение деградации CRC в векторе пакета Announce порта устанавливается равным 1.

Role Priority

Диапазон: 0–255

По умолчанию: 128

Функция: настройка приоритета коммутатора.

Backup Port

Параметры: все порты коммутатора

Функция: настройка резервного порта.

Не настраивайте кольцевой порт в качестве резервного.

VLAN List

Параметры: все созданные VLAN

Функция: выбор VLAN, управляемых текущим кольцом Sy2-RP-VLAN.

Protocol Vlan ID

Диапазон: 1–4093

Описание: идентификатор VLAN управления.

Функция: пакеты Sy2-RP с указанной VLAN служат основой для диагностики и управления кольцом Sy2-RP-VLAN-Based.

Protocol Enable

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение/отключение протокола Sy2-RP для указанного домена

3. Просмотрите и измените конфигурацию Sy2-RP, как показано на рисунке 150.

Рисунок 150 – Конфигурация Sy2-RP

Выберите запись Sy2-RP, нажмите <Edit>, чтобы изменить конфигурацию записи или <Del>, чтобы удалить ее.

4. Нажмите <Details> напротив записи, чтобы отобразить состояние кольца и портов Sy2-RP, как показано на рисунке 151.

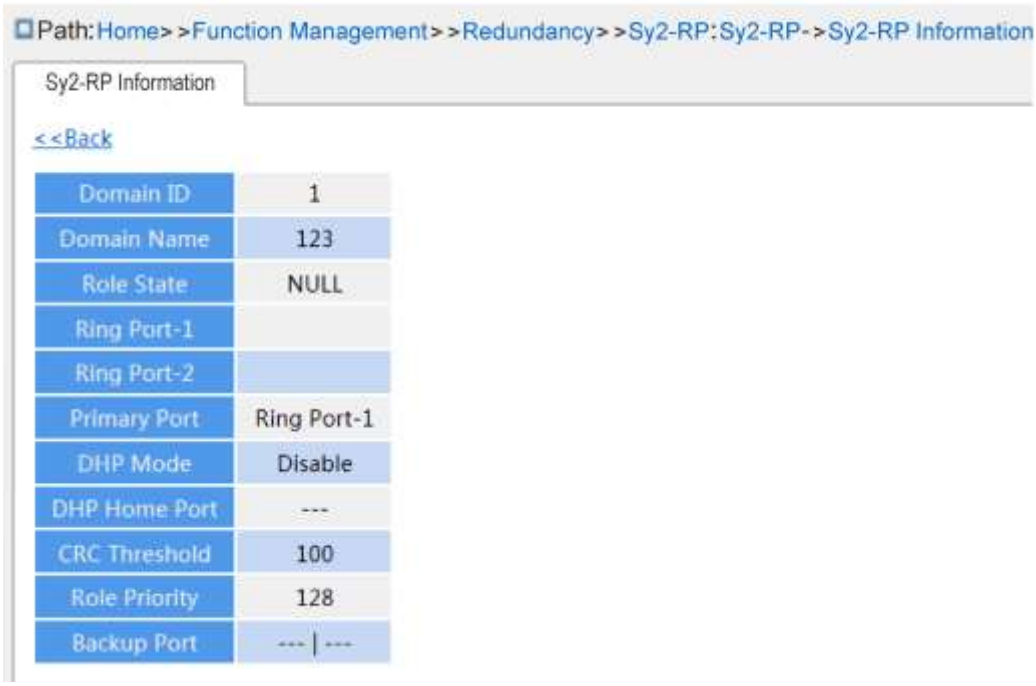


Рисунок 151 – Состояние Sy2-RP

7.5.3.6 Пример типовой настройки

Как показано на рисунке 143, A, B, C и D образуют кольцо 1; E, F, G и H образуют кольцо 2; CE и DF являются резервными каналами кольца 1 и кольца 2.

Настройка коммутаторов A и B:

1. Установите для идентификатора домена значение «1», а для имени домена значение «a». Выберите кольцевой порт 1 и кольцевой порт 2. Оставьте значения по умолчанию для ролевого приоритета и резервного порта, как показано на рисунке 148.

Настройка коммутаторов C и D:

2. Установите для идентификатора домена значение «1», для имени домена значение «a», для резервного порта значение «3». Выберите кольцевой порт 1 и кольцевой порт 2. Оставьте значение по умолчанию для ролевого приоритета, как показано на рисунке 148.

Настройка коммутаторов E, F, G и H:

3. Установите для идентификатора домена значение «2», для имени домена значение «b». Выберите кольцевой порт 1 и кольцевой порт 2. Оставьте значения по умолчанию для ролевого приоритета и резервного порта, как показано на рисунке 148.

7.5.4 STP/RSTP

7.5.4.1 Введение

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

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

7.5.4.2 Основные понятия

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

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

Назначенный порт (Designated port): порт, который отвечает за пересылку BPDU другим устройствам или локальным сетям. Все порты корневого моста являются назначенными.

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

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

7.5.4.3 BPDU

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

Таблица 6 – BPDU

…	Root bridge ID	Root path cost	Designated bridge ID	Designated port ID	Message age	Max age	Hello time	Forward delay	…
…	8 байт	4 байта	8 байт	2 байта	2 байта	2 байта	2 байта	2 байта	…

Структура данных BPDU включает:

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

Стоимость пути (Root path cost): стоимость кратчайшего пути до корневого моста

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

Идентификатор назначенного порта (Designated port ID): приоритет порта + номер порта.

Возраст сообщения (Message age): время, в течение которого BPDU может распространяться по сети.

Максимальный возраст или время старения (Max age): максимальное время хранения BPDU на устройстве. Когда возраст сообщения больше, чем время старения, BPDU отбрасывается.

Время приветствия (Hello time): интервал времени для отправки BPDU.

Задержка отправки (Forward delay): задержка изменения статуса (отбрасывание – обучение – пересылка).

7.5.4.4 Реализация

Процесс вычисления логического дерева для всех устройств следующий:

1. Начальная стадия.

Все устройства на всех своих портах генерируют BPDU, считая себя корневым мостом. И идентификатор корневого моста, и идентификатор назначенного моста являются

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

2. Выбор оптимальной конфигурации BPDU.

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

- Если приоритет конфигурации BPDU, сгенерированного локальным портом выше, чем приоритет в BPDU, принятом от другого узла, устройство не выполняет никакой обработки.
- Если приоритет полученного BPDU выше, то порт заменяет локальный BPDU полученным.

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

- 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 в BPDU плюс стоимость пути локального порта меньше, приоритет BPDU выше.
- Если стоимость пути в двух BPDU также одинаковы, по порядку сравниваются ID назначенных коммутаторов, ID назначенных портов и ID портов, получивших BPDU. BPDU с наименьшим ID будет иметь наивысший приоритет.

3. Выбор корневого моста.

Корневым мостом связующего дерева является устройство с наименьшим ID.

4. Выбор корневых портов.

Некорневые коммутаторы сделают свои порты, получающие BPDU с наилучшей конфигурацией, корневыми.

5. Расчет BPDU для назначенного порта.

В соответствии с BPDU корневого порта и его стоимостью пути, BPDU назначенного порта рассчитывается для каждого порта следующим образом:

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

6. Выбор назначенного порта.

Если вычисленные значения BPDU лучше, устройство делает этот порт назначенным, заменяет BPDU порта вычисленным и отправляет новый BPDU. Если текущие значения BPDU лучше, устройство не обновляет его и блокирует порт. Заблокированные порты могут принимать и отправлять только служебную информацию RSTP, но не данные.

7.5.4.5 Настройка с помощью WEB-интерфейса

1. Настройте временные параметры сетевого моста, как показано ниже.

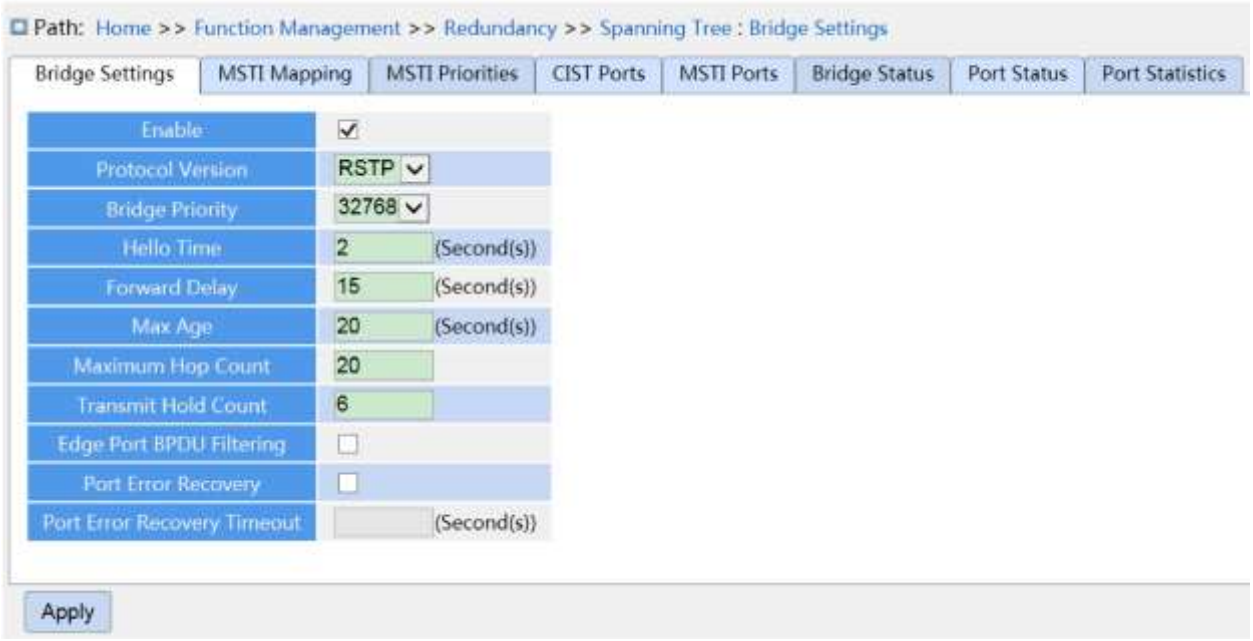


Рисунок 152 – Настройка временных параметров сетевого моста

Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение протокола связующего дерева.

- К протоколам на основе портов относятся RSTP, Sy2-Ring-Port и Sy2-RP-Port, а к протоколам на основе VLAN – MSTP, Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Протоколы на основе портов и VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один тип протокола.

Protocol Version

Варианты настройки: MSTP/RSTP/STP

По умолчанию: MSTP

Функция: выбор протокола связующего дерева.

Bridge Priority

Диапазон: 0–61440; Шаг – 4096.

По умолчанию: 32768

Функция: настройка приоритета сетевого моста.

Описание: приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

Hello Time

Диапазон: 1–10 с

По умолчанию: 2 с

Функция: настройка интервала отправки BPDU.

Forward Delay

Диапазон: 4–30 с

По умолчанию: 15 с

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

Max Age

Диапазон: 6–40 с

По умолчанию: 20 с

Функция: возраст сообщения, то есть, максимальная продолжительность, в течение которой BPDU может быть сохранен на устройстве.

Описание: если значение Max Age в BPDU больше указанного при настройке, то BPDU отбрасывается.

- Значения Forward Delay, Hello Time и Max Age должны соответствовать следующим требованиям: 2*(Forward Delay – 1,0 с) ≥ Max Age; Max Age ≥ 2*(Hello Time + 1,0 с).
- Рекомендуется использовать настройку по умолчанию.

Maximum Hop Count

Диапазон: 6–40

По умолчанию: 20

Функция: настройка максимального количества переходов для области MST. Максимальное количество переходов ограничивает масштаб региона MST; максимальное количество переходов для корневого моста области является максимальным количеством переходов для всей области MST.

Описание: начиная с корневого моста в области MST, количество переходов уменьшается на 1 при прохождении BPDU через каждое устройство в области. Устройство отбрасывает BPDU, если количество переходов достигает 0.

- Действительной является только конфигурация Maximum Hop Count корневого моста в MST-регионе. Устройства, не являющиеся корневыми, принимают значение, настроенное для корневого моста.
- Рекомендуется использовать настройку по умолчанию.

Transmit Hold Count

Диапазон: 1–10

По умолчанию: 6

Функция: указание максимального количества пакетов BPDU, которые могут быть отправлены портом в течение каждого интервала Hello Time.

Edge Port BPDU Filtering

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: управление получением и пересылкой пакетов BPDU на граничном порту.

Port Error Recovery

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: управление возможностью автоматического восстановления порта из состояния ошибки в нормальное рабочее состояние.

Port Error Recovery Timeout

Диапазон: 30–86400 с

Функция: настройка времени для восстановления порта из состояния ошибки в нормальное рабочее состояние.

2. Настройте порты RSTP, как показано ниже.

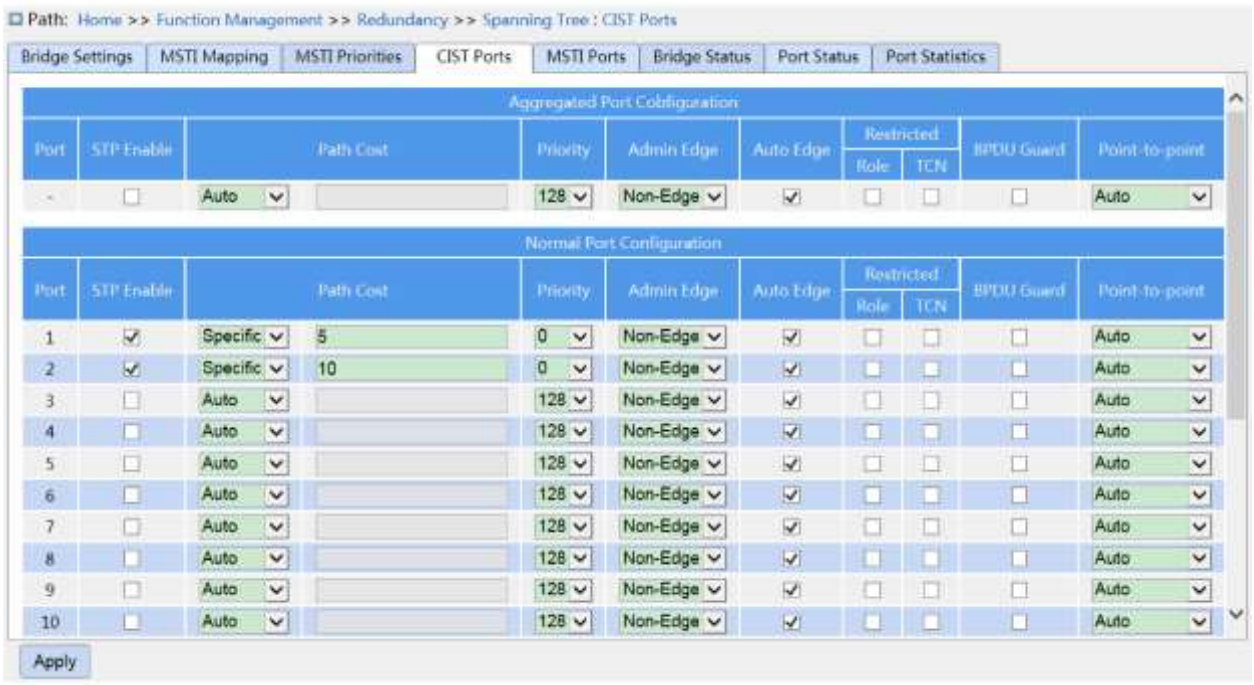


Рисунок 153 – Настройка портов RSTP

STP Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение STP/RSTP на портах.

- Порт RSTP нельзя добавить в группу агрегации; порт из группы агрегации не может быть настроен как порт RSTP.
- Настройка портов RSTP, Sy2-Ring-Port и Sy2-RP-Port является взаимоисключающей. То есть, кольцевой или резервный порт Sy2-Ring-Port не должны быть настроены как порт RSTP, Sy2-RP-Port, кольцевой или резервный порт Sy2-RP-Port. Соответственно, порт RSTP, кольцевой и резервный порт Sy2-RP-Port не должны быть настроены как кольцевой или резервный порт Sy2-Ring-Port.

Path Cost

Варианты настройки: Auto/Specific (1–200000000)

По умолчанию: Auto

Описание: данная функция используется для расчета наилучшего пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, поменяв его стоимость пути. Чтобы настроить значение вручную, выберите для параметра режим «Specific».

Priority

Диапазон: 0–240; шаг: 16

По умолчанию: 128

Функция: настройка приоритета порта, который определяет его роль.

Admin Edge

Варианты настройки: Non-Edge/Edge

По умолчанию: Non-Edge

Функция: указывает, является ли текущий порт граничным портом.

Описание: когда порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, он считается граничным. Граничный порт может быстро перейти из состояния блокировки в состояние пересылки без ожидания окончания интервала «Forward Delay». Если граничный порт начинает получать пакеты BPDU, он перестает быть граничным.

Auto Edge

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение/отключение функции автоматического определения, является ли текущий порт граничным.

Restricted Role

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: ограничение ролей. Порт, для которого включена эта функция, никогда не будет выбран в качестве корневого узла, даже если ему предоставлен наивысший приоритет.

Restricted TCN

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: ограничение сообщений об изменении топологии. Порт, для которого включена эта функция, не будет активно отправлять сообщения TCN.

BPDU Guard

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: указывает, переходит ли граничный порт в состояние Error-Disable и отключается ли он при получении пакетов BPDU.

Point-to-point

Варианты настройки: Auto/Forced True/Forced False

По умолчанию: Auto

Функция: Установка типа соединения для порта. Если порт подключен к соединению точка-точка, порт может быстро перейти в другое состояние.

Описание: «Auto» указывает, что коммутатор автоматически определяет тип соединения на основе дуплексного статуса порта. Когда порт работает в полнодуплексном режиме, коммутатор определяет тип соединения, подключенного к порту, как точка-точка; когда порт работает в полудуплексном режиме, тип соединения определяется как общее. «Forced True» означает, что соединение, подключенное к порту, является соединением точка-точка, а «Forced False» означает, что соединение общее.

7.5.4.6 Пример типовой настройки

Приоритеты коммутаторов A, B и C – 0, 4096 и 8192. Стоимость пути каналов связи – 4, 5 и 10, как показано на следующем рисунке.

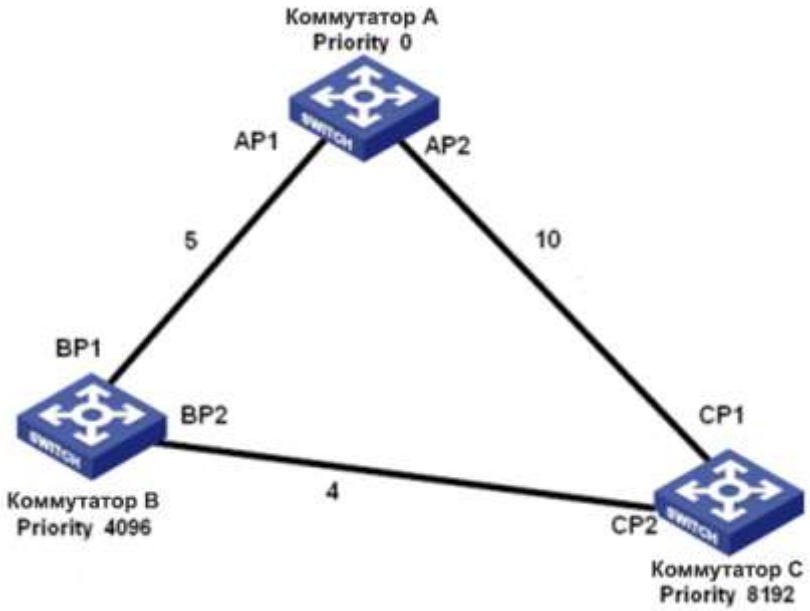


Рисунок 154 – Пример конфигурации RSTP

Настройка коммутатора A:

1. Установите приоритет на «0» и временные параметры на значения по умолчанию, как показано на рисунке 152.

2. Установите стоимость пути для порта 1 на «5», а для порта 2 на «10», как показано на рисунке 153.

Настройка коммутатора B:

1. Установите приоритет на «4096» и временные параметры на значения по умолчанию, как показано на рисунке 152.

2. Установите стоимость пути для порта 1 на «5», а для порта 2 на «4», как показано на рисунке 153.

Настройка коммутатора C:

1. Установите приоритет на «8192» и временные параметры на значения по умолчанию, как показано на рисунке 152.

2. Установите стоимость пути для порта 1 на «10», а для порта 2 на «4», как показано на рисунке 153.

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

7.5.5 MSTP

7.5.5.1 Введение

Хотя протокол RSTP обеспечивает достаточно быструю сходимость, он имеет такой же недостаток, как и STP: все мосты в локальной сети используют одно связующее дерево, и по нему пересылаются пакеты всех VLAN. Как показано на рисунке 155, определенные конфигурации могут блокировать связь между коммутаторами A и C. Поскольку коммутаторы B и D не входят в VLAN 1, они не могут пересылать пакеты VLAN 1. В результате порт VLAN 1 коммутатора A не может связываться с соответствующим портом коммутатора C.

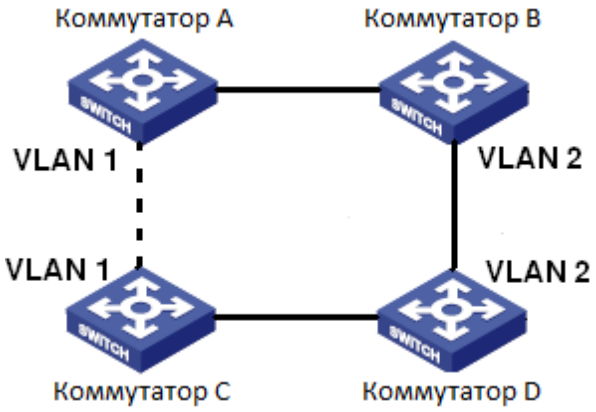


Рисунок 155 – Недостаток RSTP

Чтобы решить эту проблему, появился протокол MSTP. Он предоставляет как быструю конвергенцию, так и отдельные пути пересылки трафика разных VLAN для обеспечения лучшего механизма распределения нагрузки для каналов резервирования. MSTP группирует одну или несколько VLAN в один экземпляр (инстанцию). Коммутаторы с одинаковой конфигурацией образуют регион (область). Каждый регион содержит несколько взаимно независимых связующих деревьев. Регион служит коммутационным

узлом. Он участвует в вычислениях с другими регионами на основе алгоритма связующего дерева, вычисляя общее дерево. На основе этого алгоритма сеть на рисунке 155 образует топологию, показанную на рисунке 156. Коммутаторы A и C находятся в регионе 1. Ни один канал связи не заблокирован, потому что в регионе отсутствуют петли. Ситуация аналогична и для региона 2. Регионы 1 и 2 по сути аналогичны коммутационным узлам. Эти два «коммутатора» образуют петлю. Следовательно, линия связи должна быть заблокирована.

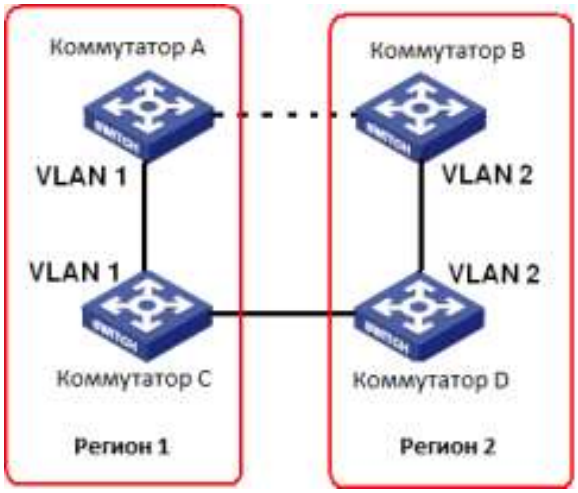


Рисунок 156 – Топология MSTP

7.5.5.2 Основные понятия

Концепция работы MSTP отображена на рисунках 157 – 160.

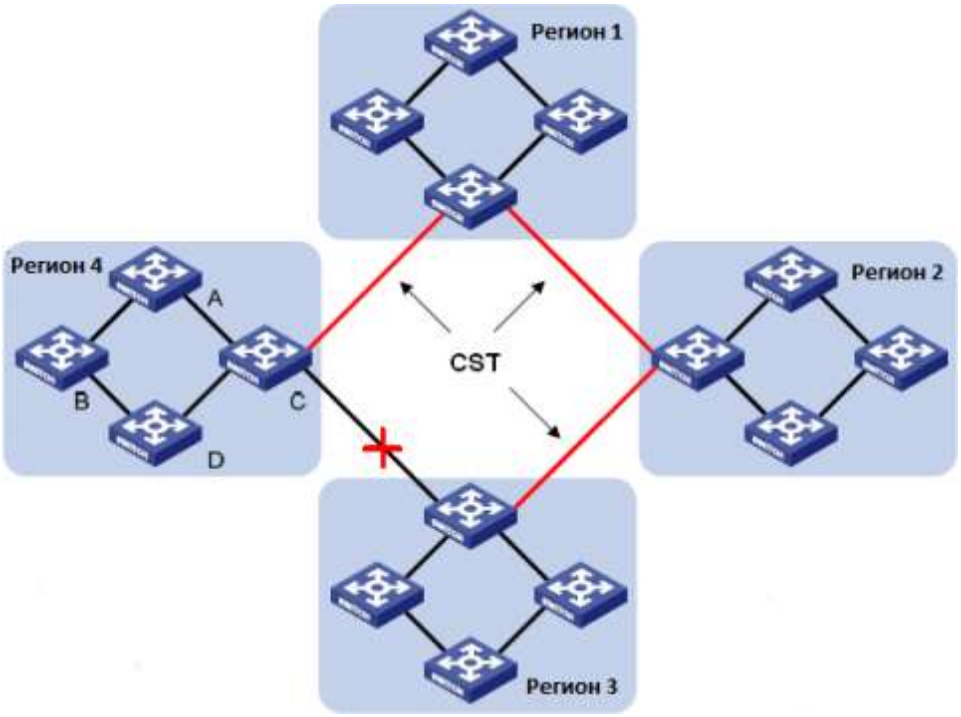


Рисунок 157 – Концепция MSTP

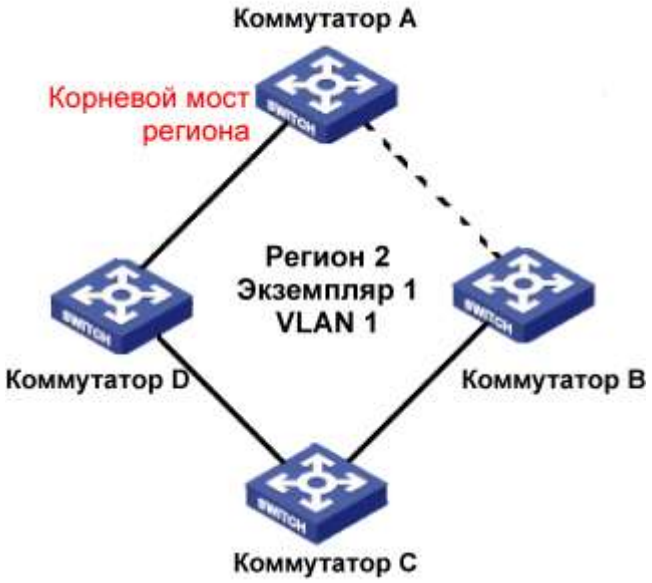


Рисунок 158 – Привязка VLAN 1 к экземпляру 1

Рисунок 159 – Привязка VLAN 2 к экземпляру 2

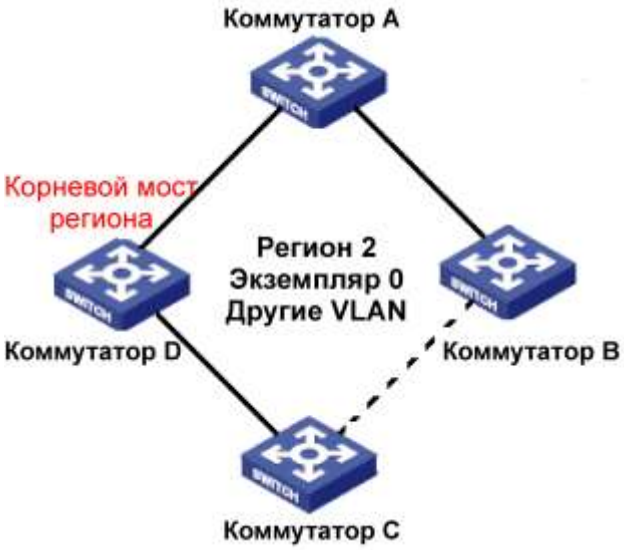


Рисунок 160 – Привязка других VLAN к экземпляру 0

Экземпляр (инстанция): набор из нескольких VLAN. Одна VLAN (см. рисунки 158 и 159) или несколько VLAN с одинаковой топологией (см. рисунок 160) могут быть сопоставлены с одним экземпляром; то есть одна VLAN может сформировать связующее дерево, а несколько VLAN могут совместно использовать одно связующее дерево. Разные экземпляры сопоставляются с разными связующими деревьями. Экземпляр 0 – это связующее дерево для устройств всех регионов, а другие экземпляры – это связующие деревья для устройств определенного региона.

Регион MST: коммутаторы с одинаковым именем региона MSTP, уровнем версии и привязкой VLAN к экземпляру находятся в одном регионе MST. Как показано на рисунке 157, регионы 1, 2, 3 и 4 – это четыре разных области MST.

Таблица сопоставления VLAN: состоит из сопоставления между VLAN и связующими деревьями. Для топологии на рисунке 157 таблица региона 2 будет содержать сопоставление между VLAN 1 и экземпляром 1, как показано на рисунке 158; VLAN 2 привязана к экземпляру 2, как показано на рисунке 159. Другие VLAN сопоставлены с экземпляром 0, как показано на рисунке 160.

CIST: общее и внутреннее связующее дерево. Означает экземпляр 0, то есть связующее дерево, охватывающее все устройства в сети. Как показано на рисунке 157, CIST состоит из IST и CST.

IST: внутреннее связующее дерево. Означает сегмент CIST в области MST, то есть экземпляр 0 для каждого региона, как показано на рисунке 160.

CST: общее связующее дерево. Означает связующее дерево, соединяющее все регионы MST в сети. Если каждый регион MST является узлом, а CST – это связующее дерево, вычисленное этими узлами на основе STP/RSTP. Красные линии обозначают связующее дерево (см. рисунок 157).

MSTI: экземпляр множественного связующего дерева. Один регион MST может образовывать несколько связующих деревьев, и они не зависят друг от друга. Каждое

связующее дерево является MSTI (см. рисунки 158 и 159). IST также является специальным MSTI.

Общий корень: означает корневой мост CIST. Коммутатор с наименьшим идентификатором корневого моста в сети является общим корневым коммутатором. В регионе MST связующие деревья имеют разную топологию и их корневые мосты также могут быть разными. Как показано на рисунках 158, 159 и 160, у этих трех экземпляров разные региональные корневые мосты. Корневой мост MSTI рассчитывается на основе STP/RSTP в текущем регионе MST. Корневой мост IST – это устройство, которое подключено к другому региону MST и выбирается на основе полученной информации о приоритете.

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

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

статус пересылки (Forwarding state): означает, что порт изучает MAC-адреса и выполняет пересылку пакетов;

статус обучения (Learning state): означает, что порт изучает MAC-адреса, но не осуществляет пересылку пакетов;

статус отбрасывания (Discarding state): означает, что порт не изучает MAC-адреса и не осуществляет пересылку пакетов.

Корневой порт: это наилучший порт подключения некорневого моста к корневому мосту, то есть порт с наименьшими затратами для корневого моста. Некорневой мост взаимодействует с корневым мостом именно через корневой порт. Некорневой мост имеет только один корневой порт, при этом у корневого моста нет корневого порта. Корневой порт может находиться в состоянии пересылки, обучения или отбрасывания.

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

Мастер-порт: главный, основной порт, который соединяет регион MST с общим корневым мостом и имеет к нему кратчайший путь. Относительно CST, главный порт – это корневой порт региона (как узел). Мастер-порт – это специальный граничный порт. Он является корневым для CIST и главным для других экземпляров. Мастер-порт может находиться в состоянии пересылки, обучения или отбрасывания.

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

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

7.5.5.3 Реализация

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

1. Расчет CIST.

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

2. Расчет MSTI.

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

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

7.5.5.4 Настройка с помощью WEB-интерфейса

1. Настройте временные параметры сетевого моста, как показано ниже.

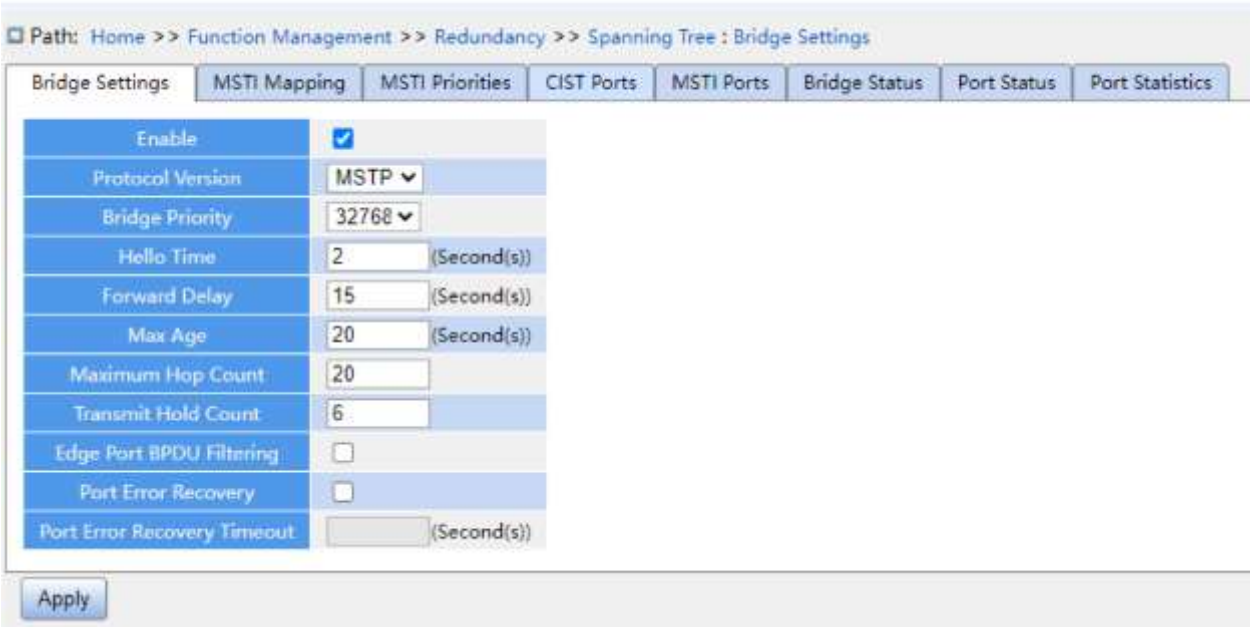


Рисунок 161 – Настройка временных параметров сетевого моста

Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение протокола связующего дерева.

- К протоколам на основе портов относятся RSTP, Sy2-Ring-Port и Sy2-RP-Port, а к протоколам на основе VLAN – MSTP, Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Протоколы на основе портов и VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один тип протокола.

Protocol Version

Варианты настройки: MSTP/RSTP/STP

По умолчанию: MSTP

Функция: выбор протокола связующего дерева.

Bridge Priority

Диапазон: 0–61440; Шаг – 4096.

По умолчанию: 32768

Функция: настройка приоритета сетевого моста.

Описание: приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

Hello Time

Диапазон: 1–10 с

По умолчанию: 2 с

Функция: настройка интервала отправки BPDU.

Forward Delay

Диапазон: 4–30 с

По умолчанию: 15 с

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

Max Age

Диапазон: 6–40 с

По умолчанию: 20 с

Функция: возраст сообщения, то есть, максимальная продолжительность, в течение которой BPDU может быть сохранен на устройстве.

Описание: если значение Max Age в BPDU больше указанного при настройке, то BPDU отбрасывается.

- Значения Forward Delay, Hello Time и Max Age должны соответствовать следующим требованиям: 2*(Forward Delay – 1,0 с) ≥ Max Age; Max Age ≥ 2*(Hello Time + 1,0 с).
- Рекомендуется использовать настройку по умолчанию.

Maximum Hop Count

Диапазон: 6–40

По умолчанию: 20

Функция: настройка максимального количества переходов для области MST. Максимальное количество переходов ограничивает масштаб региона MST; максимальное количество переходов для корневого моста области является максимальным количеством переходов для всей области MST.

Описание: начиная с корневого моста в области MST, количество переходов уменьшается на 1 при прохождении BPDU через каждое устройство в области. Устройство отбрасывает BPDU, если количество переходов достигает 0.

- Действительной является только конфигурация Maximum Hop Count корневого моста в MST-регионе. Устройства, не являющиеся корневыми, принимают значение, настроенное для корневого моста.
- Рекомендуется использовать настройку по умолчанию.

Transmit Hold Count

Диапазон: 1–10

По умолчанию: 6

Функция: указание максимального количества пакетов BPDU, которые могут быть отправлены портом в течение каждого интервала Hello Time.

Edge Port BPDU Filtering

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: управление получением и пересылкой пакетов BPDU на граничном порту.

Port Error Recovery

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: управление возможностью автоматического восстановления порта из состояния ошибки в нормальное рабочее состояние.

Port Error Recovery Timeout

Диапазон: 30–86400 с

Функция: настройка времени для восстановления порта из состояния ошибки в нормальное рабочее состояние.

2. Настройте сопоставление MSTI, как показано ниже.

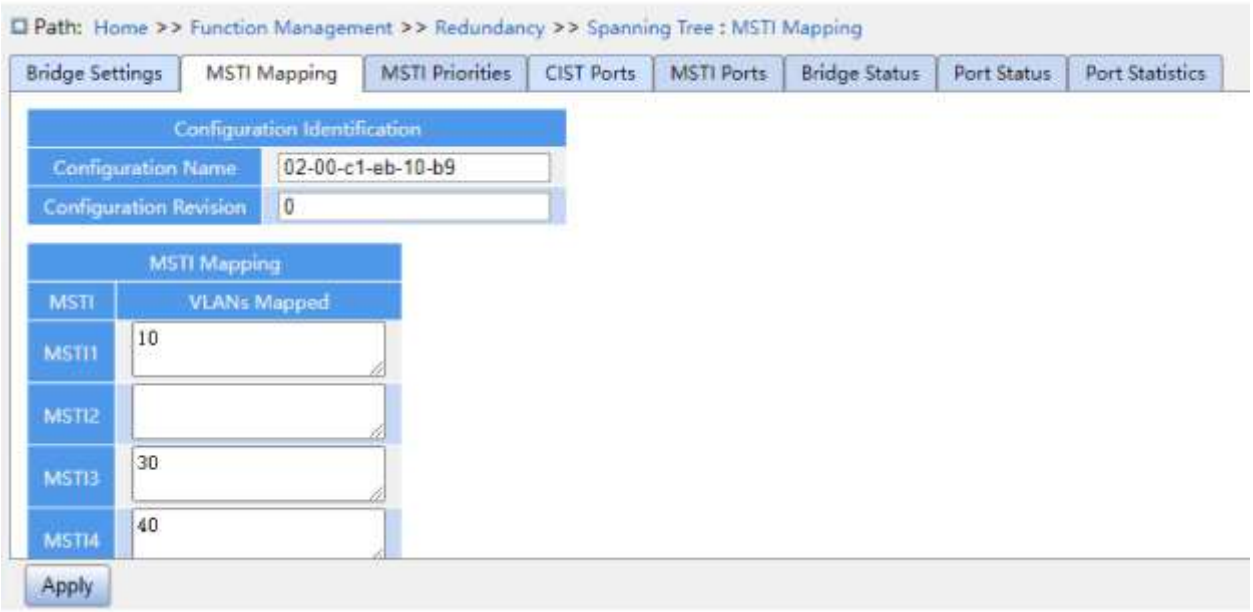


Рисунок 162 – Настройка сопоставления MSTI

Configuration Name

Диапазон: 1–32 символа

По умолчанию: MAC-адрес устройства

Функция: настройка имени региона MST.

Configuration Revision

Варианты настройки: 0–65535

По умолчанию: 0

Функция: указание номера ревизии региона MSTP.

Описание: параметр ревизии, имя региона MST и таблица сопоставления VLAN определяют регион MST, к которому принадлежит устройство. Если все настройки одинаковы, устройства находятся в одном регионе.

VLANs Mapped

Диапазон: 1–4094

Функция: настройка таблицы сопоставления VLAN в регионе MST. При наличии нескольких VLAN вы можете разделить VLAN запятой (,) и дефисом (-), где дефис используется для разделения двух крайних идентификаторов последовательного диапазона VLAN, а запятая используется для разделения двух непоследовательных идентификаторов.

Описание: по умолчанию все VLAN привязываются к экземпляру 0. Одна VLAN сопоставляется только с одним экземпляром связующего дерева. Если VLAN с существующей привязкой сопоставляется с другим экземпляром, предыдущая настройка отменяется. Если сопоставление между определенной VLAN и экземпляром удалено, эта VLAN будет сопоставлена с экземпляром 0.

3. Настройте приоритет моста коммутатора в указанном экземпляре, как показано ниже.

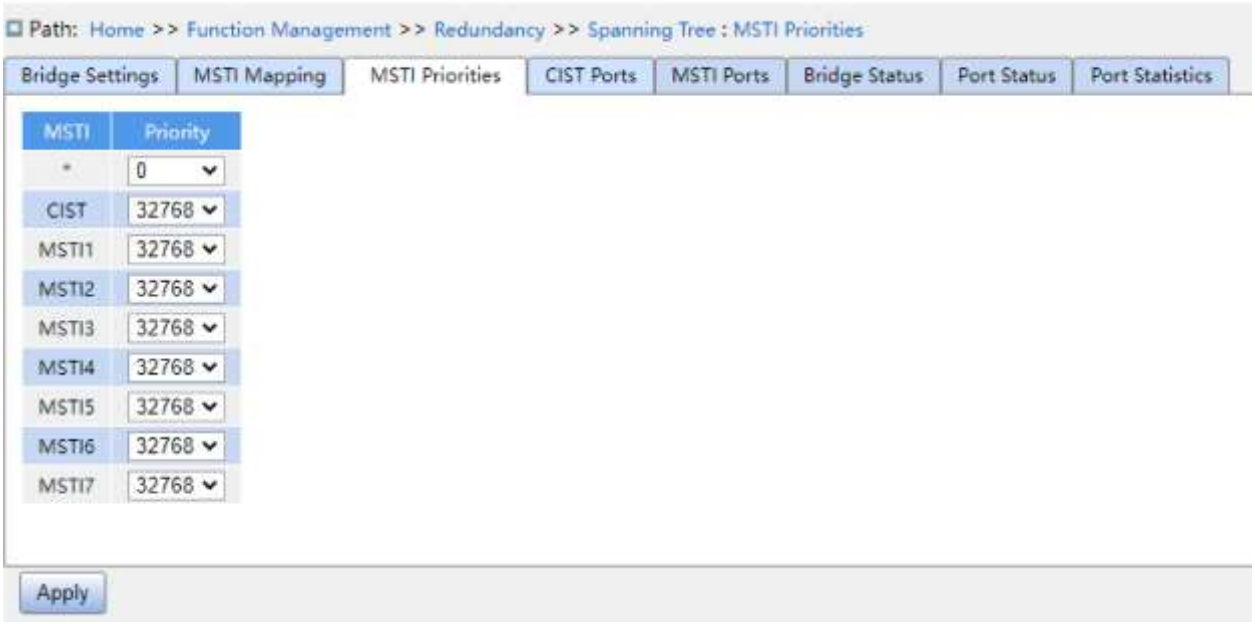


Рисунок 163 – Настройка приоритета моста

Priority

Диапазон: 0–61440 с длиной шага 4096

По умолчанию: 32768

Функция: настройка приоритета моста коммутатора в указанном экземпляре.

Описание: приоритет моста определяет, может ли коммутатор быть выбран в качестве регионального корня экземпляра связующего дерева. Чем меньше значение, тем выше приоритет, позволяющий устройству быть назначенным корневым мостом связующего дерева. Устройство с поддержкой MSTP можно настроить с разными приоритетами в разных экземплярах связующего дерева. Нажмите <Apply>, чтобы текущие настройки вступили в силу.

4. Настройте порты CIST, как показано ниже.

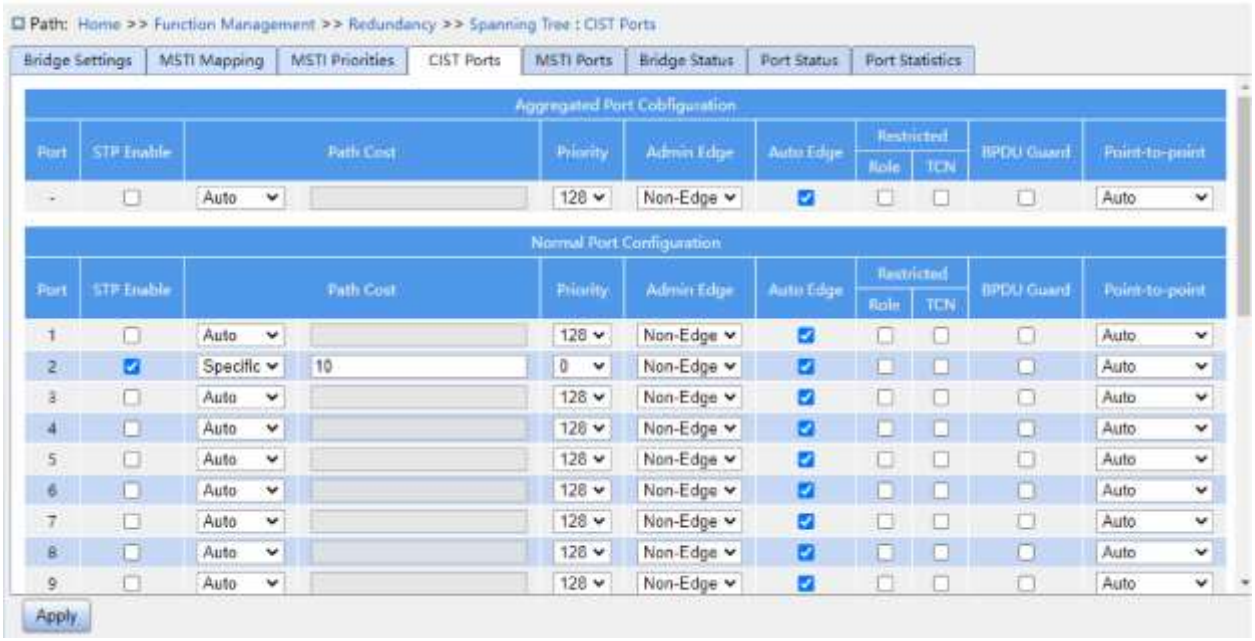


Рисунок 164 – Настройка портов CIST

STP Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение STP/RSTP на портах.

Порт MSTP нельзя добавить в группу агрегации; порт из группы агрегации не может быть настроен как порт MSTP.

Path Cost

Варианты настройки: Auto/Specific (1–200000000)

По умолчанию: Auto

Описание: данная функция используется для расчета наилучшего пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, поменяв его стоимость пути. Чтобы настроить значение вручную, выберите для параметра режим «Specific».

Priority

Диапазон: 0–240; шаг: 16

По умолчанию: 128

Функция: настройка приоритета порта, который определяет его роль.

Admin Edge

Варианты настройки: Non-Edge/Edge

По умолчанию: Non-Edge

Функция: указывает, является ли текущий порт граничным портом.

Описание: когда порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, он считается граничным. Граничный порт может быстро перейти из состояния блокировки в состояние пересылки без ожидания окончания интервала «Forward Delay». Если граничный порт начинает получать пакеты BPDU, он перестает быть граничным.

Auto Edge

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение/отключение функции автоматического определения, является ли текущий порт граничным.

Restricted Role

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: ограничение ролей. Порт, для которого включена эта функция, никогда не будет выбран в качестве корневого узла, даже если ему предоставлен наивысший приоритет.

Restricted TCN

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: ограничение сообщений об изменении топологии. Порт, для которого включена эта функция, не будет активно отправлять сообщения TCN.

BPDU Guard

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: указывает, переходит ли граничный порт в состояние Error-Disable и отключается ли он при получении пакетов BPDU.

Point-to-point

Варианты настройки: Auto/Forced True/Forced False

По умолчанию: Auto

Функция: Установка типа соединения для порта. Если порт подключен к соединению точка-точка, порт может быстро перейти в другое состояние.

Описание: «Auto» указывает, что коммутатор автоматически определяет тип соединения на основе дуплексного статуса порта. Когда порт работает в полнодуплексном режиме, коммутатор определяет тип соединения, подключенного к порту, как точка-точка; когда порт работает в полудуплексном режиме, тип соединения определяется как общее.

«Forced True» означает, что соединение, подключенное к порту, является соединением точка-точка, а «Forced False» означает, что соединение общее.

5. Настройте порты MSTI, как показано ниже.

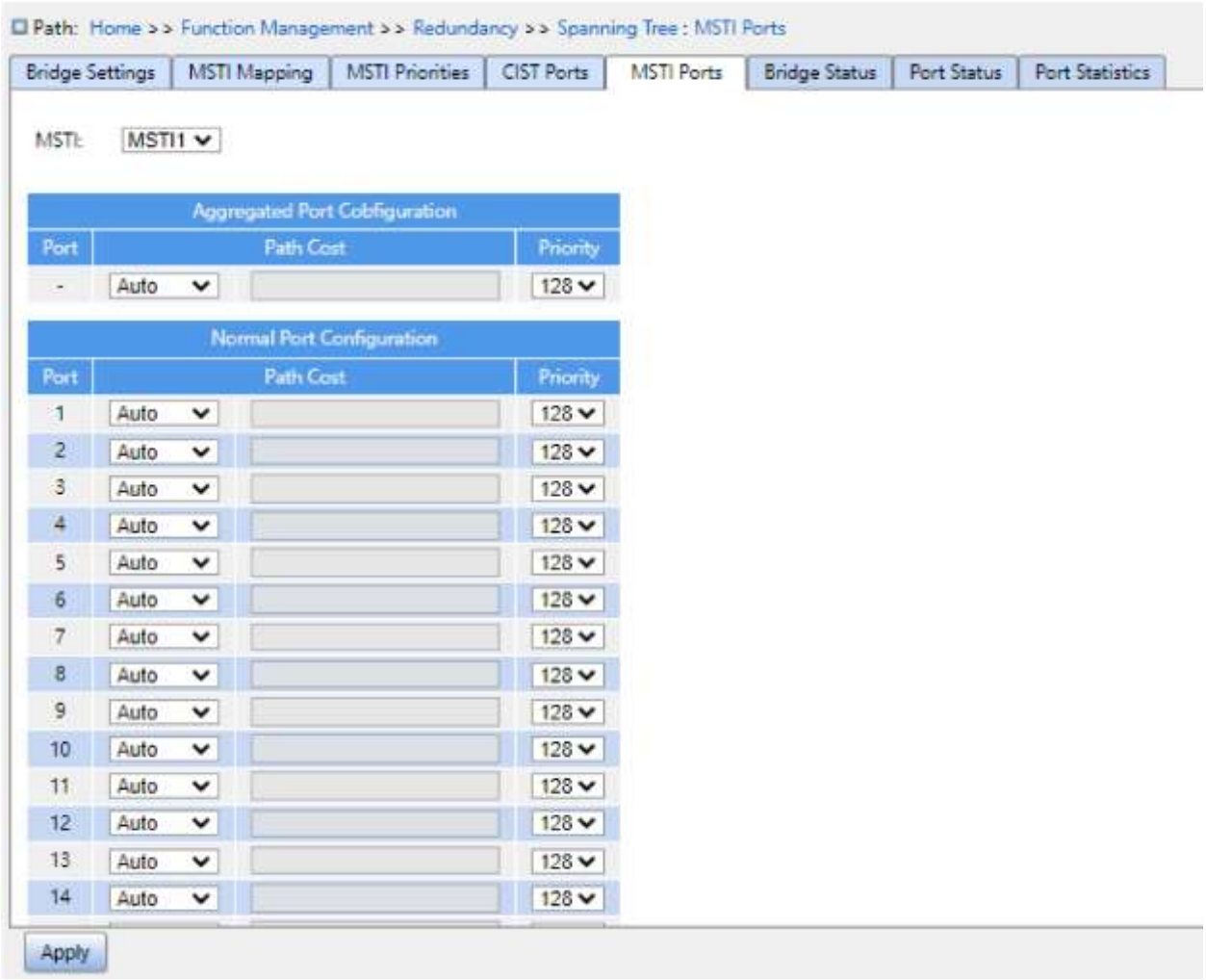


Рисунок 165 – Настройка портов MSTI

MSTI

Диапазон: MST1–MST7

По умолчанию: MST1

Функция: выбор MSTI.

Aggregated Port Configuration

Функция: выбор группы агрегации в качестве порта MSTP и настройка ее стоимости пути и приоритета в указанном экземпляре.

Path Cost

Варианты настройки: Auto/Specific (1–200000000)

По умолчанию: Auto

Функция: настройка стоимости пути порта в указанном экземпляре.

Описание: данная функция используется для расчета наилучшего пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Изменение стоимости пути порта может изменить путь передачи между устройством и корневым мостом, тем самым изменяя роль порта. Порт с поддержкой MSTP может быть настроен с различной стоимостью пути в различных экземплярах связующего дерева. Чтобы настроить значение вручную, выберите для параметра режим «Specific».

Priority

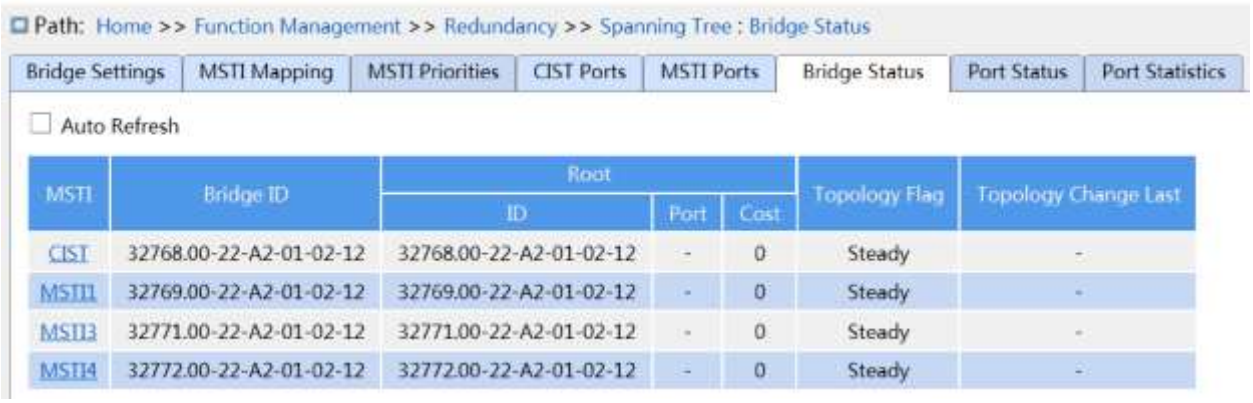
Диапазон: 0–240; шаг: 16

По умолчанию: 128

Функция: настройка приоритета порта в указанном экземпляре.

Описание: приоритет порта определяет, может он быть выбран в качестве корневого. При прочих равных условиях порт с более низким значением будет выбран в качестве корневого. Порты с поддержкой MSTP могут быть настроены с разными приоритетами и играть разные роли в разных экземплярах связующего дерева. Нажмите кнопку <Apply>, чтобы текущая конфигурация вступила в силу.

6. Просмотрите состояние моста, как показано ниже.



MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-22-A2-01-02-12	32768.00-22-A2-01-02-12	-	0	Steady	-
MSTI1	32769.00-22-A2-01-02-12	32769.00-22-A2-01-02-12	-	0	Steady	-
MSTI3	32771.00-22-A2-01-02-12	32771.00-22-A2-01-02-12	-	0	Steady	-
MSTI4	32772.00-22-A2-01-02-12	32772.00-22-A2-01-02-12	-	0	Steady	-

Рисунок 166 – Статус моста

7. Просмотрите статус STP на портах, как показано ниже.

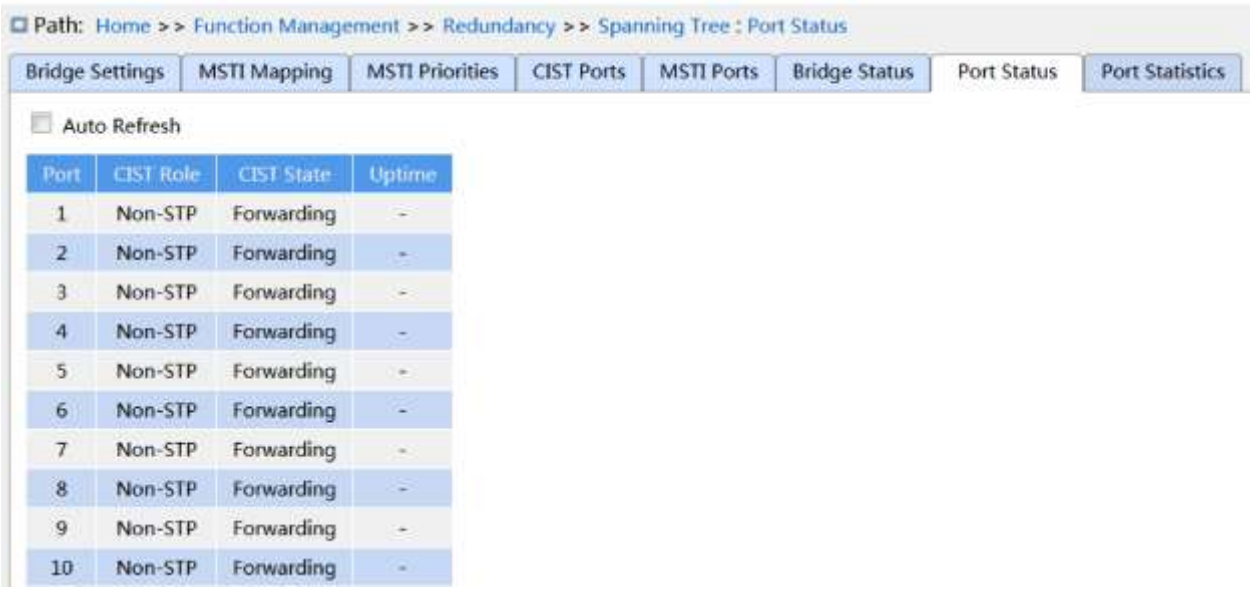


Рисунок 167 – Статус STP на портах

8. Просмотрите статистику пакетов на STP-портах, как показано ниже.

Рисунок 168 – Статистика сообщений STP

7.5.5.5 Пример типовой настройки

Как показано на рисунке 169, коммутаторы A, B, C и D принадлежат одному и тому же региону MST. VLAN, отмеченные красным, означают, что пакеты VLAN могут быть переданы по каналам связи. После завершения настройки пакеты VLAN можно пересылать по разным экземплярам связующего дерева. Пакеты VLAN 10 пересылаются по экземпляру 1, а корневым мостом экземпляра 1 является коммутатор A. Пакеты VLAN 30 пересылаются по экземпляру 3, а корневой мост экземпляра 3 – это коммутатор B. Пакеты VLAN 40 пересылаются по экземпляру 4, а корневой мост экземпляра 4 – это коммутатор C. Пакеты VLAN 20 пересылаются по экземпляру 0, а корневым мостом экземпляра 0 является коммутатор B.

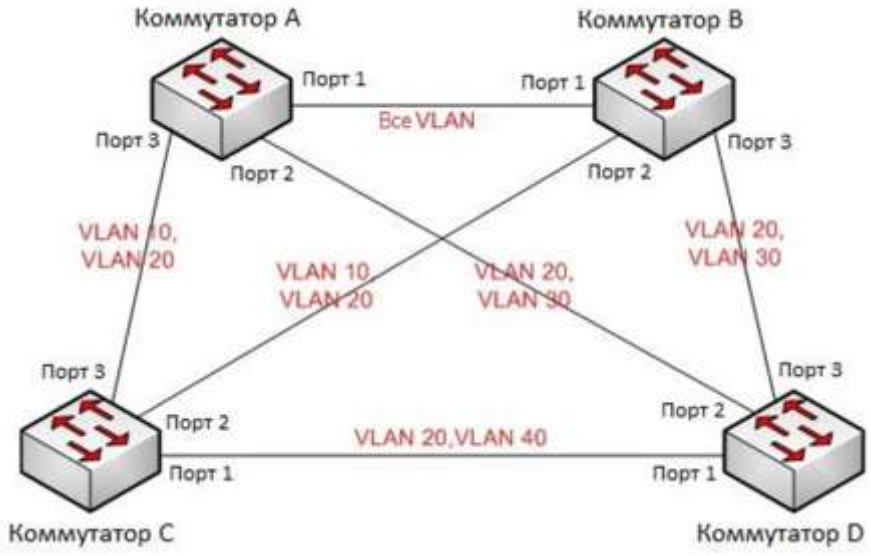


Рисунок 169 – Пример типовой настройки MSTP

Настройка коммутатора A:

1. Создайте VLAN 10, 20 и 30 на коммутаторе A; на портах установите разрешение на прохождение пакетов, соответствующих VLAN.

2. Включите глобальный протокол MSTP (см. рисунок 161).

3. Задайте для имени региона MST значение «Region», а для параметра «Configuration Revision» – 0 (см. рисунок 165).

4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно (см. рисунок 165).

5. Установите приоритет моста коммутатора в MSTI 1 на 4096 и сохраните приоритет по умолчанию в других экземплярах (см. рисунок 163).

Настройка коммутатора B:

1. Создайте VLAN 10, 20 и 30 на коммутаторе B; на портах установите разрешение на прохождение пакетов, соответствующих VLAN.

2. Включите глобальный протокол MSTP (см. рисунок 161).

3. Задайте для имени региона MST значение «Region», а для параметра «Configuration Revision» – 0 (см. рисунок 165).

4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно (см. рисунок 165).

5. Установите приоритет моста коммутатора в MSTI 3 и MSTI 0 на 4096 и сохраните приоритет по умолчанию в других экземплярах (см. рисунок 163).

Настройка коммутатора C:

1. Создайте VLAN 10, 20 и 40 на коммутаторе C; на портах установите разрешение на прохождение пакетов, соответствующих VLAN.

2. Включите глобальный протокол MSTP (см. рисунок 161).

3. Задайте для имени региона MST значение «Region», а для параметра «Configuration Revision» – 0 (см. рисунок 165).

4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно (см. рисунок 165).

5. Установите приоритет моста коммутатора в MSTI 4 на 4096 и сохраните приоритет по умолчанию в других экземплярах (см. рисунок 163).

Настройка коммутатора D:

1. Создайте VLAN 20, 30 и 40 на коммутаторе D; на портах установите разрешение на прохождение пакетов, соответствующих VLAN.

2. Включите глобальный протокол MSTP (см. рисунок 161).

3. Задайте для имени региона MST значение «Region», а для параметра «Configuration Revision» – 0 (см. рисунок 165).

4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно (см. рисунок 165).

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

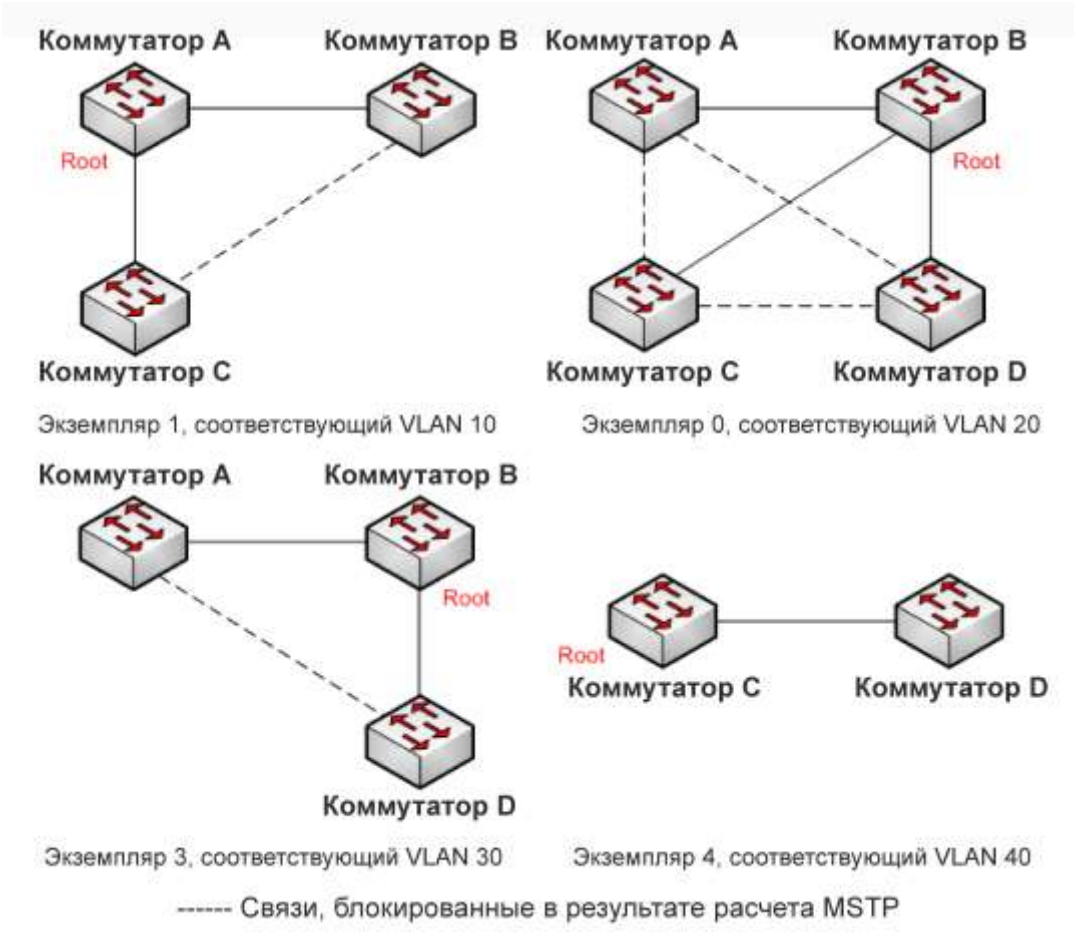


Рисунок 170 – Экземпляры связующего дерева для каждой VLAN

7.6 ARP

7.6.1 Введение

Address Resolution Protocol (ARP) – протокол разрешения адресов, определяющий соответствие между IP-адресом и MAC-адресом через механизм запросов и ответов. Коммутатор может запоминать соответствие между IP-адресом и MAC-адресом устройств в сети. Также коммутаторы поддерживают статические записи ARP, связывающие IP- и MAC-адреса. Динамические ARP-записи периодически устаревают, что обеспечивает обновление информации.

Данные коммутаторы поддерживают не только коммутацию второго уровня, но и ARP-разрешение адресов, обеспечивая взаимодействие между NMS и управляемыми устройствами.

7.6.2 Описание

Записи ARP делятся на статические и динамические.

Динамические записи генерируются и поддерживаются на основании полученных коммутатором ARP-запросов. Динамические записи могут устаревать, обновляться благодаря обмену ARP-запросами и перезаписываться статическими записями.

Статические записи вводятся вручную и также вручную поддерживаются. Они не устаревают и не перезаписываются динамически.

7.6.3 Proxy ARP

Proxy ARP – это функция, при которой шлюз может отвечать на ARP-запросы, отправленные с одного хоста в сети на другой хост, находящийся в той же логической сети, но не на том же физическом сегменте. Это позволяет устройствам в разных физических сетях взаимодействовать друг с другом, используя ARP.

Процесс Proxy ARP выглядит следующим образом:

1. Исходный хост отправляет ARP-запрос, пытаясь узнать MAC-адрес хоста в другой физической сети.

2. Шлюз, непосредственно подключенный к исходному хосту и имеющий включенную функцию Proxy ARP на интерфейсе VLAN, получает этот запрос. Если у него есть нормальный маршрут к целевому хосту, он отвечает на запрос, подменяя MAC-адрес целевого хоста своим собственным.

3. IP-сообщения, отправленные исходным хостом на целевой хост, направляются на устройство с включенной функцией Proxy ARP.

4. Шлюз выполняет нормальную маршрутизацию IP-сообщений.

5. IP-сообщения, отправленные на целевой хост, достигают его через сеть.

7.6.4 Настройка с помощью WEB-интерфейса

1. Настройте элементы таблицы статических адресов ARP, как показано ниже.

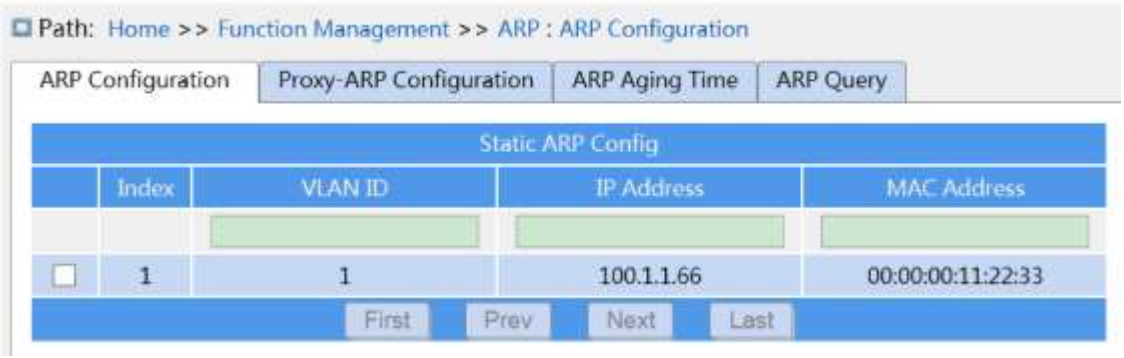


Рисунок 171 – Настройка таблицы статических адресов

VLAN ID

Варианты настройки: созданный интерфейс L3 VLAN

Диапазон: 1–4094

Функция: выбор интерфейса L3 VLAN текущего элемента таблицы ARP.

IP address

Формат конфигурации: A.B.C.D

Функция: настройка IP-адресов для статических элементов таблицы ARP.

MAC address

Формат конфигурации: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)

Функция: настройка MAC-адресов статических элементов таблицы ARP.

Как правило, коммутатор автоматически изучает элементы таблицы ARP, и администратору не нужно настраивать статические адреса.

Ниже показана настройка Proxy ARP.

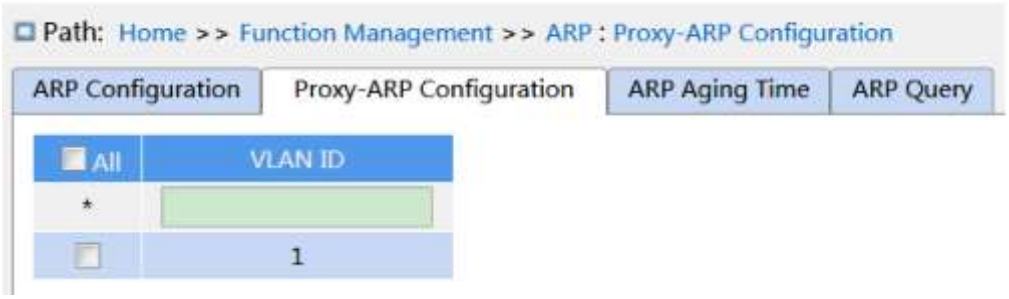


Рисунок 172 – Настройка Proxy ARP

VLAN ID

Диапазон: 1–4094

Функция: выбор интерфейса L3 включенного прокси-ARP.

3. Ниже показана настройка времени устаревания ARP.

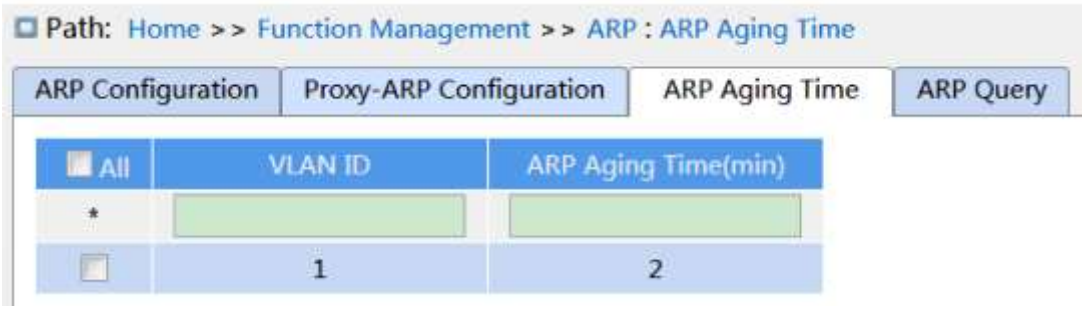


Рисунок 173 – Настройка времени устаревания ARP

VLAN ID

Диапазон: 1–4094

Функция: указывает интерфейс L3 для настройки времени устаревания ARP

ARP Aging Time

Диапазон: 1– 60 мин

По умолчанию: 5 мин

Функция: настройка времени устаревания ARP

Описание: отсчет времени начинается с момента добавления динамической записи в таблицу ARP. По истечении указанного времени запись будет удалена из таблицы.

4. Ниже показан просмотра текущего состояния таблицы ARP на коммутаторе.

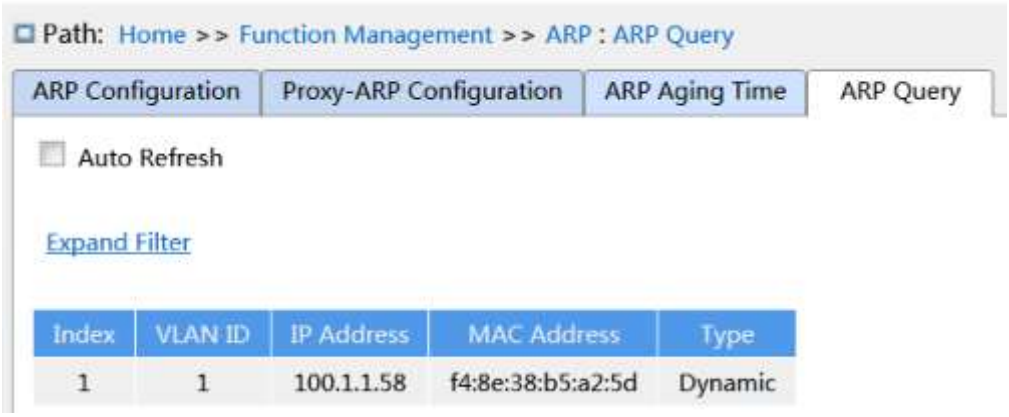


Рисунок 174 – Просмотр ARP

ARP Query

Отображаемые параметры: {Index, VLAN ID, IP Address, MAC Address, Type}

Функция: отображение элементов таблицы ARP.

Описание: этот список отображает все элементы таблицы ARP, соответствующие состоянию активных на данный момент портов. В таблице могут быть как статические, так и динамические записи.

7.7 ACL

7.7.1 Введение

С развитием сетевых технологий вопросы безопасности становятся все более актуальными, требуя механизма контроля доступа. С помощью функции списка управления доступом (ACL) коммутатор сопоставляет пакеты со списком для реализации запрета и разрешения трафика различных устройств согласно определенным правилам.

7.7.2 Реализация

Коммутаторы данной серии фильтруют пакеты в соответствии с выбранным для сопоставления списком ACL. Каждая запись состоит из нескольких условий в логическом отношении «И». Записи ACL независимы друг от друга.

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

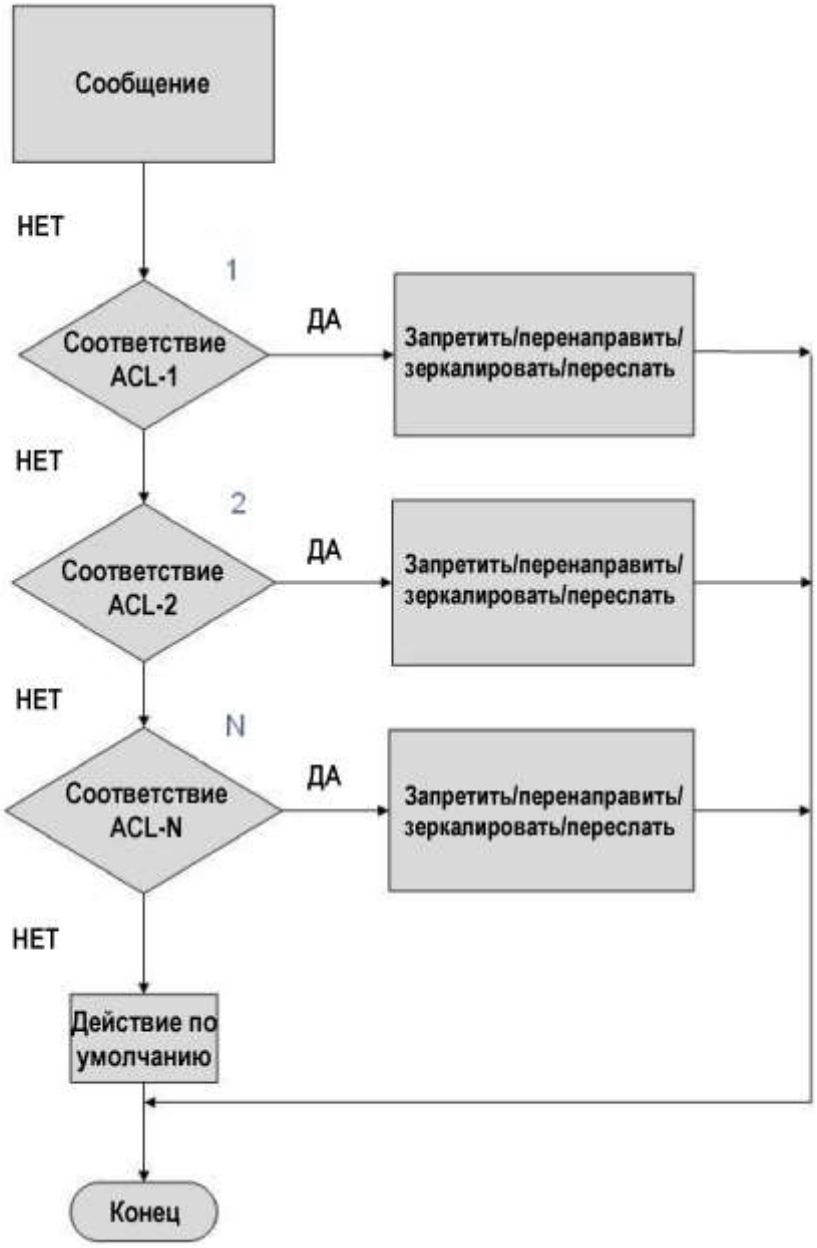


Рисунок 175 – Блок-схема обработки ACL

Действие по умолчанию указывает на режим обработки пакетов, не соответствующих ни одной записи ACL.

7.7.3 Настройка с помощью WEB-интерфейса

1. Настройте ограничители скорости для ACL, как показано ниже.

Рисунок 176 – Настройка полисеров

Policer ID

Диапазон: 1–16

Описание: номер полисера (ограничителя скорости)

Rate, Unit

Диапазон: 0–5000000 pps (шаг 10) / 0–10000000 Kbps (шаг 25)

По умолчанию: 10 pps

Функция: настройка предельной скорости, соответствующей указанному идентификатору полисера.

2. Настройте элемент таблицы ACL, как показано ниже.

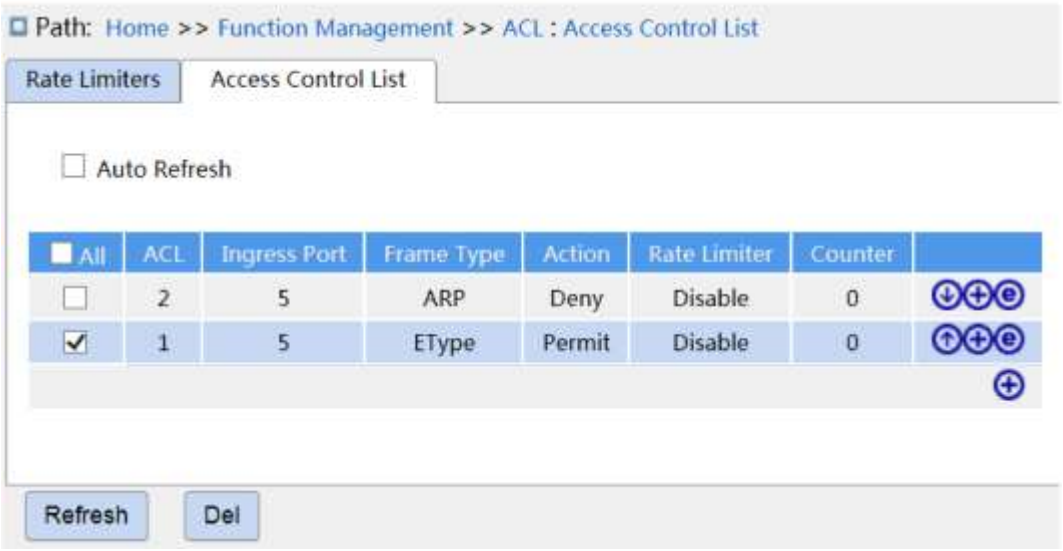


Рисунок 177 – Настройка элемента таблицы ACL

Если в таблице ACL существует несколько элементов, устройство сравнивает с ними сообщения один за другим (сверху вниз). Как только для сообщения обнаруживается соответствующий первый элемент таблицы ACL, немедленно выполняется соответствующее действие.

Нажмите кнопку <⊕>, чтобы создать элемент таблицы ACL. Нажмите кнопку <ⓔ>, чтобы отредактировать текущий элемент таблицы. Нажмите кнопку <⬆>, чтобы переместить текущий элемент таблицы вверх. Нажмите кнопку <⬇>, чтобы переместить текущий элемент таблицы вниз. Нажмите <☑>, затем нажмите кнопку <Del>, чтобы удалить текущий элемент таблицы.

3. Настройка правил ACL

➢ Настройте параметры элемента таблицы ACL, как показано ниже.

Рисунок 178 – Настройка элемента ACL

ACL

Диапазон: 1–512

Функция: настройка идентификатора элемента таблицы ACL.

Ingress port

Варианты настройки: любой указанный порт

Функция: указание порта для данного элемента ACL.

Frame type

Варианты настройки: Any/Ethernet Type/IPv4/ARP

По умолчанию: Any

Функция: настройка условного параметра ACL – тип кадра. Условие успешно выполняется, когда тип кадра, полученный входящим портом, соответствует конфигурации параметра.

Action

Варианты настройки: Deny/Permit

По умолчанию: Permit

Функция: метод обработки портом кадра, соответствующего элементу таблицы ACL.

Deny: отбросить кадр, соответствующий элементу таблицы ACL.

Permit: переслать кадр, соответствующий элементу таблицы ACL.

Rate Limiter

Диапазон: Disable/1–16

По умолчанию: Disable

Функция: включение или отключение ограничителя скорости порта и выбор нужного номера полисера.

Counter

Функция: подсчет количества кадров, полученных входным портом, которые соответствуют ACL.

VLAN ID filter

Варианты настройки: Any/Specific (1–4094)

По умолчанию: Any

Функция: настройка условного параметра ACL – VID. При выборе «Specific» необходимо настроить значение VID. Когда VID полученного кадра с порта входящего трафика удовлетворяет настроенному параметру, условие успешно выполняется.

- Настройте параметры ACL для кадров типа Ethernet, как показано ниже.

Рисунок 179 – Параметры для кадров Ethernet

SMAC Filter

Варианты настройки: Any/Specific

По умолчанию: Any

Функция: настройка условного параметра ACL – MAC-адреса источника. Если выбрано «Specific», необходимо указать исходный MAC-адрес кадра. Когда с порта входящего трафика приходит кадр с таким адресом, условие успешно выполняется.

DMAC Filter

Варианты настройки: Any/Specific

По умолчанию: Any

Функция: настройка условного параметра ACL – MAC-адреса назначения. Если выбрано «Specific», необходимо указать MAC-адрес назначения кадра. Когда с порта входящего трафика приходит кадр с таким адресом, условие успешно выполняется.

Ether Type Filter

Варианты настройки: Any/Specific (0x600–0xFFFF)

По умолчанию: Any

Функция: настройка условного параметра – типа Ethernet. Если выбрано «Specific», необходимо указать тип Ethernet. Когда полученный Ethernet-кадр удовлетворяет настроенному параметру, условие успешно выполняется.

- Настройте параметры для кадров ARP.

SMAC Filter

Варианты настройки: Any/Specific

По умолчанию: Any

Функция: настройка условного параметра ACL – MAC-адреса источника. Если выбрано «Specific», необходимо указать исходный MAC-адрес кадра. Когда с порта входящего трафика приходит кадр с таким адресом, условие успешно выполняется.

ARP/RARP

Варианты настройки: Any/ARP/RARP

По умолчанию: Any

Функция: настройка условного параметра – типа кадра. Когда полученный с порта входящего трафика тип кадра удовлетворяет настроенному параметру, условие успешно выполняется.

Source IP Filter

Варианты настройки: Any/Host/Network

По умолчанию: Any

Функция: настройка условного параметра – исходного IP-адреса. Если выбрано «Host», необходимо настроить определенный IP-адрес. если выбрано «Network», необходимо настроить IP-адрес и маску. Когда исходный IP-адрес полученного кадра удовлетворяет настроенному параметру, условие успешно выполняется.

Destination IP Filter

Варианты настройки: Any/Host/Network

По умолчанию: Any

Функция: настройка условного параметра – IP-адреса назначения. Если выбрано «Host», необходимо настроить определенный IP-адрес. если выбрано «Network», необходимо настроить IP-адрес и маску. Когда IP-адрес назначения полученного кадра удовлетворяет настроенному параметру, условие успешно выполняется.

- Настройте параметры для кадров IPv4, как показано ниже.

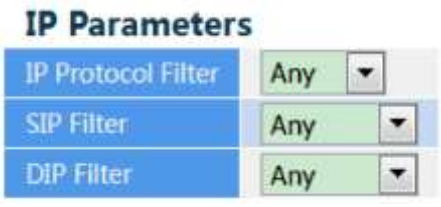


Рисунок 180 – Настройка параметров для IP-кадра

IP Protocol Filter

Варианты настройки: Any/ICMP/UDP/TCP/Other (0~255)

По умолчанию: Any

Функция: настройка условного параметра – типа протокола кадра IPv4. Если выбрано «ICMP/UDP/TCP», необходимо настроить соответствующие параметры. Если выбрано «Other», необходимо указать номер протокола. Если тип протокола полученного кадра IPv4 с входного порта удовлетворяет настроенному параметру, условие успешно выполнено.

SIP Filter

Варианты настройки: Any/Host/Network

По умолчанию: Any

Функция: настройка условного параметра – исходного IP-адреса. Если выбрано «Host», необходимо настроить определенный IP-адрес. если выбрано «Network», необходимо настроить IP-адрес и маску. Когда исходный IP-адрес полученного кадра IPv4 с порта входящего трафика удовлетворяет настроенному параметру, условие успешно выполняется.

DIP Filter

Варианты настройки: Any/Host/Network

По умолчанию: Any

Функция: настройка условного параметра – IP-адреса назначения. Если выбрано «Host», необходимо настроить определенный IP-адрес. если выбрано «Network», необходимо настроить IP-адрес и маску. Когда IP-адрес назначения полученного кадра IPv4 с порта входящего трафика удовлетворяет настроенному параметру, условие успешно выполняется.

- Настройте параметры ICMP, как показано ниже.

Рисунок 181 – Настройка параметров ICMP

ICMP Type Filter

Варианты настройки: Any/Specific (0–255)

По умолчанию: Any

Функция: настройка условного параметра – значения типа ICMP. если выбрано «Specific», необходимо указать значение. Когда значение типа ICMP полученного кадра IPv4 с порта входящего трафика удовлетворяет настроенному параметру, условие успешно выполняется.

ICMP Code Filter

Варианты настройки: Any/Specific (0–255)

По умолчанию: Any

Функция: настройка условного параметра – значения кода ICMP. если выбрано «Specific», необходимо указать значение. Когда значение кода ICMP полученного кадра IPv4 с порта входящего трафика удовлетворяет настроенному параметру, условие успешно выполняется.

➢ Настройте параметры UDP, как показано ниже.

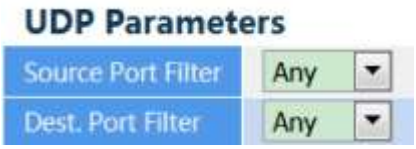


Рисунок 182 – Настройка параметров UDP

Source Port Filter/Destination Port Filter

Варианты настройки: Any/Range (0–65535)

По умолчанию: Any

Функция: настройка условного параметра – номера исходного и конечного порта UDP. Если выбрано «Range», необходимо настроить диапазон номеров портов. Когда номер порта UDP полученного кадра IPv4 с порта входящего трафика удовлетворяет настроенному параметру, условие успешно выполняется.

➢ Настройте параметры TCP, как показано ниже.

Рисунок 183 – Настройка параметров TCP

Source Port Filter/Destination Port Filter

Варианты настройки: Any/Range (0–65535)

По умолчанию: Any

Функция: настройка условного параметра – номера исходного и конечного порта TCP. Если выбрано «Range», необходимо настроить диапазон номеров портов. Когда номер порта TCP полученного кадра IPv4 с порта входящего трафика удовлетворяет настроенному параметру, условие успешно выполняется.

7.7.4 Пример типовой настройки

Подключите порт 2 коммутатора. Настройте порт для приема пакетов только с исходного MAC-адреса 02-02-02-02-02-02 и пересылайте пакеты через порт 1.

Этапы настройки:

1. Создайте ACL1, укажите входной порт 2, в поле «Action» выберите «Permit», укажите тип кадра «Ethernet Type», как показано на рисунке 178.

2. Настройте для записи ACL1, параметры Ethernet, установите фильтр SMAC на 02-02-02-02-02-02, как показано на рисунке 179.

3. Создайте ACL, укажите входной порт 2, в поле «Action» выберите «Deny», как показано на рисунке 178.

4. Оставьте все остальные параметры с настройками по умолчанию или пустыми.

7.8 Настройка MAC-адресов

7.8.1 Введение

При пересылке пакета коммутатор выбирает порт для отправки в таблице MAC-адресов на основе MAC-адреса назначения пакета.

MAC-адрес может быть статическим или динамическим.

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

Динамические MAC-адреса изучаются коммутатором при пересылке данных. Они действительны только в течение определенного периода. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра данных для пересылки коммутатор узнает исходный MAC-адрес кадра, устанавливает сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса назначения кадра. Если совпадение найдено, коммутатор пересылает кадр данных с соответствующего порта. Если совпадение не найдено, коммутатор транслирует кадр в своем широковещательном домене.

Время устаревания начинается с момента добавления динамического MAC-адреса в таблицу MAC-адресов. Если ни один порт не получает кадр с этим MAC-адресом в пределах одного-двух периодов времени устаревания, коммутатор удаляет данную запись из таблицы динамических адресов. Записи статических MAC-адресов не зависят от времени устаревания.

7.8.2 Настройка с помощью WEB-интерфейса

1. Настройте время устаревания MAC-адресов, как показано ниже.

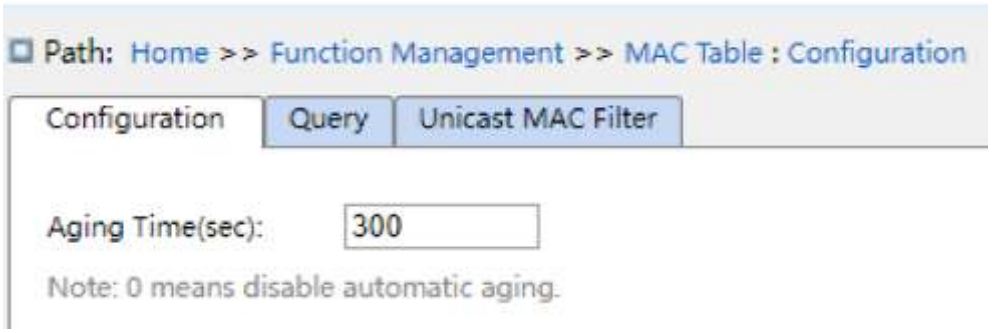


Рисунок 184 – Настройка времени устаревания

Aging Time

Диапазон: 0 или 10–1000000 с

По умолчанию: 300 с

Функция: установка времени устаревания для записи динамического MAC-адреса.

2. Настройте элементы таблицы статических MAC-адресов, как показано ниже.

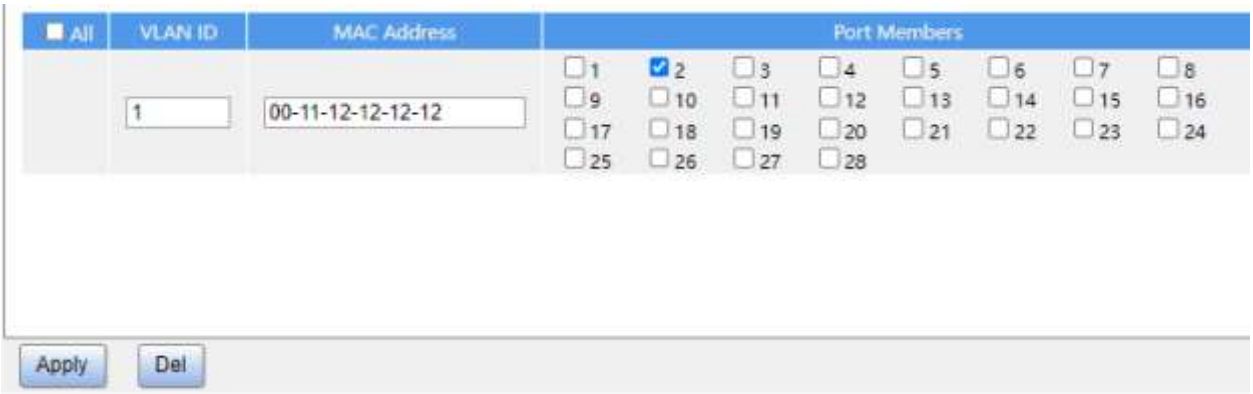


Рисунок 185 – Настройка статического MAC-адреса

VLAN ID

Варианты настройки: все созданные VLAN ID

По умолчанию: VLAN 1

Функция: настройка VLAN ID статического MAC-адреса.

MAC address

Формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число)

Функция: настройка MAC-адреса. Для юникастового MAC-адреса младший бит в первом байте равен 0. Для мультикастового MAC-адреса младший бит в первом байте равен 1.

Port Members

Функция: выбор портов для пересылки пакетов с этим MAC-адресом назначения.

Нажмите <Add New Static Entry>, чтобы добавить новую запись статического MAC-адреса. Поддерживается до 64 записей статических адресов.

3. Просмотрите таблицу MAC-адресов, как показано ниже.

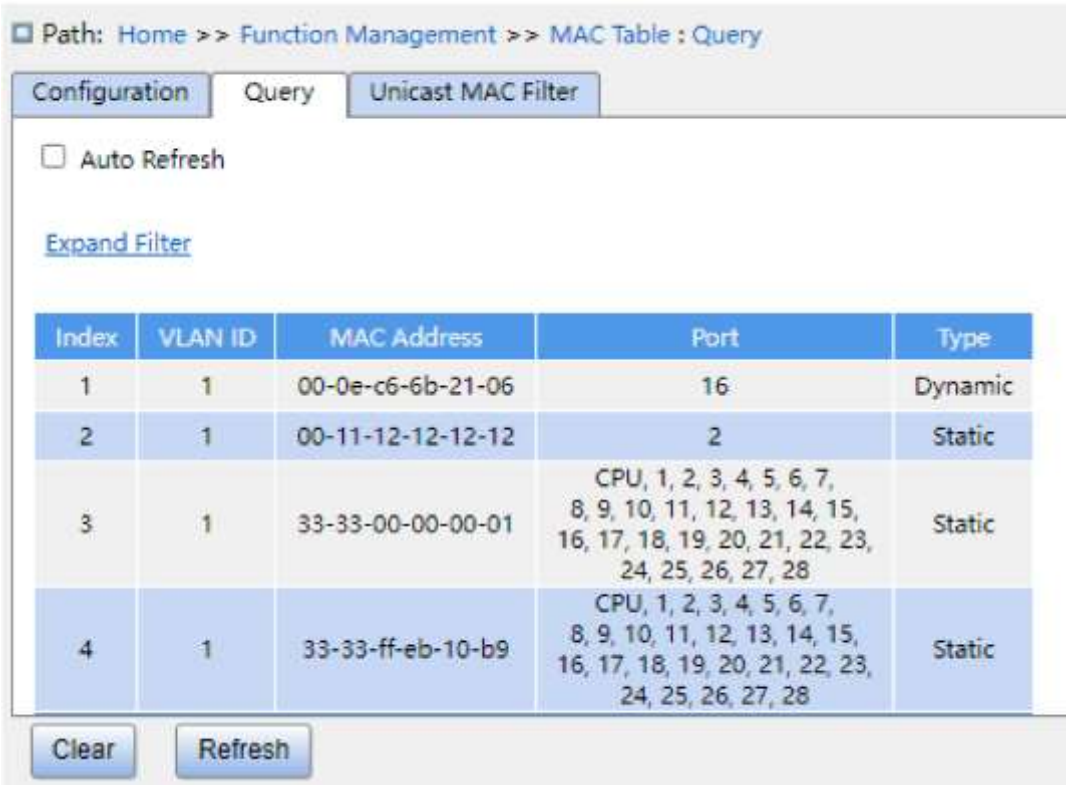


Рисунок 186 – Таблица MAC-адресов

VLAN ID

Варианты настройки: */≥/≤/select range

По умолчанию: *

Функция: отображение таблицы MAC-адресов в соответствии с выбранным VLAN ID.

MAC Address

Варианты настройки: */≥/≤/select range

По умолчанию: *

Функция: отображение таблицы MAC-адресов в соответствии с выбранным MAC-адресом.

Port

Варианты настройки: */include/not include

По умолчанию: *

Функция: отображение таблицы MAC-адресов в соответствии с выбранным портом.

Type

Варианты настройки: */static/dynamic

По умолчанию: *

Функция: отображение таблицы MAC-адресов в соответствии с выбранным типом.

4. Настройте фильтр MAC-адресов Unicast, как показано ниже.

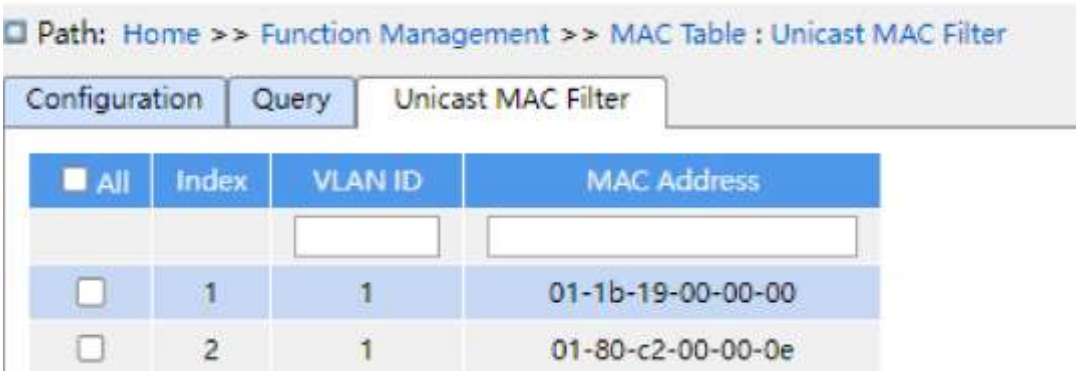


Рисунок 187 – Фильтр юникастовых адресов

VLAN ID

Варианты настройки: все созданные VLAN ID

Функция: настройка VLAN ID статического MAC-адреса.

MAC address

Формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число)

Функция: настройка MAC-адреса. Для юникастового MAC-адреса младший бит в первом байте равен 0. Для мультикастового MAC-адреса младший бит в первом байте равен 1.

7.9 PoE

7.9.1 Введение

PoE (Power Over Ethernet) означает, что коммутатор может подавать питание по витой паре удаленно через порт Ethernet. Расстояние надежной передачи питания составляет до 100 м. Данная технология эффективно решает проблему централизованного питания для IP-телефонов, беспроводных точек доступа, портативных зарядных устройств, камер наблюдения, программаторов карт и т. д. При этом отпадает необходимость прокладки внутренней системы электропитания, поскольку питание подается на оборудование одновременно с подключением к сети.

Последовательный коммутатор PoE соответствует стандарту IEEE 802.3at. Основная терминология включает в себя PSE и PD:

PSE (Power Sourcing Equipment) – это устройство, которое подает питание на другое устройство.

PD (Powered Device) – это устройство, которое получает в системе PoE.

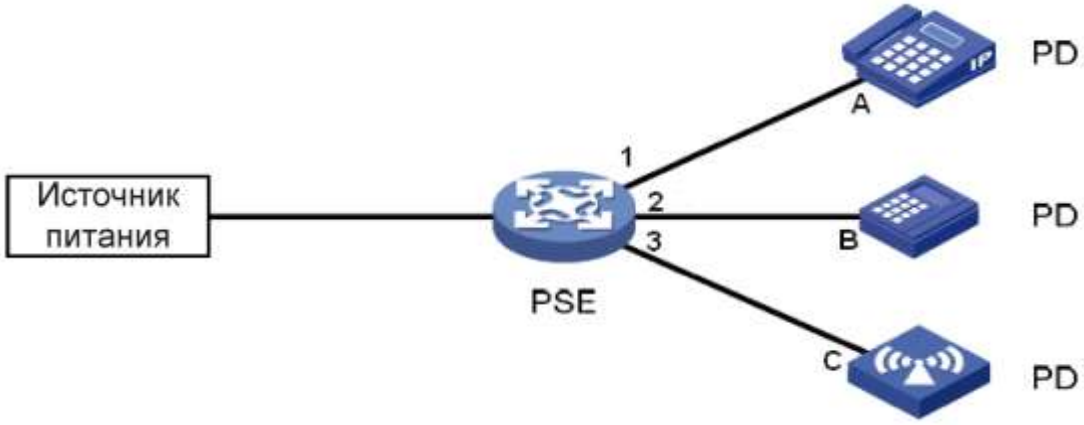


Рисунок 188 – Система подачи питания PoE

7.9.2 Настройка с помощью WEB-интерфейса

1. Ниже показана глобальная настройка функции PoE.

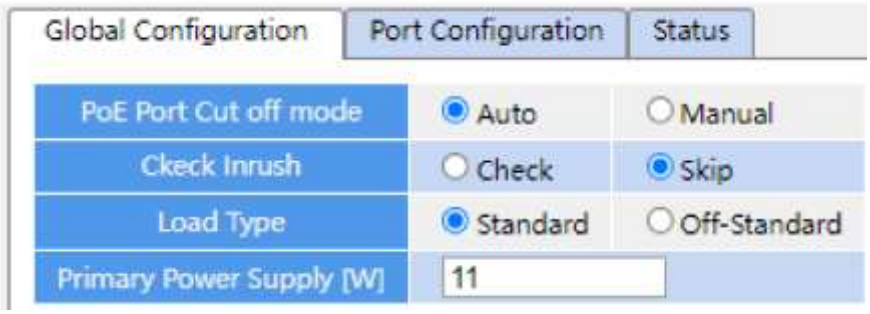


Рисунок 189 – Глобальная конфигурация PoE

PoE Port Cut off mode

Варианты настройки: Auto/Manual

По умолчанию: Auto

Функция: настройка режима управления питанием PoE.

Описание: когда общая потребляемая мощность всех устройств PD превышает максимальную мощность, которую может обеспечить PSE, в ручном режиме PSE подает питание в соответствии с порядком доступа устройств PD, то есть первым подается питание на первое доступное устройство PD. В автоматическом режиме PSE подает питание на подключенные устройства PD в соответствии с приоритетом питания порта.

Check Inrush

Варианты настройки: Check/Skip

По умолчанию: Check

Функция: проверка пускового тока устройства PD.

Load Type

Варианты настройки: Standard/Off-Standard

По умолчанию: Standard

Функция: настройка типа устройства PD, которое может быть запитано.

Primary Power Supply

Варианты настройки: 1–120 (без вспомогательного питания); 1–240 (со вспомогательным питанием)

По умолчанию: 240

Функция: позволяет настроить максимальную мощность, которую может обеспечить устройство PSE. Когда устройство используется как PSE, максимальная мощность, которую может обеспечить вся машина:

без вспомогательного источника питания максимальная мощность составляет 120 Вт;

с внешним вспомогательным источником питания максимальная мощность составляет 240 Вт.

Если общая потребляемая мощность всех устройств PD превышает значение конфигурации, последнее доступное устройство PD (ручной режим) или устройство PD с самым низким приоритетом (автоматический режим) не смогут быть запитаны.

2. Ниже показана настройка функции PoE на портах.

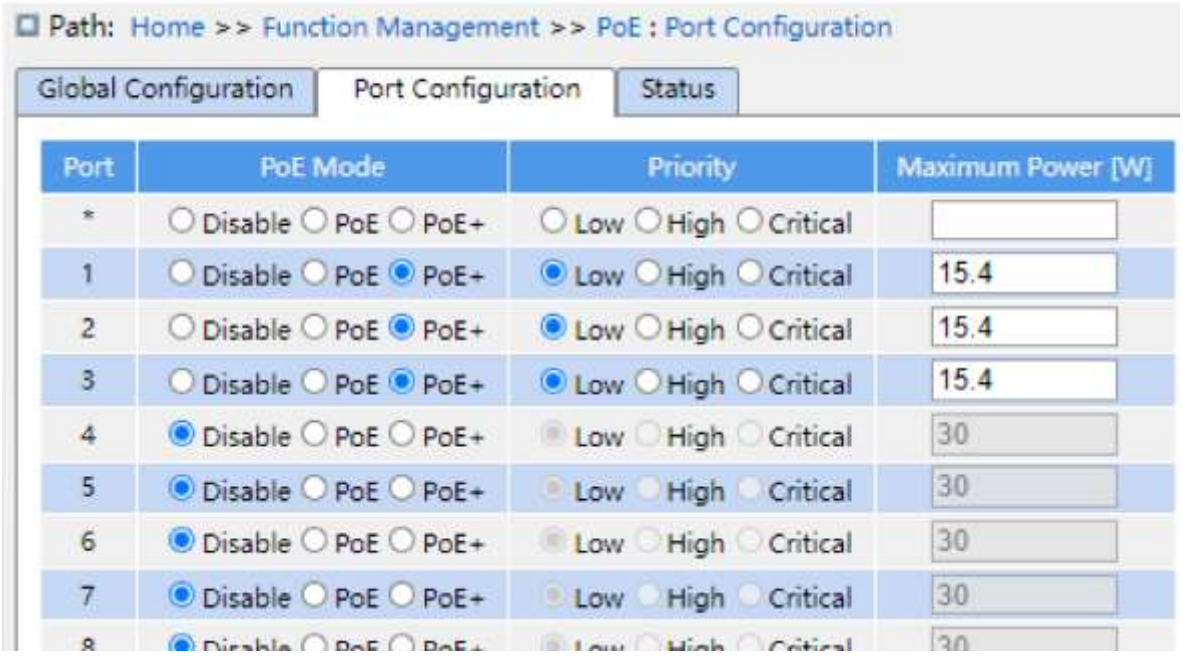


Рисунок 190 – Настройка PoE на портах

PoE Mode

Варианты настройки: Disable/PoE/PoE+

По умолчанию: Disable

Функция: включение и выбор режима PoE порта.

PoE: 100M Ethernet поддерживает выход PoE, соответствующий IEEE802.3af;

PoE+: 100M Ethernet поддерживает выход PoE, соответствующий IEEE802.3at.

Priority

Варианты настройки: Low/High/Critical

Функция: настройка приоритета питания порта. «Low» – самый низкий приоритет, «High» – второстепенный приоритет, «Critical» – самый высокий приоритет.

Maximum Power [W]

Диапазон: 1–15,4 Вт (PoE)/1–30,0 Вт (PoE+)

Функция: настройка максимальной выходной мощности порта PoE. Если потребляемая мощность подключенного к порту устройства PD превышает это значение конфигурации, устройство PD не сможет быть запитано. В соответствии с фактическими условиями пользователь может самостоятельно настроить предел выходной мощности, удовлетворяющий требованиям по электропитанию для каждого порта.

3. Просмотрите текущее состояние PoE, как показано ниже.

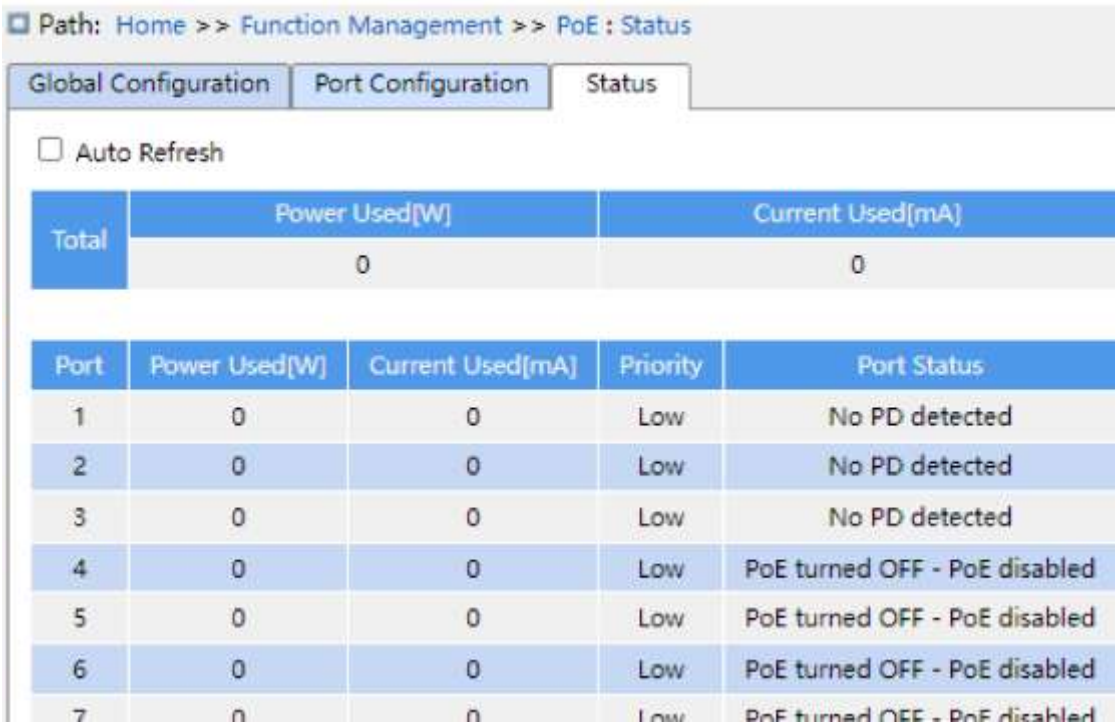


Рисунок 191 – Статус PoE

Power Used/Current Used/Priority

Функция: отображение параметров энергопотребления, тока и приоритета для портов PoE.

Port Status

Параметры отображения: No PD detected / Invalid PD / PoE turned ON / PoE turned OFF - PoE disabled / PoE turned OFF - Power budget exceeded / PoE turned OFF - PD overload / PoE turned ON - PD forced ON

Функция: отображение состояния PoE порта.

Пояснение: «No PD detected» означает, что функция PoE включена, но устройство PD не обнаружено.

«Invalid PD» означает, что функция PoE включена, устройство PD обнаружено, но питание неисправно.

«PoE turned ON» означает, что функция PoE включена, устройство PD обнаружено и происходит нормальная подача питания.

«PoE turned OFF - PoE disabled» означает отключение PoE.

«PoE turned OFF - Power budget exceeded» означает, что функция PoE включена, устройство PD обнаружено, но его подключение приводит к тому, что общее энергопотребление всех устройств PD начинает превышать максимальный лимит энергопотребления, предоставляемый для всех устройств. Таким образом, данное устройство PD не может быть запитано.

«PoE turned OFF - PD overload» означает, что функция PoE включена, устройство PD обнаружено, общее энергопотребление всех устройств PD не превышает максимальный лимит, но энергопотребление данного устройства PD превышает максимальную выходную мощность порта PoE. Устройство PD не может быть запитано.

«PoE turned ON - PD forced ON» означает включение PoE и режима принудительного питания.

7.9.3 Пример типовой настройки

Как показано на рисунке 188, максимальная мощность, обеспечиваемая коммутатором в качестве PSE, составляет 11 Вт, порты коммутатора 1 и 2 подключены к устройствам A и B, максимальная потребляемая мощность A составляет 5 Вт, максимальная потребляемая мощность B составляет 4 Вт, а порт 3 коммутатора, как ожидается, будет подключен к устройству C. Максимальная потребляемая мощность C составляет 5 Вт.

Требование:

1. Коммутатор подключен только к устройствам A и B, он может нормально подавать питание;

2. Если устройство PD C подключено к порту 3 коммутатора, общая потребляемая мощность всех устройств PD превышает максимальную мощность, которую может обеспечить коммутатор, необходимо обеспечить питание устройства C, которое первым подключено к порту 3 коммутатора.

Настройка PSE следующая:

1. Настройте параметр «PoE Port Cut off mode» на режим «Auto», а «Primary Power Supply» на 11 Вт, как показано на рисунке 189.

2. Включите функцию PoE для портов 1–3, настройте укажите приоритет порта 3 «Critical», остальные настройки оставьте по умолчанию, как показано на рисунке 190.

7.10 IGMP Snooping

7.10.1 Введение

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

Существует три версии протокола IGMP: IGMPv1, IGMPv2 и IGMPv3. IGMPv1 определен в RFC1112, IGMPv2 – в RFC2236, а IGMPv3 – в RFC3376.

IGMPv1 поддерживает два типа пакетов: пакеты отчетов (report) и запросов (query). Протокол определяет основной процесс запроса и отчета членов группы.

IGMPv2 на основе IGMPv1 предоставляет механизм быстрого выхода для членов группы. С помощью этого механизма, когда последний участник покидает группу многоадресной рассылки, маршрутизатору дается указание провести быструю конвергенцию. По сравнению с IGMPv1, IGMPv2 поддерживает два типа пакетов запросов: общий запрос и запрос, специфичный для группы. Коммутатор периодически отправляет пакет общего запроса для проверки статуса участия в группе. Когда хост покидает группу, он отправляет сообщение о выходе (пакет leave). Получив пакет leave, коммутатор отправляет пакет query, специфичный для группы, чтобы определить, все ли участники покидают данную группу.

В IGMPv3 добавлена функция фильтрации источников на стороне хоста. Благодаря этой функции устройство в сети может самостоятельно решать, хочет ли он получать или блокировать трафик от конкретных источников мультимедийных групп.

7.10.2 Основные понятия

Генератор запросов: периодически отправляет IGMP-запросы для проверки и обновления информации о многоадресных группах. Если в сети присутствует несколько запросчиков, они автоматически определяют одного (с наименьшим IP адресом), который непосредственно и будет осуществлять запросы, остальные будут их только получать и передавать.

Маршрутизирующий порт: получает общие запросы (на IGMP-коммутаторе) от главного запрашивающего устройства. При получении IGMP-ответа, коммутатор инициализирует многоадресную группу и добавляет в нее порт, на который пришел ответ. Если настроен

маршрутизирующий порт, он также добавляется. Затем коммутатор ретранслирует IGMP-ответ другим устройствам через маршрутизирующий порт.

IGMP Snooping Proxy: функция прокси в IGMP Snooping настраивается на периферийном устройстве для уменьшения количества IGMP-пакетов report и leave, получаемых вышестоящим устройством, тем самым повышая его общую производительность. Устройство, на котором настроена функция прокси, функционирует как хост для своего вышестоящего устройства и как запросчик для своего нижестоящего хоста.

7.10.3 Принцип работы

IGMP Snooping управляет участниками групп многоадресной рассылки путем обмена связанными пакетами между поддерживающими IGMP устройствами.

Пакет общего запроса: генератор запросов периодически отправляет общие запросы (с IP-адресом назначения 224.0.0.1) для уточнения, есть ли у мультикастовой группы порты-участники. При получении запроса, устройство, не являющееся генератором запросов, ретранслирует пакет на все свои порты.

Пакет запроса, специфичного для группы: если устройство хочет покинуть группу многоадресной рассылки, оно отправляет пакет IGMP leave. После получения такого пакета, запросчик отправляет пакет специфичного запроса (с IP-адресом назначения, равным IP-адресу мультикастовой группы) для удостоверения, что у коммутатора остались какие-либо порты-участники данной группы.

Пакет отчета о принадлежности: если устройство хочет получать данные группы многоадресной рассылки, оно отправляет пакет IGMP-оповещения (с IP-адресом назначения, равным IP-адресу мультикастовой группы) в ответ на IGMP-запрос группы.

Пакет leave: если устройство хочет покинуть группу многоадресной рассылки, оно отправляет IGMP-пакет leave (с IP адресом назначения: 224.0.0.2).

7.10.4 Настройка с помощью WEB-интерфейса

1. Включите IGMP Snooping, как показано ниже.

Рисунок 192 – Глобальная настройка IGMP Snooping

Snooping Enabled

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: глобальное включение/отключение протокола IGMP Snooping.

IGMP SSM Range

Формат конфигурации: A.B.C.D/4–32

По умолчанию: 232.0.0.0/8

Функция: только хосты и маршрутизаторы с адресом в пределах значения этого параметра могут запускать модель обслуживания IGMP Source Specific Multicast (SSM) при условии, что данная модель поддерживается устройствами. Модель SSM позволяет пользователям выбирать, от каких конкретных источников они хотят получать мультимедийный трафик.

Leave Proxy Enabled

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: указывает, следует ли пересылать пакеты leave запрашивающей стороне. Если эта опция включена, пакеты leave не пересылаются.

Proxy Enabled

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: указывает, следует ли пересылать пакеты leave и пакеты report об участниках группы запрашивающей стороне. Если эта опция включена, пакеты leave и отчеты об участниках не пересылаются.

Discard Unregistered Multicast

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: указывает, следует ли коммутатору отбрасывать полученные неизвестные пакеты многоадресной рассылки.

2. Настройте порты IGMP, как показано ниже.

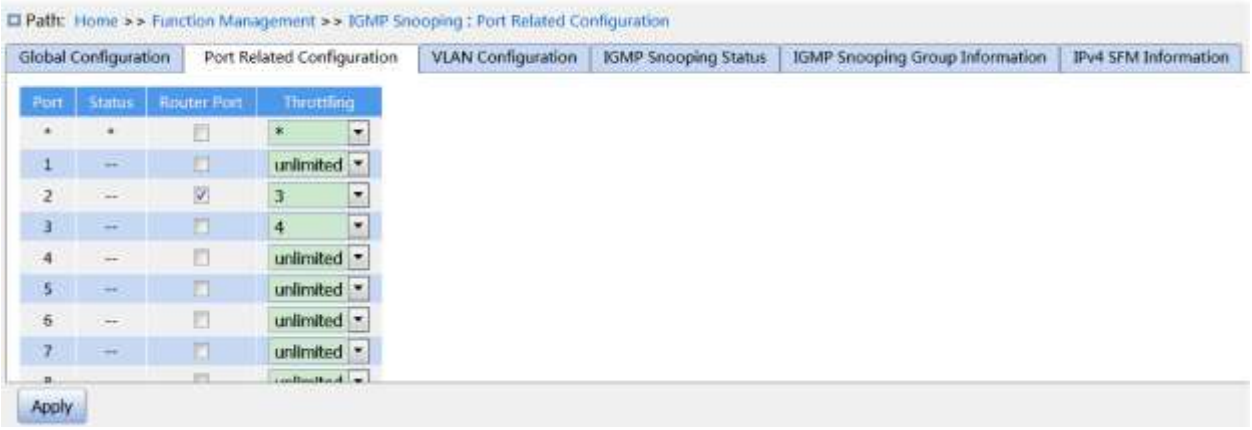


Рисунок 193 – Настройка портов IGMP

Status

Варианты настройки: --/static/dynamic/both

Функция: отображает статус порта маршрутизации.

static: порт статически настроен как маршрутизирующий. Это значит, что его конфигурация задана вручную и не изменяется.

dynamic: порт автоматически определяется как маршрутизирующий. Это значит, что его настройки могут изменяться в зависимости от сети.

both: порт может как динамически определяться, так и быть статически настроенным.

Router Port

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: позволяет включать или отключать маршрутизирующий порт. Если включено, порт будет участвовать в маршрутизации трафика, если отключено – не будет.

Throttling

Варианты настройки: unlimited/1–10

По умолчанию: unlimited

Функция: определяет, нужно ли ограничивать количество многоадресных записей, которые могут быть изучены портом.

3. Настройте IGMP Snooping для VLAN, как показано ниже.

Рисунок 194 – Настройка IGMP Snooping для VLAN

VLAN Interface

Варианты настройки: все созданные VLAN ID

Snooping Enabled

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение IGMP Snooping для указанной VLAN. Предварительным условием является глобальное включение IGMP Snooping.

Querier Election

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение/отключение функции генератора IGMP-запросов для выбранной VLAN. Предварительным условием является включение IGMP Snooping глобально и для VLAN.

Описание: если в сети есть несколько опрашивающих устройств, они автоматически выберут устройство с наименьшим IP-адресом в качестве генератора запросов. Если такое устройство только одно, оно станет генератором запросов.

Querier Address

Формат конфигурации: A.B.C.D

Функция: настройка IP-адреса источника отправки пакетов запроса. Если установлено значение 0.0.0.0, IP-адрес порта VLAN используется в качестве адреса запросчика.

Compatibility

Варианты настройки: Forced IGMPv1/Forced IGMPv2/Forced IGMPv3

По умолчанию: Forced IGMPv2

Функция: настройка версии IGMP.

PRI

Диапазон: 0–7

По умолчанию: 0

Функция: настройка приоритета пакета управления IGMP (приоритет интерфейса).

RV

Диапазон: 1–255

По умолчанию: 2

Функция: указывает «переменную надежности» функции IGMP-запросчика.

Описание: чем больше параметр, тем хуже сетевая среда. Пользователь может установить подходящий параметр надежности в соответствии с фактической сетью.

QI

Диапазон: 1–31744 с

По умолчанию: 125 с

Функция: настройка интервала отправки пакета общего запроса.

QRI

Диапазон: 0–31744 (единица измерения: 0,1 с)

По умолчанию: 100

Функция: настройка максимального времени ответа на общий запрос.

LLQI

Диапазон: 0–31744 (единица измерения: 0,1 с)

По умолчанию: 10

Функция: настройка максимального времени ответа на специфичный запрос.

Настройка параметров QI, QRI и LLQI действительна только для генератора запросов.

URI

Диапазон: 0–31744 с

По умолчанию: 1 с

Функция: установка интервала для повторной отправки хостом пакета report о присоединении к группе многоадресной рассылки.

Нажмите <Add New IGMP VLAN>, чтобы настроить новую VLAN для IGMP Snooping. Можно настроить до 32 VLAN.

4. Просмотрите состояние IGMP Snooping, как показано ниже.

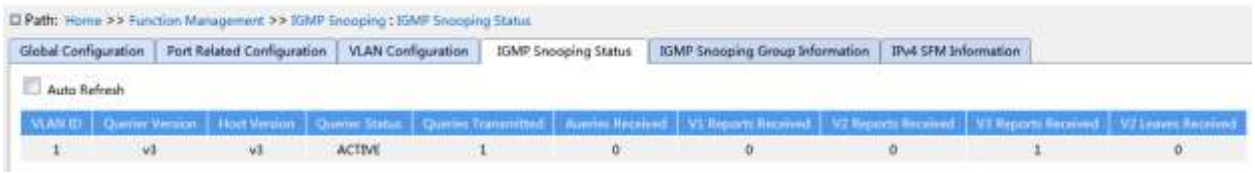


Рисунок 195 – Статус IGMP Snooping

5. Просмотрите список участников многоадресной рассылки, как показано ниже.

Рисунок 196 – Участники многоадресной рассылки

VLAN ID

Варианты настройки: */≥/≤/select range

По умолчанию: *

Функция: отображение информации о группах в соответствии с выбранным VLAN ID.

Group

Варианты настройки: */≥/≤/select range

По умолчанию: *

Функция: отображение информации о группах в соответствии с выбранным адресом.

Port Members

Варианты настройки: */include/not include

По умолчанию: *

Функция: отображение информации о группах в соответствии с выбранным портом.

Type

Варианты настройки: */static/dynamic

По умолчанию: *

Функция: отображение таблицы MAC-адресов в соответствии с выбранным типом.

6. Просмотрите информацию IPv4 SFM, как показано ниже.

Рисунок 197 – Фильтр источников

7.10.5 Пример типовой настройки

Как показано на рисунке 198, функция IGMP Snooping включена на коммутаторах 1, 2 и 3.

Опция Querier Election включена на коммутаторах 2 и 3. IP-адрес коммутатора 2 – 192.168.1.2, а коммутатора 3 – 192.168.0.2, поэтому коммутатор 3 выбран в качестве генератора запросов.

1. Включите IGMP Snooping на коммутаторе 1.
2. Включите IGMP Snooping и Querier Election на коммутаторе 2.
3. Включите IGMP Snooping и Querier Election на коммутаторе 3.

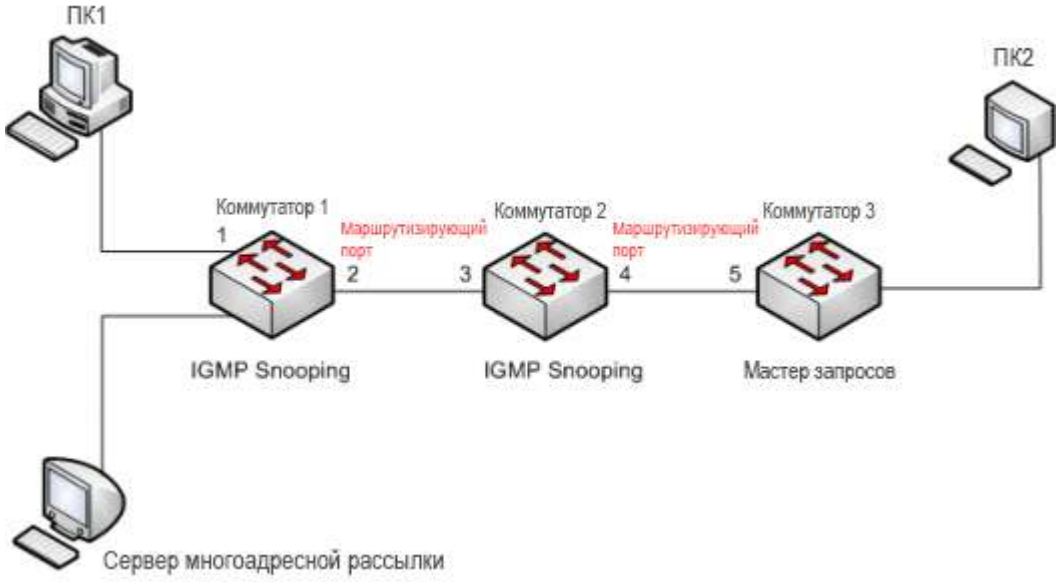


Рисунок 198 – Пример настройки IGMP Snooping

Поскольку коммутатор 3 выбран в качестве мастера запросов, он периодически отправляет сообщение общего запроса.

Порт 4 коммутатора 2 принимает пакеты и поэтому выбирается в качестве порта маршрутизации. Коммутатор 2 пересылает пакеты через порт 3. Затем порт 2 коммутатора 1 принимает пакеты и, таким образом, выбирается в качестве порта маршрутизации.

Когда ПК 1 добавляется в группу многоадресной рассылки 225.1.1.1 и отправляет пакеты отчетов IGMP, порт 1 и порт 2 (порт маршрутизации) коммутатора 1 добавляются в группу многоадресной рассылки 225.1.1.1. Пакеты отчетов IGMP пересылаются на коммутатор 2 через порт 2. Затем порт 3 и порт 4 коммутатора 2 также добавляются в многоадресную группу 225.1.1.1. Коммутатор 2 пересылает пакеты отчетов на коммутатор 3 через порт 4. В результате порт 5 коммутатора 3 также добавляется в многоадресную группу 225.1.1.1.

Когда данные сервера многоадресной рассылки достигают коммутатора 1, они будут перенаправлены на ПК1 через порт 1. Поскольку маршрутизирующий порт 2 также является членом группы многоадресной рассылки, данные будут пересылаться через него. Таким образом, когда данные достигают порта 5 коммутатора 3, он прекратит

пересылку, потому что получателя больше нет. Но если ПК2 также присоединится к группе 255.1.1.1, многоадресные данные будут перенаправлены на ПК2.

7.11 DHCP

В связи с постоянным увеличением масштаба сети и ростом ее сложности, в условиях частого перемещения компьютеров (таких как ноутбуки или устройства с беспроводным подключением), а также ввиду того, что число компьютеров значительно превышает выделяемые для них IP-адреса, протокол BootP, предназначенный для статической конфигурации хоста, все чаще становится неспособным удовлетворить существующие потребности. Для быстрого доступа в сеть, выхода из сети и улучшения коэффициента использования ресурсов IP-адресов было необходимо разработать автоматический механизм распределения IP-адресов на основе протокола BootP, в результате чего был представлен протокол динамической конфигурации хоста DHCP.

Данный протокол работает согласно модели «клиент-сервер». На этапе конфигурации клиент обращается к серверу, который в ответ сообщает необходимые параметры настроек, такие как IP-адрес, используя динамическую конфигурацию IP-адресов. На рисунке 199 показана типичная структура применения DHCP-протокола.

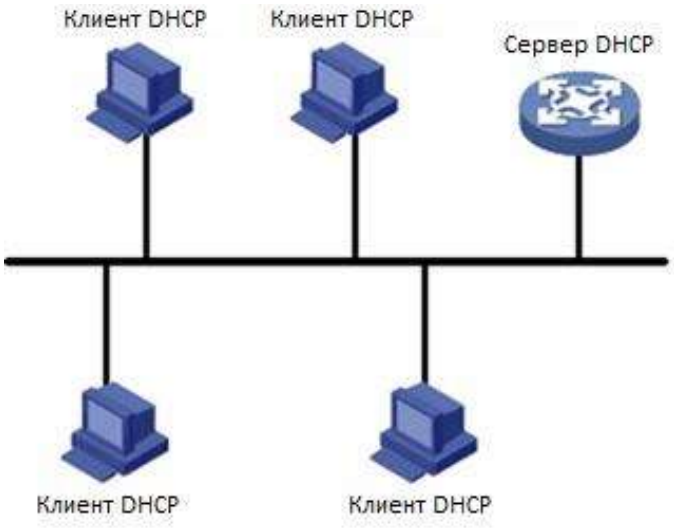


Рисунок 199 – Типовая схема DHCP

В процессе динамического распределения IP-адресов происходит отправка широковещательного сообщения, поэтому необходимо, чтобы DHCP-клиент и DHCP-сервер находились в одном сегменте. Если они находятся в разных сегментах, чтобы получить IP-адрес и другие параметры конфигурации, клиент может связаться с сервером через ретранслятор DHCP-протокола.

Протокол DHCP поддерживает два механизма распределения IP-адресов.

- Статическое распределение: сетевой администратор статично привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как, например, WWW-сервер, и отсылает привязанные IP-адреса клиентам через протокол DHCP.
- Динамическое распределение: DHCP-сервер производит динамическую выдачу IP-адреса клиенту. Этот механизм распределения может назначить для клиента постоянный IP-адрес или адрес с ограниченным сроком пользования. Когда время аренды адреса истекает, клиент должен повторно запросить IP-адрес. Сетевой администратор может выбирать для каждого клиента свой механизм распределения по протоколу DHCP.

7.11.1 Настройка сервера DHCP

7.11.1.1 Введение

DHCP-сервер – это поставщик услуг DHCP-протокола. Он использует DHCP-сообщения для связи с клиентом, чтобы назначить ему подходящий IP-адрес и при необходимости сообщить другие сетевые параметры. DHCP-сервер обычно используется для выделения IP-адресов в следующих случаях:

- большой масштаб сети. При ручном распределении рабочая нагрузка возрастает и управлять всей сетью становится трудно;
- количество хостов превышает число распределяемых IP-адресов, отчего становится невозможно назначить фиксированный IP-адрес каждому хосту;
- только несколько хостов в сети нуждаются в фиксированных IP-адресах.

7.11.1.2 Пул адресов DHCP

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

- IP-адрес, статически привязанный к MAC-адресу клиента;
- IP-адрес, записанный на DHCP-сервере, который когда-либо был выделен клиенту;
- IP-адрес, указанный в сообщении запроса клиента;
- Первый свободный IP-адрес, найденный в пуле адресов;
- Если доступный IP-адрес отсутствует, проверяется IP-адрес, срок аренды которого истекает и тот, у которого был конфликт. Если такой IP-адрес найден, он выделяется клиенту, если нет – подключения не происходит.

7.11.1.3 Настройка с помощью WEB-интерфейса

1. Включите DHCP-сервер, как показано ниже.

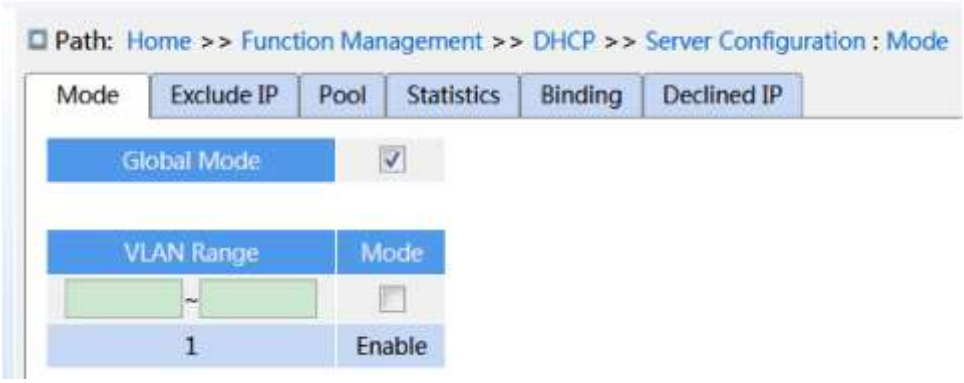


Рисунок 200 – Включение DHCP-сервера

Global Mode

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: выбор текущего коммутатора в качестве DHCP-сервера, для назначения IP-адресов клиентам.

{VLAN Range, Mode}

Диапазон: {1–4093, Enable/Disable}

Функция: если VLAN клиента, который подает заявку на IP-адрес, настроена на «Enable», DHCP-сервер выделяет IP-адрес клиенту. В противном случае адрес не выделяется.

2. Создайте пул адресов DHCP, как показано ниже.

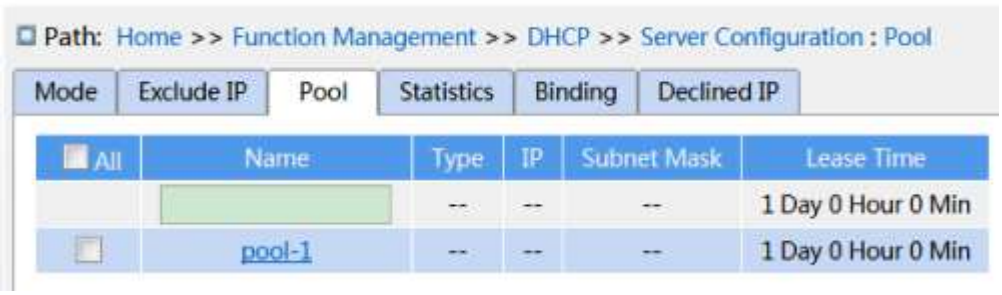


Рисунок 201 – Создание адресного пула

Name

Диапазон: 1–32 символа

Описание: имя пула IP-адресов.

Нажмите <Apply>, чтобы создать новый пул адресов DHCP.

3. Нажмите имя созданного пула адресов и настройте его, как показано ниже.

Рисунок 202 – Настройка адресного пула

Type

Варианты настройки: None/Network/Host

По умолчанию: None

Функция: указывает тип пула адресов.

Network: коммутатор динамически выделяет IP-адреса нескольким клиентам DHCP.

Host: коммутатор поддерживает статическое выделение IP-адресов специальным клиентам DHCP.

{IP, Subnet Mask}

Функция: в режиме «Network» вы можете настроить диапазон IP-адресов, который определяется маской подсети. Маска подсети – это 32-битное число, состоящее из последовательности единиц и нулей. «1» обозначает поля сетевого номера и номера подсети, а «0» – поля номера хоста. Обычно маска подсети устанавливается на 255.255.255.0.

В режиме «Host» вы можете статически задать IP-адрес для клиента. Статическое выделение IP-адресов осуществляется путем связывания MAC-адреса и IP-адреса клиента. Когда клиент с данным MAC-адресом запрашивает IP-адрес, DHCP-сервер находит соответствующий IP-адрес и выделяет его клиенту. Этот метод выделения имеет более высокий приоритет, чем динамическое выделение, и срок аренды является постоянным.

Lease Time

Диапазон: 0 дней 0 часов 0 минут – 365 дней 23 часа 59 минут

По умолчанию: 1 день 0 часов 0 минут

Описание: настройка времени аренды динамически назначаемых IP-адресов. Для разных адресных пулов DHCP-сервер может устанавливать разное время аренды, но адреса в одном пуле имеют одинаковое время аренды.

Domain Name

Диапазон: 1–36 символов

Функция: настройка доменного имени пула IP-адресов. При выделении IP-адреса клиенту отправляется также суффикс доменного имени.

Broadcast Address

Формат: A.B.C.D

Функция: настройка широковещательного адреса, выделяемого DHCP-сервером клиенту.

Default Router

Формат: A.B.C.D

Функция: настройка адреса шлюза, выделяемого DHCP-сервером клиенту.

Пояснение: когда DHCP-клиент посещает хост, который находится в другом сегменте, данные должны быть пересланы через шлюзы. Выделяя IP-адреса клиентам, DHCP-сервер может одновременно указывать адреса шлюзов. Для одного адресного пула можно настроить до 4 шлюзов.

DNS Server

Формат: A.B.C.D

Функция: настройка адреса DNS-сервера, выделяемого DHCP-сервером клиенту.

Пояснение: когда для посещения сетевого узла используется доменное имя, оно должно быть преобразовано в IP-адрес, что реализуется при помощи DNS (системы доменных имен). Чтобы позволить DHCP-клиенту посещать сетевой узел через доменное имя, DHCP-сервер может одновременно с выделением IP-адреса указывать клиенту IP-адреса серверов доменных имен. Для одного адресного пула можно настроить до 4 DNS-серверов.

NTP Server

Формат: A.B.C.D

Функция: настройка адреса NTP-сервера, выделяемого DHCP-сервером клиенту.

NetBIOS Node Type

Варианты настройки: None/B-node/P-node/M-node/H-node

По умолчанию: None

Функция: настройка типа узла NetBIOS для клиентов, выделяемого DHCP-сервером. При использовании протокола NetBIOS для связи в сети необходимо установить соответствие между именем хоста и IP-адресом. Разные типы узлов получают это соответствие различными способами.

Описание: B-узел получает соответствие в режиме широковещательной рассылки.

P-узел получает соответствие, отправляя одноадресный пакет для связи с WINS-сервером.

M-узел сначала отправляет широковещательный пакет для получения соответствия. Если это не удается, отправляет одноадресный пакет для связи с WINS-сервером.

H-узел сначала отправляет одноадресный пакет для связи с WINS-сервером. Если это не удается, отправляет широковещательный пакет для получения информации.

NetBIOS Scope

Диапазон: 1–36 символов

Функция: настройка имени NetBIOS.

NetBIOS Name Server

Формат: A.B.C.D

Функция: настройка адреса сервера WINS, выделяемого DHCP-сервером клиенту.

Пояснение: для клиента, работающего под управлением операционной системы Microsoft Windows (ОС), сервер службы имен Интернета Windows (WINS) предоставляет услугу разрешения имени хоста в IP-адрес в случае если хост использует для связи протокол NetBIOS. Поэтому большинству клиентов на базе ОС Windows требуется настройка WINS. Чтобы клиент DHCP мог разрешать имя хоста в IP-адрес, DHCP-сервер одновременно с выделением IP-адреса указывает клиенту IP-адреса серверов WINS. Для одного адресного пула можно настроить до 4 серверов WINS.

NIS Domain Name

Диапазон: 1–36 символов

Функция: настройка имени домена NIS, выделяемого DHCP-сервером клиенту.

NIS Server

Формат: A.B.C.D

Функция: настройка адреса сервера NIS, выделяемого DHCP-сервером клиенту.

Client Identifier

Варианты настройки: None/FQDN/MAC

По умолчанию: None

Функция: если тип пула – «Host», укажите уникальный идентификатор клиента.

FQDN – полное доменное имя;

MAC – MAC-адрес.

Hardware Address

Формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число)

Функция: если тип пула – «Host», укажите статически привязанный MAC-адрес клиента.

Client Name

Диапазон: 1–32 символа

Функция: настройка имени пользователя клиента.

Vendor Class Identifier

Диапазон: 1–64 символа

Функция: настройка идентификатора класса поставщика, выделяемого DHCP-сервером клиенту.

Vendor Specific Information

Диапазон: 1~64 шестнадцатеричных числа

Функция: настройка информации, специфичной для поставщика, выделяемой DHCP-сервером клиенту.

4. Настройте исключенные IP-адреса (IP-адреса в пуле, которые не выделяются динамически DHCP-сервером), как показано ниже.

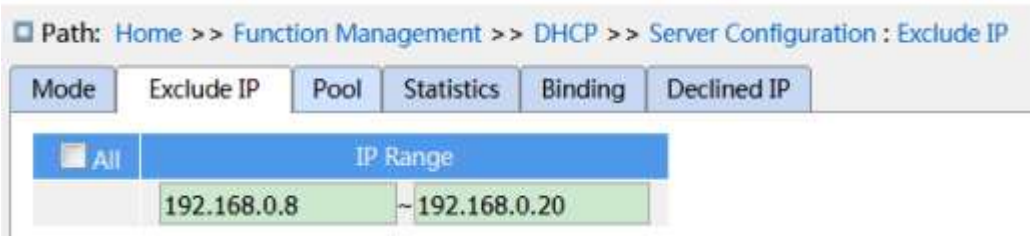


Рисунок 203 – Исключенные IP-адреса

IP Range

Функция: настройка диапазона IP-адресов, которые не выделяются динамически из адресного пула DHCP.

Пояснение: при выделении IP-адресов DHCP-сервер должен исключить занятые IP-адреса (например, IP-адреса шлюза и DNS-сервера). В противном случае один и тот же адрес может быть выделен двум клиентам, что приведет к конфликту в сети.

5. Просмотрите статистическую информацию DHCP-сервера, как показано ниже.

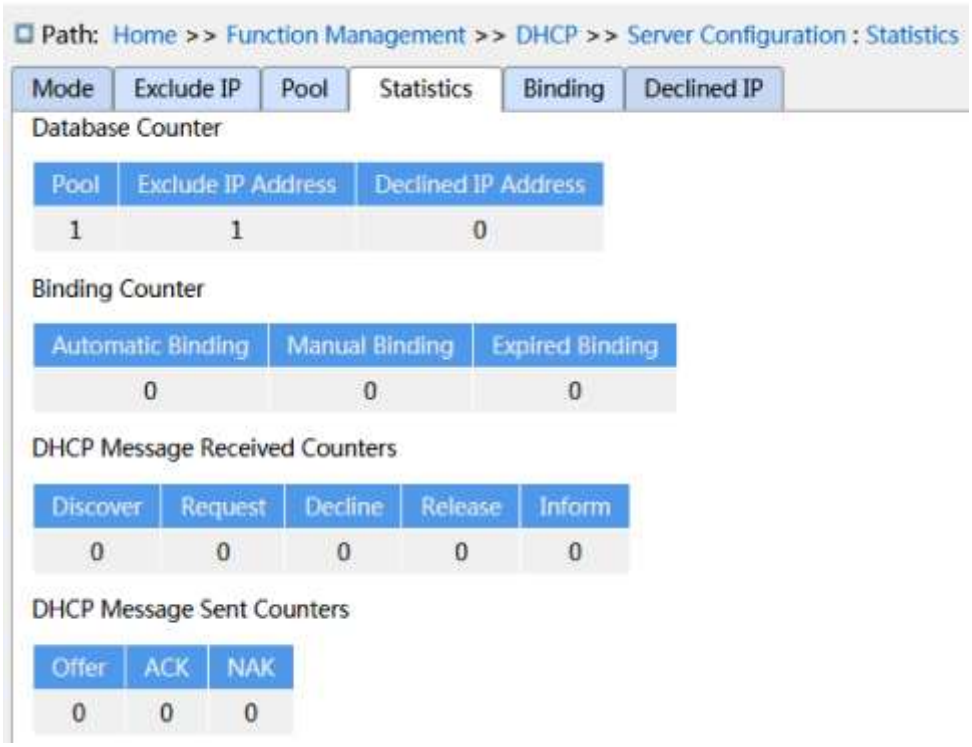


Рисунок 204 – Статистика DHCP-сервера

6. Просмотрите информацию об IP-адресах, выделенных DHCP-сервером, как показано ниже.

Рисунок 205 – Список выделенных адресов

7. Просмотрите IP-адреса, отклоненные DHCP-клиентами, как показано ниже.

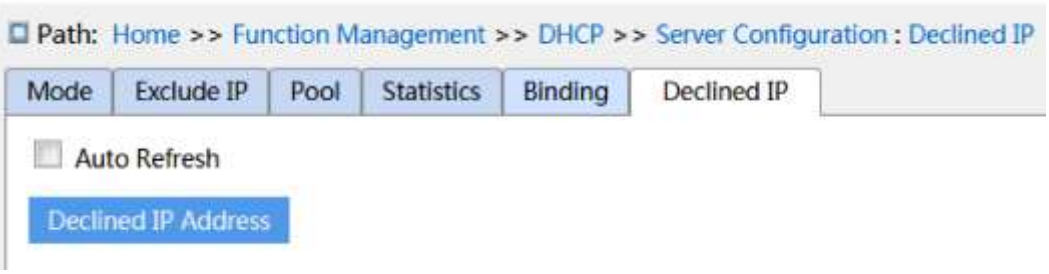


Рисунок 206 – Адреса, отклоненные клиентами

Когда клиент обнаруживает, что выделенный сервером IP-адрес конфликтует со статическим IP-адресом в том же сегменте сети, он отправляет серверу сообщение об отклонении этого адреса. Сервер записывает IP-адрес, отклоненный клиентом, и не будет выделять его другим клиентам в течение определенного периода времени.

7.11.1.4 Пример типовой настройки

Как показано на рисунке 207, коммутатор A работает как DHCP-сервер, а коммутатор B – как DHCP-клиент. Порт 3 коммутатора A соединяется с портом 4 коммутатора B. Клиент отправляет запросы на выделение ему IP-адреса. Сервер может назначить IP-адрес клиенту двумя способами. В текущей конфигурации настроен диапазон исключенных IP-адресов 192.168.0.1 – 192.168.0.10.

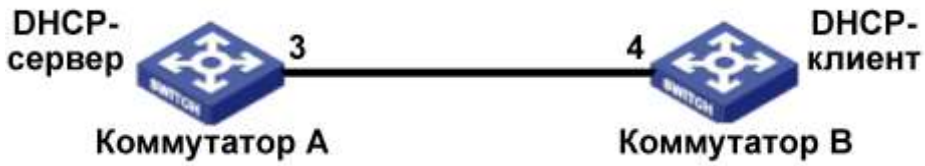


Рисунок 207 – Пример типовой настройки DHCP

Статическое выделение IP-адреса

➢ Настройка коммутатора A:

1. Включите статус DHCP-сервера в соответствующих VLAN, как показано на рисунке 200.

2. Создайте пул DHCP IP «pool-1», как показано на рисунке 201.

3. Установите тип пула «Host»; IP-адрес 192.168.0.6; маску 255.255.255.0; привяжите MAC-адрес коммутатора B: 00-11-22-33-44-55, как показано на рисунке 202.

➢ Настройка коммутатора B:

1. Укажите, чтобы коммутатор B автоматически получал IP-адрес через DHCP.

2. Коммутатор B получает IP-адрес 192.168.0.6 и маску подсети 255.255.255.0 от DHCP-сервера, как показано на рисунке 208.

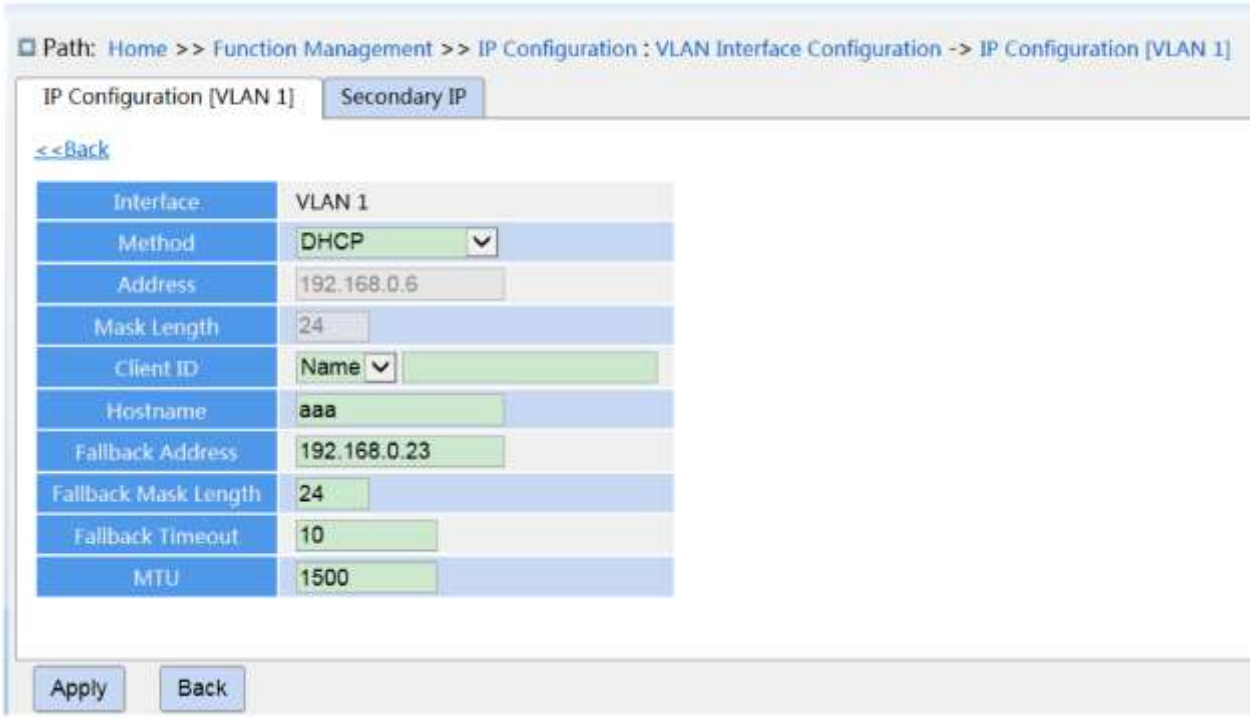


Рисунок 208 – Получение клиентом статического адреса

Динамическое выделение IP-адреса

- Настройка коммутатора A:

1. Включите статус DHCP-сервера в соответствующих VLAN, как показано на рисунке 200.

2. Создайте пул DHCP IP «pool-1», как показано на рисунке 201.

3. Укажите тип пула «Network»; IP-адрес 192.168.0.6; маску 255.255.255.0, остальные настройки оставьте по умолчанию.

4. Настройте диапазон исключенных IP-адресов 192.168.0.1 – 192.168.0.10, как показано на рисунке 203.

- Настройка коммутатора B:

1. Укажите, чтобы коммутатор B автоматически получал IP-адрес через DHCP.

2. DHCP-сервер ищет свободные IP-адреса в пуле адресов по порядку и выделяет первый найденный IP-адрес и другие сетевые параметры коммутатору B. Маска подсети – 255.255.255.0, как показано на рисунке 209.

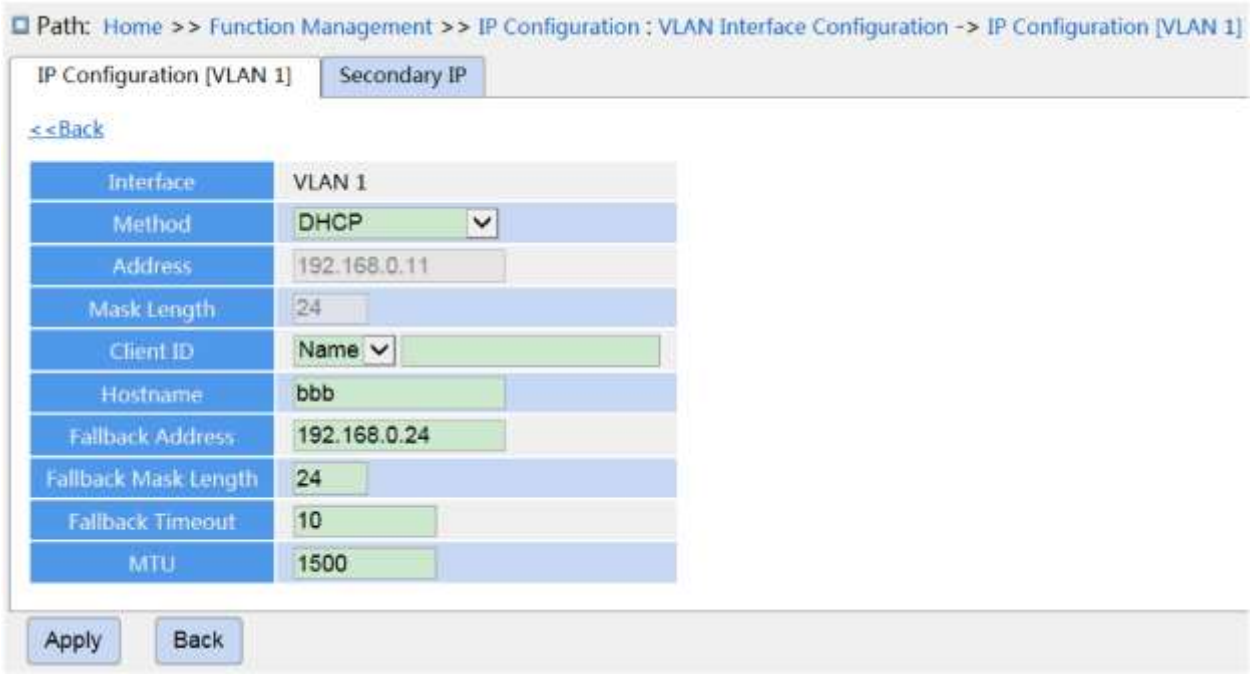


Рисунок 209 – Получение клиентом динамического адреса

7.11.2 DHCP Snooping

7.11.2.1 Введение

DHCP Snooping – это функция мониторинга служб DHCP на втором уровне, являющаяся одной из функций безопасности DHCP, которая дополнительно обеспечивает безопасность клиента. Механизм безопасности DHCP Snooping позволяет контролировать, чтобы только доверенные порты могли пересылать запросы клиента DHCP к легальному серверу. Также он контролирует источник ответных сообщений сервера DHCP, гарантируя, что клиент получит IP-адрес от действительного сервера и предотвращая выдачу IP-адресов или других параметров конфигурации поддельными или недействительными серверами DHCP.

Механизм безопасности DHCP Snooping разделяет порты на доверенные и недоверенные.

Доверенный порт – это порт, который прямо или косвенно соединяется с легальным DHCP-сервером. Доверенный порт обычно пересылает сообщения запросов клиентов и ответные сообщения серверов, чтобы гарантировать получение клиентами действительных IP-адресов.

Недоверенный порт не подключен к действительному DHCP-серверу. Недоверенные порты блокируются от отправки или получения данных DHCP, чтобы предотвратить возможные атаки или несанкционированное распределение IP-адресов.

7.11.2.2 Настройка с помощью WEB-интерфейса

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

Рисунок 210 – Включение DHCP Snooping

DHCP Snooping Mode

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение DHCP Snooping на коммутаторе.

Коммутатор, работающий как DHCP-сервер или клиент, не может активировать функцию DHCP Snooping.

---

2. Настройте доверенные порты, как показано ниже.

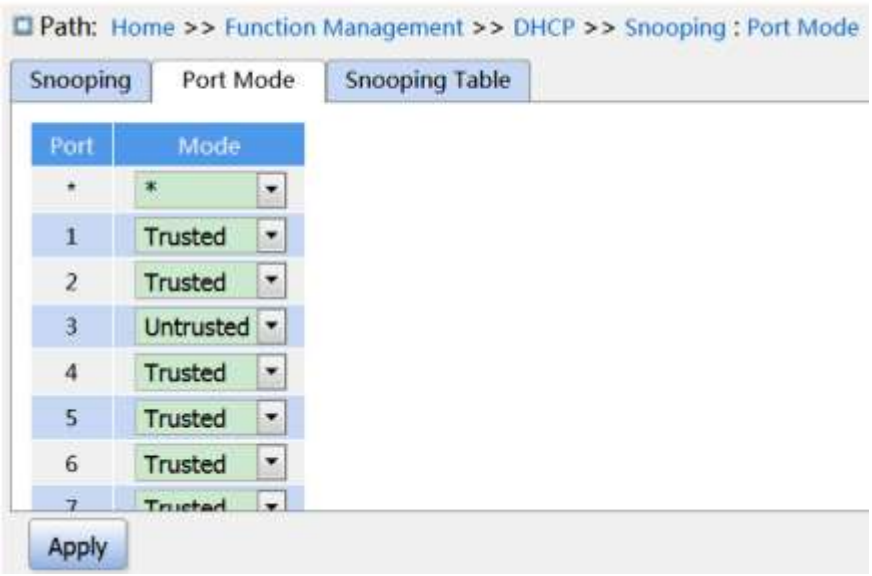


Рисунок 211 – Настройка доверенных портов

Mode

Варианты настройки: Trusted/Untrusted

По умолчанию: Untrusted

Функция: установить доверенный или недоверенный режим для портов. Порты, которые напрямую или косвенно подключаются к допустимым серверам DHCP, настраиваются как доверенные.

3. Просмотрите записи DHCP Snooping, как показано ниже.

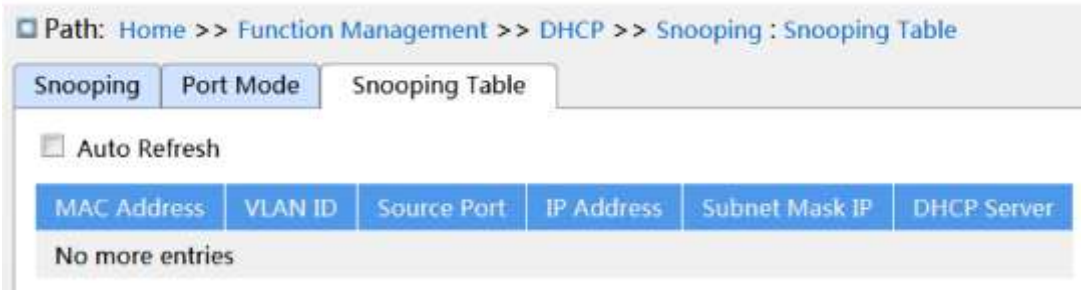


Рисунок 212 – Записи DHCP Snooping

7.11.2.3 Пример типовой настройки

Как показано на рисунке 213, DHCP-клиент запрашивает IP-адрес у DHCP-сервера. В сети существует неавторизованный DHCP-сервер. Установите для порта 1 доверенный режим с помощью DHCP Snooping, чтобы сервер и клиент могли свободно обмениваться DHCP-сообщениями. Порт 3 настройте как недоверенный, чтобы запретить ему пересылать DHCP-сообщения между сервером и клиентом. Таким образом гарантируется, что клиент сможет получить действительный IP-адрес от действительного DHCP-сервера.

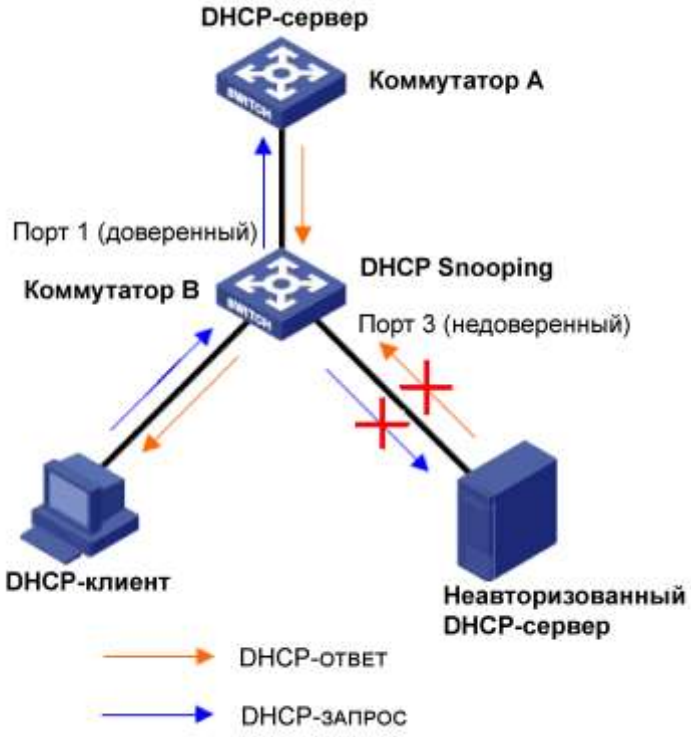


Рисунок 213 – Типовая конфигурация DHCP Snooping

➢ Настройка коммутатора B:

1. Включите функцию DHCP Snooping, как показано на рисунке 210.

2. Настройте порт 1 коммутатора B в качестве доверенного, а порт 3 – в качестве недоверенного, как показано на рисунке 211.

7.11.3 DHCP Relay

7.11.3.1 Введение

1. DHCP Relay

DHCP Relay – это механизм перенаправления DHCP-пакетов между DHCP-сервером и клиентом. Когда DHCP-клиент находится не в той же подсети, что и сервер, необходим ретранслятор для пересылки запросов и ответов DHCP.

Пересылка данных через DHCP Relay отличается от обычной маршрутизации. Обычная маршрутизация относительно прозрачна, и устройство, как правило, не изменяет содержимое IP-пакета. В случае же использования ретранслятора, после получения DHCP-сообщения агент DHCP Relay регенерирует это сообщение и отправляет его дальше.

С точки зрения DHCP-клиента, агент DHCP Relay воспринимается как DHCP-сервер; с точки зрения DHCP-сервера, агент DHCP Relay воспринимается как DHCP-клиент.

DHCP Relay пересылает полученный пакет запроса DHCP на DHCP-сервер в режиме одноадресной передачи и передает полученный пакет ответа DHCP обратно DHCP-клиенту. Ретранслятор выступает в роли промежуточной станции и отвечает за связь между DHCP-клиентами и DHCP-серверами, расположенными в разных сетевых сегментах. Это позволяет реализовать динамическое управление IP-адресами для нескольких сетевых сегментов при наличии установленного DHCP-сервера, то есть управление динамическими IP-адресами в режиме «клиент – ретранслятор – сервер».

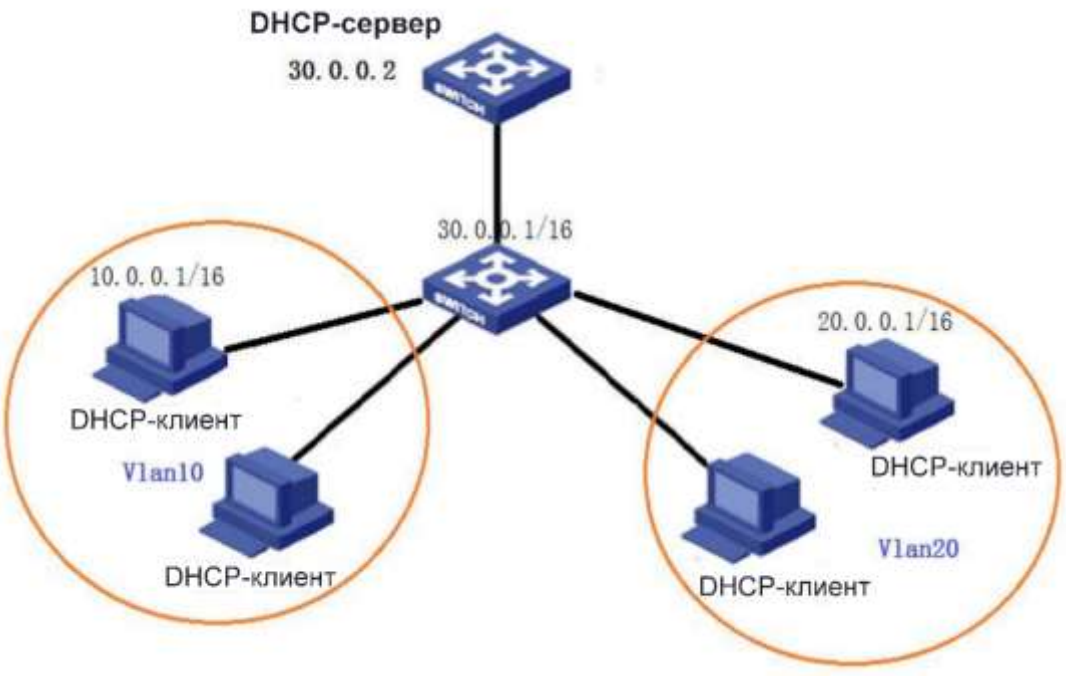


Рисунок 214 – Режим «клиент – ретранслятор – сервер»

2. Информация агента DHCP Relay (опция 82)

Когда устройство выполняет функцию DHCP-ретранслятора, вы можете добавить некоторые опции, чтобы указать сетевую информацию о DHCP-клиенте. Это позволяет серверу назначать разные IP-адреса пользователям на основе более точных данных. Согласно RFC 3046, номер опции для данной настройки – 82, поэтому ее также называют опцией 82 (Option 82).

Опция 82 (Relay Agent Information Entry) записывает информацию о клиенте. Когда поддерживающее опцию 82 DHCP Snooping получает сообщение запроса от DHCP-клиента, оно добавляет соответствующее поле опции 82 в сообщения и затем пересылает их на DHCP-сервер. Сервер, поддерживающий опцию 82, может гибко назначать адреса в зависимости от информации, содержащейся в сообщении опции 82.

После включения опции 82 соответствующее поле будет добавлено в сообщение. Поле Option 82 в данном типе коммутаторов содержит две суб-опции: суб-опция 1 (Circuit ID) и суб-опция 2 (Remote ID).

- Суб-опция 1 содержит информацию о VLAN ID и номере порта, который принимает сообщение запроса от DHCP-клиента, как показано в таблице 7.

Таблица 7 – Формат поля Sub-option 1

Тип суб-опции (0x01)	Длина (0x04)	VLAN ID	Номер портаr
1 байт	1 байт	2 байта	2 байта

Тип суб-опции равен 1.

На устройстве DHCP Relay длина указывает на количество байтов, которые занимают идентификатор VLAN и номер порта.

На устройстве DHCP Relay VLAN ID обозначает идентификатор VLAN порта, который получает сообщение запроса от клиента DHCP.

На устройстве DHCP Relay номер порта указывает на порт, который получает сообщение запроса от DHCP-клиента.

- Содержимым суб-опции 2 является MAC-адрес устройства DHCP Relay, которое получает сообщение запроса от клиента DHCP, как показано в таблице 8, или строка символов, настроенная пользователями, как показано в таблице 9.

Таблица 8 – Sub-option 2, формат поля MAC-адреса

Тип суб-опции (0x02)	Длина (0x06)	MAC-адрес
1 байт	1 байт	6 байт

Таблица 9 – Sub-option 2, формат поля символьной строки

Тип суб-опции (0x02)	Длина (0x10)	Строка символов
Один байт	Один байт	16 байт

Тип суб-опции равен 2.

Длина указывает на количество байтов, которые занимает содержимое суб-опции 2. MAC-адрес занимает 6 байт, а строка символов – 16 байт.

MAC-адрес относится к устройству DHCP Relay, которое получает сообщение запроса от DHCP-клиента.

Строка символов: содержимое суб-опции 2 составляет 1–16 символов, заданных пользователем. Символы вводятся в кодировке ASCII, и каждый символ занимает один байт. Длина фиксирована и равна 16. Если настроена строка длиной менее 16 байт, позиции недостающих символов заполняются нулями.

Если ретранслятор поддерживает опцию 82, то, получив DHCP-сообщение запроса, оно обрабатывает его в зависимости от того, содержит ли сообщение Option 82 и политику клиента, а затем пересылает обработанное сообщение на DHCP-сервер. Конкретный метод обработки показан в таблице 10.

Таблица 10 – Режимы обработки сообщений запроса ретранслятором

Получение сообщения запроса от DHCP-клиента	**Политика конфигурации**	**Обработка сообщения запроса устройством DHCP Snooping**
Сообщение содержит Option 82	Drop	Удаляет сообщение запроса
	Keep	Сохраняет формат сообщения неизменным и пересылает его
	Replace	Заменяет поле Option 82 в сообщении на свое поле Option 82 и пересылает новое сообщение
Сообщение не содержит Option 82	Drop/Keep/Replace	Добавляет свое поле Option 82 в сообщение и пересылает его

Если ретранслятор получает ответное сообщение от DHCP-сервера, и оно содержит поле Option 82, данное поле удаляется, а сообщение пересылается клиенту.

7.11.3.2 Настройка с помощью WEB-интерфейса

Глобальная настройка DHCP Relay показана ниже.

Рисунок 215 – Глобальная настройка DHCP Relay

Mode

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение ли DHCP Relay.

Server Address

Функция: настройка адреса DHCP-сервера.

Option82 State

Варианты настройки: Enable/Forbid

По умолчанию: Forbid

Функция: указывает, следует ли добавлять поле Option 82.

Client Policy

Варианты настройки: Replace/Keep/Drop

По умолчанию: Keep

Функция: настройка политики, в соответствии с которой DHCP Relay обрабатывает отправленный клиентом запрос. См. таблицу 10.

2. Просмотрите элементы таблицы безопасности DHCP, как показано ниже.

Рисунок 216 – Таблица безопасности DHCP

7.11.3.3 Пример типовой настройки

Как показано на рисунке 217, коммутатор A выступает как DHCP-сервер, коммутатор B как DHCP-ретранслятор, коммутатор C как DHCP-клиент. Порт 1 коммутатора A подключен к порту 1 коммутатора B, порт 2 коммутатора B подключен к порту 2 коммутатора C. DHCP-сервер не находится в той же локальной сети, что и DHCP-клиент. Клиент динамически получает IP-адрес и другие сетевые параметры при помощи DHCP через ретранслятор.

Рисунок 217 – Топология DHCP-устройств

Настройка коммутатора A:

1. Создайте VLAN1 и настройте IP-интерфейс 100.1.1.156, как показано на рисунке 123.
2. Включите сервер DHCP на VLAN 1, как показано на рисунке 200.
3. Создайте пул адресов «pool-33», как показано на рисунке 201.
4. Укажите для пула адресов тип Network, IP-адрес 33.1.1.6 и маску 255.0.0.0.

Настройка коммутатора B:

1. Создайте VLAN1 и настройте IP-интерфейс 100.1.1.180, как показано на рисунке 123;
2. Создайте VLAN33 и настройте IP-интерфейс 33.1.1.2, как показано на рисунке 123;
3. Включите DHCP Relay, как показано на рисунке 215;
4. Укажите IP-адрес сервера 100.1.1.156, как показано на рисунке 215;

Настройка коммутатора C:

1. Создайте VLAN33 и включите DHCP-клиент.
2. Коммутатор A назначит IP-адрес 33.0.0.1 коммутатору C.

7.12 IEEE 802.1X

7.12.1 Введение

Для обеспечения безопасности WLAN комитет IEEE 802 LAN/WAN предложил протокол 802.1X. Этот протокол служит общим механизмом контроля доступа для портов LAN в Ethernet и реализует аутентификацию и безопасность в сети Ethernet.

802.1X представляет собой систему контроля доступа на основе портов. Это означает, что аутентификация и контроль доступа осуществляются на уровнях портов устройств, предоставляющих доступ к локальной сети (LAN). Если пользователь успешно проходит

аутентификацию, ему предоставляется доступ к ресурсам в LAN. В противном случае, если аутентификация не пройдена, доступ к ресурсам в LAN будет запрещен.

Системы 802.1X используют структуру «клиент-сервер», как показано ниже. Для аутентификации пользователей и авторизации доступа на основе портов необходимы следующие элементы:

Рисунок 218 – Структура 802.1X

Клиент обычно представляет собой пользовательский терминал. Когда пользователь хочет получить доступ к Интернету, он запускает клиентскую программу и вводит необходимые имя пользователя и пароль. Клиентская программа отправляет запрос на подключение. Клиент должен поддерживать протокол EAPOL.

Устройство обозначает коммутатор аутентификации в Ethernet-системе. Оно загружает и передает информацию об аутентификации пользователя, а также включает или отключает порт в зависимости от результата аутентификации.

Сервер аутентификации – это сущность, предоставляющая услуги аутентификации для устройств. Он проверяет, есть ли у пользователей разрешения на использование сетевых сервисов на основе идентификаторов (имя пользователя и пароль), отправленных клиентами, и включает или отключает порты в зависимости от результатов аутентификации.

7.12.2 Настройка с помощью WEB-интерфейса

1. Ниже показана конфигурация диспетчера задач 802.1X.

Рисунок 219 – Диспетчер задач 802.1X

Operation Type

Варианты настройки: Restart Authentication Process / Initialize

Функция: Когда для порта установлен режим аутентификации «Mac-Based» или «Port-Based» (см. рисунок 221), вы можете выбрать <Restart Authentication Process> или <Initialize> для повторной аутентификации. В процессе повторной аутентификации статус порта изменяется на «неаутентифицированный», что означает, что устройство на данный момент не имеет доступа к сети, пока не пройдет успешную аутентификацию.

Port

Варианты настройки: включено/выключено

Функция: выбор порта, на котором необходимо перезапустить процесс аутентификации или провести инициализацию.

2. Ниже показана базовая конфигурация 802.1X.

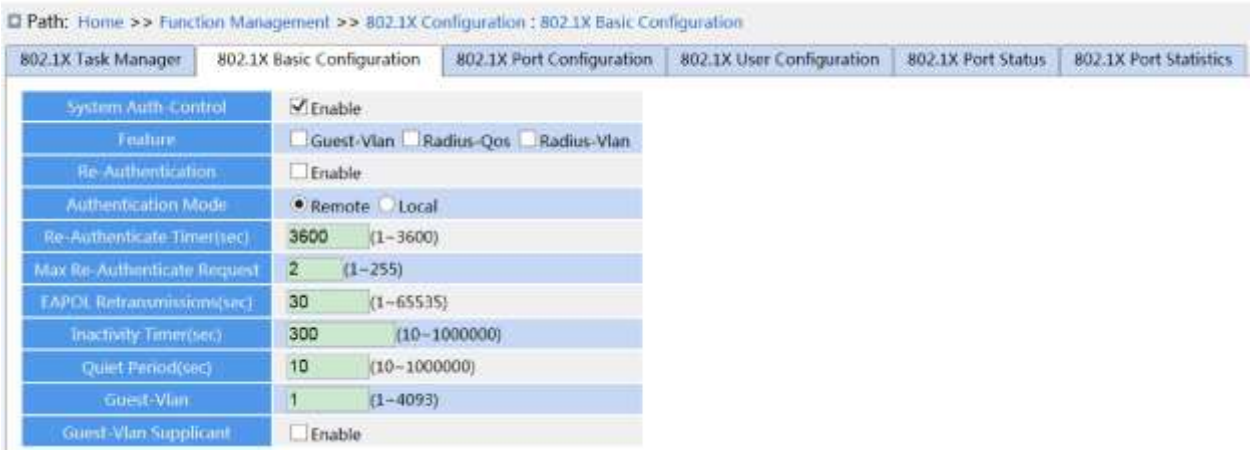


Рисунок 220 – Базовая конфигурация 802.1X

System Auth-Control

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение глобальной функции безопасности IEEE 802.1X.

Guest-Vlan

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: при включении этой опции, если пользователь не прошел аутентификацию или не смог пройти ее успешно, устройство автоматически добавляет порт аутентификации клиента в гостевую VLAN. Все пользователи, подключенные к этому порту, получают доступ к ресурсам, доступным в гостевой VLAN, что позволяет временно предоставить ограниченный доступ к сети для неаутентифицированных пользователей.

Radius-Qos

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: при включении этой опции, после успешной аутентификации клиента, сервер передает информацию об авторизации устройству. Если на сервере активирована функция RADIUS-QoS, информация об авторизации включает данные CoS, которые присваиваются в процессе авторизации. Устройство изменяет значение CoS порта аутентификации клиента в соответствии с этим значением, что позволяет управлять приоритетами трафика и обеспечивать качественное обслуживание (QoS) для аутентифицированных пользователей.

Radius-Vlan

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: при включении этой опции, после прохождения клиентом аутентификации сервер передает информацию об авторизации на устройство. Если на сервере активирована функция RADIUS-VLAN, информация об авторизации включает данные о VLAN, которые присваиваются в процессе авторизации. Оборудование добавит порт аутентификации клиента в назначенную VLAN.

Re-Authentication

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: указывает, требуется ли регулярная повторная аутентификация успешно аутентифицированных клиентов.

Authentication Mode

Варианты настройки: Remote/Local

По умолчанию: Remote

Функция: настройка режима удаленной или локальной аутентификации RADIUS.

Re-Authenticate Timer (sec)

Диапазон: 1–3600 с

По умолчанию: 3600 с

Функция: настройка временного интервала для повторной аутентификации. Таймер можно настроить только при включенной функции «Re-Authentication».

Max Re-Authenticate Request

Диапазон: 1–255

По умолчанию: 2

Функция: настройка максимального количества попыток повторной передачи пакетов EAPOL для запроса идентификации. Если устройство не получает ответные пакеты от клиента после достижения максимального количества попыток повторной передачи, оно считает процесс аутентификации неудачным.

EAPOL Retransmissions

Диапазон: 1–65535 с

По умолчанию: 30 с

Функция: настройка дополнительного времени для ответа от клиента. После отправки запроса идентификации устройство повторно передаст запрос, если по истечении указанного времени оно не получит ответа от клиента.

Inactivity Timer

Диапазон: 10–1000000 с

По умолчанию: 300 с

Функция: после аутентификации MAC-адреса, если аутентификация прошла успешно, но в течение установленного времени не было передано ни одного пакета, соответствующая запись безопасности удаляется.

Quiet Period (sec)

Диапазон: 10–1000000 с

По умолчанию: 10 с

Функция: если аутентификация клиента завершается неудачей, устройство переходит в период тишины. В течение этого времени оно не отвечает на запросы аутентификации от клиента.

Guest-Vlan

Диапазон: 1–4095

По умолчанию: 1

Функция: настройка идентификатора гостевой VLAN.

Guest-Vlan Supplicant

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: при включении, если пользователь не аутентифицирован или не смог пройти аутентификацию, устройство добавляет порт аутентификации клиента в гостевую VLAN. При отключении устройство добавляет порт в гостевую VLAN только в том случае, если на этом порту нет записей о кадрах EAPOL.

- Предварительным условием для настройки параметров «Guest-Vlan», «Max Re-Authenticate Request» и «Guest-Vlan Supplicant» является включение «Guest -Vlan» в поле «Feature».
- Рекомендуется отключить «Radius-Vlan» и «Guest-Vlan», если тип порта аутентификации Trunk или Hybrid.
- Значение CoS, назначенное для авторизации, не влияет на конфигурацию порта и не изменяет ее. Однако приоритет значения, назначенного для авторизации, выше значения, настроенного пользователем. Другими словами, после аутентификации действительным является значение CoS,

назначенное для авторизации. Если пользователь не прошел аутентификацию или отключается, вступает в силу значение CoS, настроенное пользователем.

- VLAN, назначенная для авторизации, или гостевая VLAN не влияет на конфигурацию порта и не изменяет ее. Однако VLAN, назначенная для авторизации, или гостевая VLAN имеет более высокий приоритет, чем VLAN, настроенная пользователем.
- После того, как пользователь инициирует аутентификацию, и она проходит успешно:

  если на порту включена функция «Radius-Vlan», порт добавляется в VLAN, назначенную сервером RADIUS;
  если на порту не включена функция «Radius-Vlan», порт добавляется в VLAN, настроенную пользователем.
- Если пользователь не прошел аутентификацию или отключается:

  если на порту включены функции «Guest-Vlan» и «Guest-Vlan Supplicant», порт добавляется в гостевую VLAN;
  если на порту включена функция «Guest-Vlan», но не включена «Guest-Vlan Supplicant», порт будет добавлен в гостевую VLAN только в том случае, если нет записей о кадрах EAPOL (т.е. если не было попыток аутентификации через EAPOL). Если записи о кадрах EAPOL доступны (т.е. если были попытки аутентификации, но они не увенчались успехом), порт будет добавлен в VLAN, настроенную пользователем;
  если на порту не включена функция «Guest-Vlan», он добавляется в VLAN, настроенную пользователем.

---

3. Настройте порты 802.1X, как показано ниже.

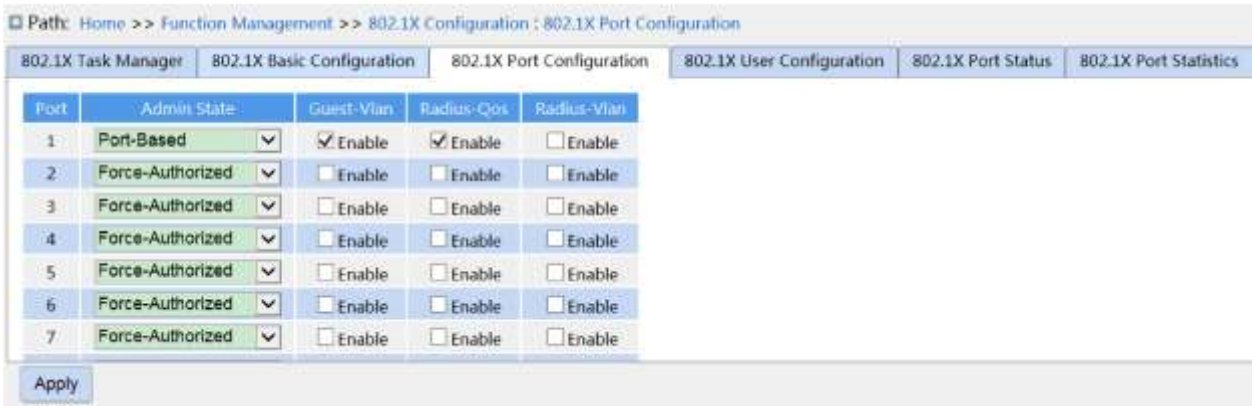


Рисунок 221 – Настройка портов 802.1X

Port

Варианты настройки: все порты коммутатора.

Admin State

Варианты настройки: Force Authorized/Force Unauthorized/Port-Based/MAC-Based

По умолчанию: Force Authorized

Функция: выбор режима аутентификации порта.

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

«Force Unauthorized» означает, что порт всегда находится в неавторизованном состоянии и не позволяет пользователям проводить аутентификацию, а коммутатор не предоставляет услуги аутентификации клиентам, которые получают доступ к коммутатору с этого порта.

«MAC-Based» указывает, что каждый пользователь, подключающийся к порту, должен проходить аутентификацию индивидуально. Если пользователь отключается (например, выходит из сети), только этот пользователь теряет доступ к сети, в то время как другие пользователи, подключенные к тому же порту, могут продолжать использовать сеть.

«Port-Based» указывает, что аутентификация осуществляется на уровне порта. После того как первый пользователь, использующий порт, успешно проходит аутентификацию, все последующие пользователи, подключающиеся к этому порту, могут использовать сеть без аутентификации. Однако, если первый пользователь отключается от сети, порт становится неактивным, и все остальные пользователи, подключенные к этому порту, теряют доступ к сети.

Guest-Vlan

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: при включении этой опции, если пользователь не прошел аутентификацию или не смог пройти ее успешно, устройство автоматически добавляет порт аутентификации клиента в гостевую VLAN. Все пользователи, подключенные к этому порту, получают доступ к ресурсам, доступным в гостевой VLAN, что позволяет временно предоставить ограниченный доступ к сети для неаутентифицированных пользователей.

Radius-Qos

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: позволяет включить или отключить применение параметров качества обслуживания (QoS), назначенных сервером RADIUS, на данном порту.

Radius-Vlan

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: позволяет включить или отключить применение VLAN, назначенной сервером RADIUS, на данном порту.

Данные функции доступны только если включены как на глобальном уровне, так и на уровне порта.

4. Ниже показана конфигурация пользователей 802.1X.

Рисунок 222 – Конфигурация пользователей 802.1X

User Name

Диапазон: 1–16 символов

По умолчанию: не задано

Функция: настройка имени пользователя для локальной аутентификации.

Password

Диапазон: 1–16 символов

По умолчанию: не задано

Функция: настройка пароля для локальной аутентификации.

5. Просмотрите состояние портов 802.1X, как показано ниже.

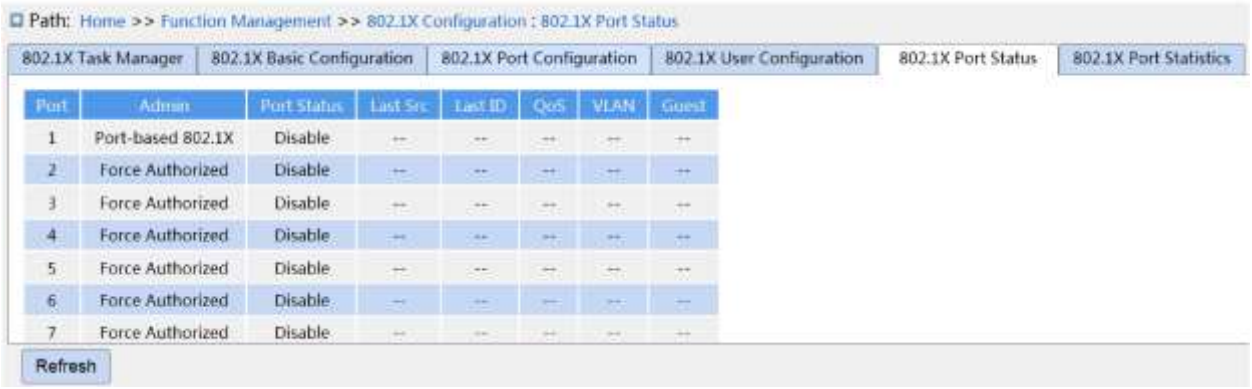


Рисунок 223 – Состояние портов 802.1X

Port Status

Варианты настройки: Disable, Auth, UnAuth, DOWN, x A/y UnA

Функция: отображение состояния аутентификации порта.

«Disable» означает, что 802.1X отключен глобально;

«Auth» означает, что пользователь, подключенный к порту, прошел аутентификацию;

«UnAuth» означает, что пользователь, подключенный к порту, не прошел аутентификацию;

«DOWN» означает, что порт отключен;

«x A/y UnA» означает, что x пользователей авторизованы, а y пользователей не авторизованы, когда порт находится в режиме аутентификации на основе MAC-адресов.

6. Просмотрите статистику 802.1X, как показано ниже.

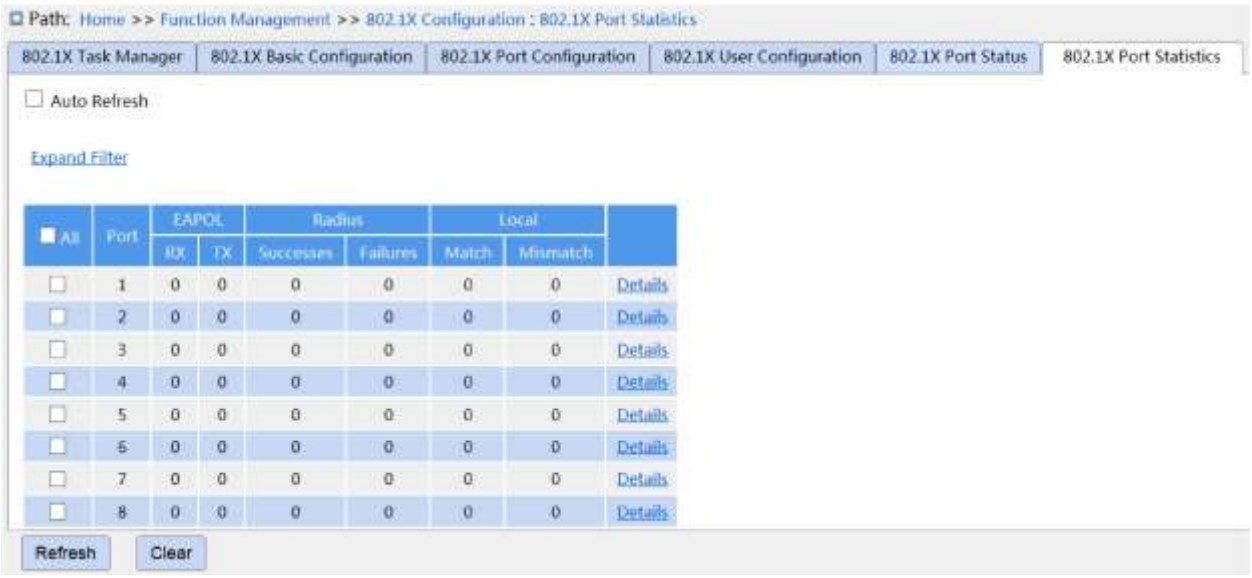


Рисунок 224 – Статистика 802.1X

Нажмите <Details>, чтобы открыть в интерфейс статистической информации 802.1X соответствующего порта, как показано ниже.

<<Back

Statistics		
Eapol	Rx Total	0
	Tx Total	0
	Rx RespId	0
	Tx ReqId	0
	Rx RespMD5	0
	Tx ReqMD5	0
	Rx Resp	0
	Tx Req	0
	Rx Start	0
	Rx LogOff	0
	Rx Invalid Type	0
	Rx Invalid Len	0
Radius	Rx Access Challenges	0
	Rx Other Requests	0
	Rx Auth Successes	0
	Rx Auth Failures	0
	Tx Responses	0
	Mac Address	--
Local	MD5-Challenge Match	0
	MD5-Challenge Mismatch	0
	Error User	0
	Error Decode	0
	Error InvalidNethod	0

Рисунок 225 – Статистика порта 802.1X

7.12.3 Пример типовой настройки

Как показано на рисунке 226, на порту 1 коммутатора включена работа протокола стандарта IEEE 802.1X. Соответственно, пользователи могут зайти на коммутатор через порт 1 после прохождения аутентификации на сервере RADIUS. IP-адрес сервера 192.168.0.23. Ключ для обмена пакетами между коммутатором и сервером – aaa.

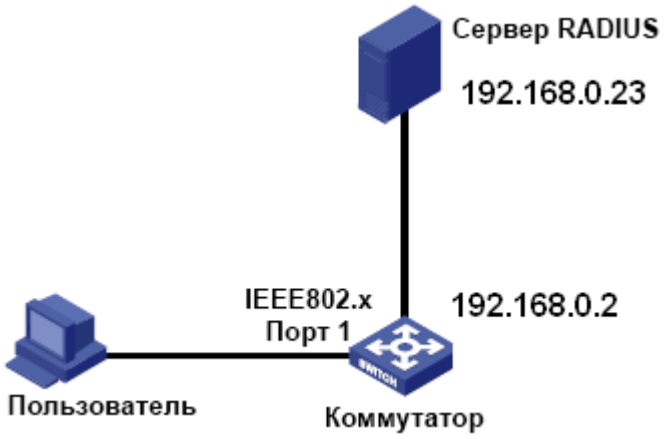


Рисунок 226 – Пример аутентификации IEEE 802.1X

1. Установите для IP-адреса сервера аутентификации значение 192.168.0.23 и пароль «aaa», как показано на рисунке 79.

2. Настройки IEEE 802.1X: включите IEEE 802.1X глобально, как показано на рисунке 220.

Выберите административное состояние порта 1 «Port-Based» (см. рисунок 221), оставьте настройки по умолчанию для других параметров.

3. Настройте имя пользователя и пароль на сервере RADIUS «ccc», ключ шифрования – «aaa».

4. Установите и запустите клиентское программное обеспечение 802.1X на ПК. Введите «ccc» в качестве имени пользователя и пароля. После этого пользователь может пройти аутентификацию и получить доступ к коммутатору через порт 1.

7.13 GMRP

7.13.1 Протокол GARP

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

Благодаря GARP, информация о настройках коммутатора может быть передана по всей локальной сети. Объекты GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путем отправки соответствующих Join и Leave-сообщений. GARP предусматривает три типа сообщений: Join, Leave и LeaveAll.

- Когда объект GARP хочет передать свои настройки другим коммутаторам, он отсылает Join-сообщение. Join-сообщения бывают двух типов: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для зарегистрированного атрибута, в то время как JoinEmpty – для атрибута, который еще не был зарегистрирован.
- Когда объект GARP хочет удалить свои настройки с других коммутаторов, он отправляет сообщение Leave. Leave-сообщения бывают двух типов: LeaveEmpty и LeaveIn.

Сообщение LeaveIn отправляется для зарегистрированного атрибута, в то время как LeaveEmpty – для атрибута, который еще не был зарегистрирован.

- После запуска объекта GARP, он начинает отсчитывать период LeaveAll. Когда период заканчивается, объект отсылает сообщение LeaveAll.

Объект GARP означает порт, на котором включен протокол GARP.

Для работы GARP использует таймеры Hold, Join, Leave и LeaveAll.

Таймер Hold. При получении сообщения о регистрации настроек, объект GARP не отправляет сообщение Join сразу, а запускает таймер Hold. Когда таймер заканчивает отсчет, объект отправляет все сообщения о настройках, полученные за этот период в одном Join-сообщении, что уменьшает количество передаваемых по сети данных.

Таймер Join. Для того, чтобы убедиться, что Join-сообщения получены другими объектами, после отправки сообщения Join объект GARP запускает таймер Join. Если за период до истечения установленного срока в ответ не получено JoinIn-сообщение, объект отправляет Join-сообщение снова. В противном случае, сообщение Join не отправляется.

Таймер Leave. Если объект GARP хочет удалить информацию об атрибуте, он отсылает Leave-сообщение. Объект, получивший это сообщение, запускает таймер Leave. Если он не получает ни одного Join-сообщения до истечения таймера, он удаляет информацию о данном атрибуте.

Таймер LeaveAll. При старте объекта GARP, запускается таймер LeaveAll. По его истечении, объект отправляет LeaveAll-сообщение для того, чтобы другие объекты GARP перерегистрировали все атрибуты. После этого объект запускает таймер LeaveAll заново.

7.13.2 Протокол GMRP

GMRP – протокол регистрации многоадресной рассылки, основанный на принципах GARP. Он используется для поддержки информации о многоадресных группах на коммутаторах. 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 информации гарантирует единообразие информации о многоадресной рассылке на всех GMRP-коммутаторах сети.

Если коммутатор или терминал хотят войти или выйти из многоадресной группы, GMRP-порт передает информацию об этом в широковещательном режиме на все порты своей VLAN.

7.13.3 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.

Динамически изученные многоадресные записи GMRP и записи агентов передаются портом распространения на аналогичные порты устройств нижнего уровня.

Все таймеры GMRP в одной сети должны быть согласованными, чтобы предотвратить взаимные помехи. Таймеры должны следовать следующим правилам:

Hold < Join, 2*Join < Leave, Leave < LeaveAll.

7.13.4 Настройка с помощью WEB-интерфейса

1. Включите протокол GMRP в глобальном режиме и настройте глобальный таймер, как показано ниже.

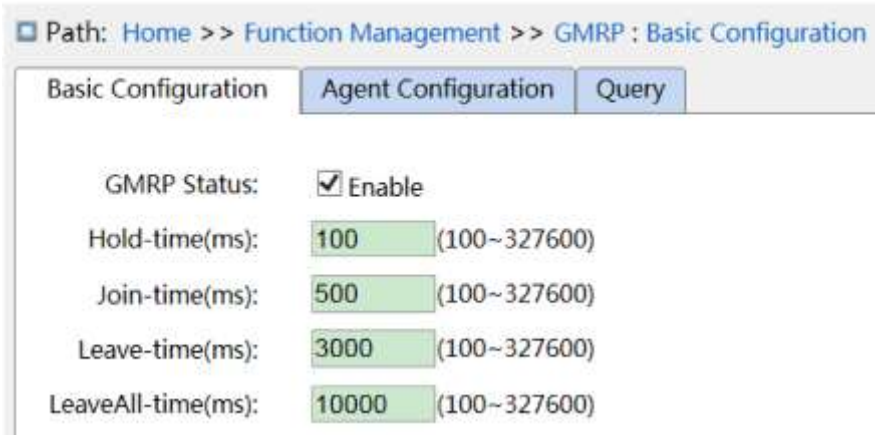


Рисунок 227 – Глобальна конфигурация GMRP

GMRP Status

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/выключение глобальной функции GMRP. Функция не может использоваться вместе с функцией IGMP Snooping.

Hold-timer

Диапазон: 100 – 327600 мс

По умолчанию: 100 мс

Описание: это значение должно быть кратно 100. Лучше установить одинаковое время таймеров Hold на всех портах с поддержкой GMRP

Join-timer

Диапазон: 100 – 327600 мс

По умолчанию: 500 мс

Описание: это значение должно быть кратно 100. Лучше установить одинаковое время таймеров Join на всех портах с поддержкой GMRP

Leave-timer

Диапазон: 100 – 327600 мс

По умолчанию: 3000 мс

Описание: это значение должно быть кратно 100. Лучше установить одинаковое время таймеров Leave на всех портах с поддержкой GMRP.

LeaveAll-timer

Диапазон: 100 – 327600 мс

По умолчанию: 10000 мс

Функция: интервал времени для отправки пакетов LeaveAll. Значение должно быть кратно 100.

Пояснение: если таймеры LeaveAll разных устройств истекают в одно и то же время, они отправят несколько сообщений LeaveAll одновременно, что увеличит нагрузку на сеть. Чтобы избежать истечения таймеров LeaveAll разных устройств в одно и то же время, фактическое время работы таймера LeaveAll представляет собой случайное значение, которое больше настроенного времени таймера, но не более, чем в 1,5 раза.

2. Настройте функцию GMPR на портах, как показано ниже.

Port	GMRP Enable	GMRP Agent Enable	Last PDU Origin
1	☑	☑	00-00-00-00-00-00
2	☑	☐	00-00-00-00-00-00
3	☐	☐	--
4	☐	☐	--
5	☐	☐	--
6	☐	☐	--

Рисунок 228 – Настройка GMRP на портах

GMRP Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение функции GMRP на порту.

GMRP Agent Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение функции агента GMRP на порту.

Last PDU Origin

Функция: исходный MAC-адрес пакета протокола, полученного на порту последним.

- Порт агента не может распространять запись агента.
- Для включения агента GMRP на порту необходимо вначале включить на этом порту функцию GMRP.

---

3. Добавьте запись агента GMRP, как показано ниже.

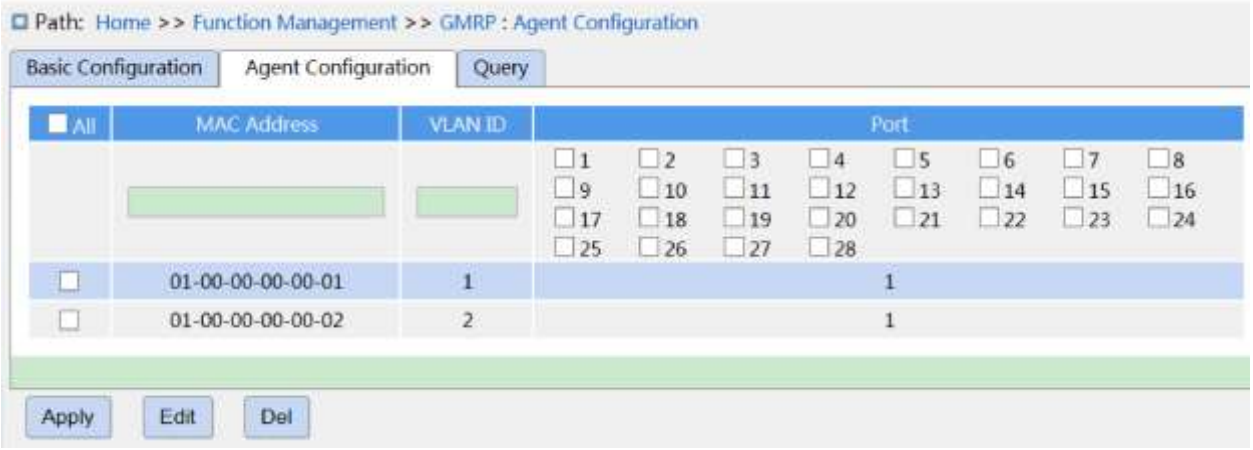


Рисунок 229 – Настройка записи агента GMRP

MAC Address

Формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число)

Функция: настройка MAC-адреса группы многоадресной рассылки. Самый младший бит первого байта равен 1.

VLAN ID

Варианты настройки: все созданные номера VLAN

Функция: настройка идентификатора VLAN для записи агента GMRP.

Описание: запись агента GMRP может быть перенаправлена только с порта распространения с VLAN ID, совпадающим с VLAN ID этой записи.

Port

Варианты настройки: все настроенные агентские порты

4. Просмотрите конфигурацию GMRP, как показано ниже.

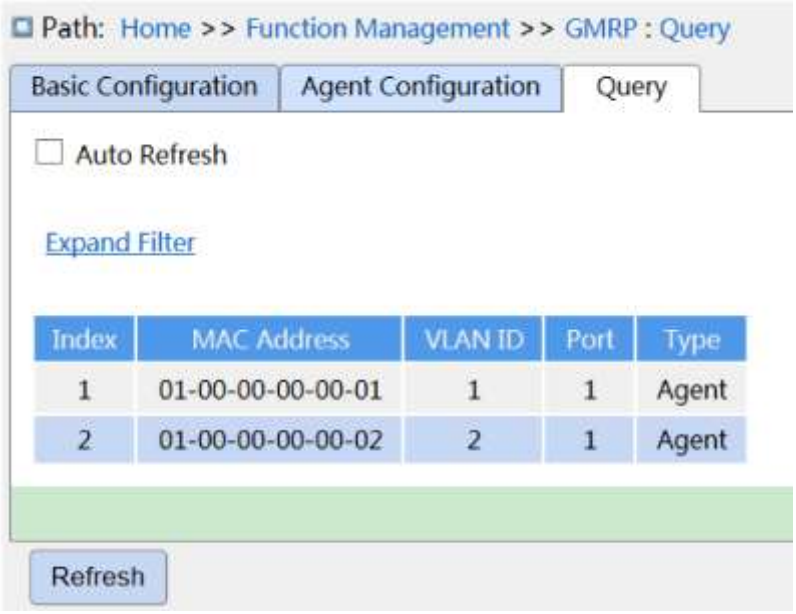


Рисунок 230 – Конфигурация GMRP

7.13.5 Пример типовой настройки

Как показано на рисунке 231, коммутатор A и коммутатор B подключены через порт 2. Порт 1 коммутатора A настроен как порт агента и создает две многоадресные записи:

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

После настройки различных атрибутов VLAN на портах наблюдайте за динамической регистрацией между коммутаторами и обновлением информации о многоадресной рассылке.

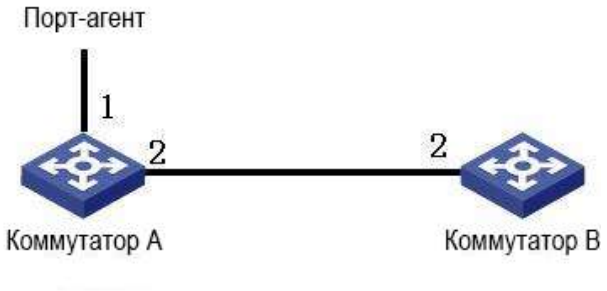


Рисунок 231 – Сеть GMRP

Настройка коммутатора A:

1. Включите глобальную функцию GMRP на коммутаторе A; оставьте для таймеров значение по умолчанию, как показано на рисунке 227.

2. Включите функцию GMRP и функцию агента для порта 1; включите только функцию GMRP для порта 2, как показано на рисунке 228.

3. Настройте многоадресную запись агента. Установите <MAC Address, VLAN ID, Port> на <01-00-00-00-00-01, 1, 1> и <01-00-00-00-00-02, 2, 1>, как показано на рисунке 229.

Настройка коммутатора B:

4. Включите глобальную функцию GMRP на коммутаторе B; оставьте для таймеров значения по умолчанию, как показано на рисунке 227.

5. Включите функцию GMRP на порту 2; оставьте для таймеров значения по умолчанию, как показано на рисунке 228.

В таблице 11 перечислены динамические записи многоадресной рассылки GMRP на коммутаторе B.

Таблица 11 – Динамические многоадресные записи

Атрибут порта 2 на коммутаторе A	Атрибут порта 2 на коммутаторе B	Многоадресные записи, полученные на коммутаторе B
Access VID=1	Access VID=1	MAC: 01-00-00-00-00-01 VLAN ID: 1 Member port: 2
Access VID=2	Access VID=2	MAC: 01-00-00-00-00-02 VLAN ID: 2 Member port: 2
Access VID=1	Access VID=2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Member port: 2

7.14 NAT

7.14.1 Введение

NAT (транслятор сетевых адресов) – это метод изменения исходного или конечного адреса в IP-пакете. Он позволяет нескольким хостам в локальной сети получать доступ к внешним ресурсам, используя небольшое количество легитимных адресов или по мере необходимости. Установите внутренние службы WWW, FTP, TELNET для использования внешней сети. NAT эффективно скрывает IP-адрес хоста внутренней локальной сети и играет роль в защите безопасности.

7.14.2 Принцип работы

Основной принцип работы NAT заключается в том, что только хосты внутренней сети нуждаются в доступе к Интернету для получения действительного публичного IP-адреса, в то время как внутренняя сеть использует частные IP-адреса. Когда пакет, предназначенный для доступа в Интернет, проходит через NAT-шлюз, этот шлюз заменяет исходный IP-адрес в пакете на действительный публичный IP-адрес и записывает эту замену в таблицу преобразований. Когда пакет возвращается из Интернета, NAT-шлюз ищет в своей таблице преобразований оригинальную запись, заменяет адрес назначения пакета на исходный адрес внутренней сети и отправляет его обратно к запрашивающему хосту. Таким образом, с точки зрения устройств внутренней и внешней сети, этот процесс не отличается от обычного сетевого доступа.

В примере, показанном на следующем рисунке, хост 10.1.1.1 отправляет исходящий пакет на граничное устройство, на котором настроен NAT. Граничное устройство распознает, что этот IP-адрес является внутренним локальным IP-адресом. Целью является внешняя сеть, поэтому граничное устройство преобразует внутренний локальный IP-адрес в публичный и регистрирует результаты преобразования в таблице NAT.

После преобразования пакет отправляется на внешний интерфейс с новым исходным адресом. Когда внешний хост возвращает пакет обратно к целевому хосту, маршрутизатор NAT использует таблицу NAT для перевода внутреннего глобального IP-адреса обратно во внутренний локальный IP-адрес и отправляет пакет к запрашивающему хосту.

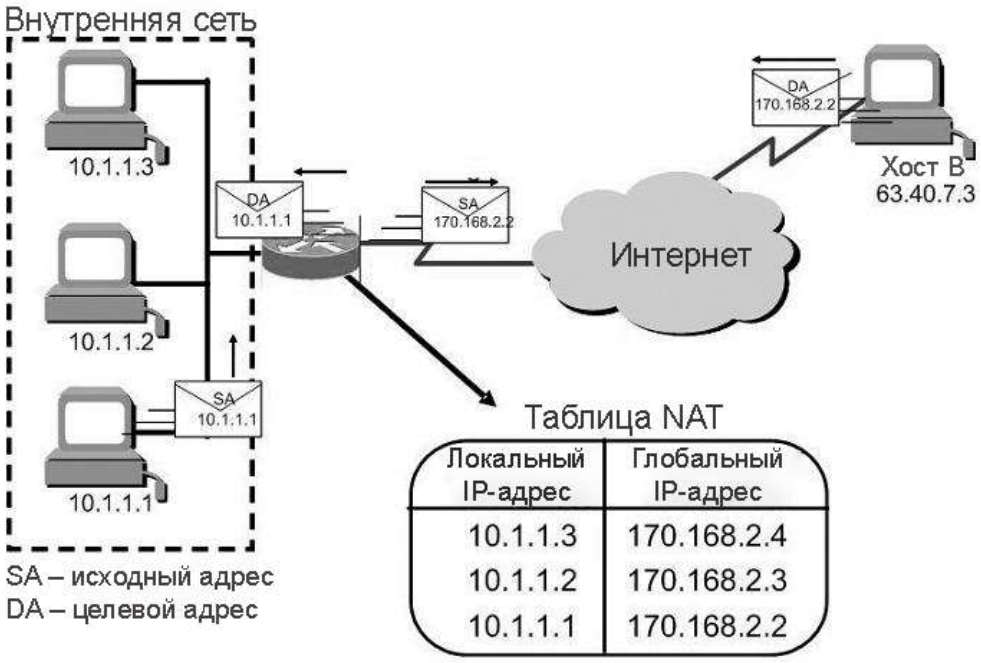


Рисунок 232 – Трансляция NAT

Функция NAT поддерживается только в коммутаторах 3-го уровня серии SEWM3GX28P.

7.14.3 Настройка с помощью WEB-интерфейса

1. Настройка интерфейса NAT

В дереве навигации выберите [Function Management] → [NAT] → [Interface Configuration], чтобы войти в меню настройки интерфейса NAT, как показано ниже.

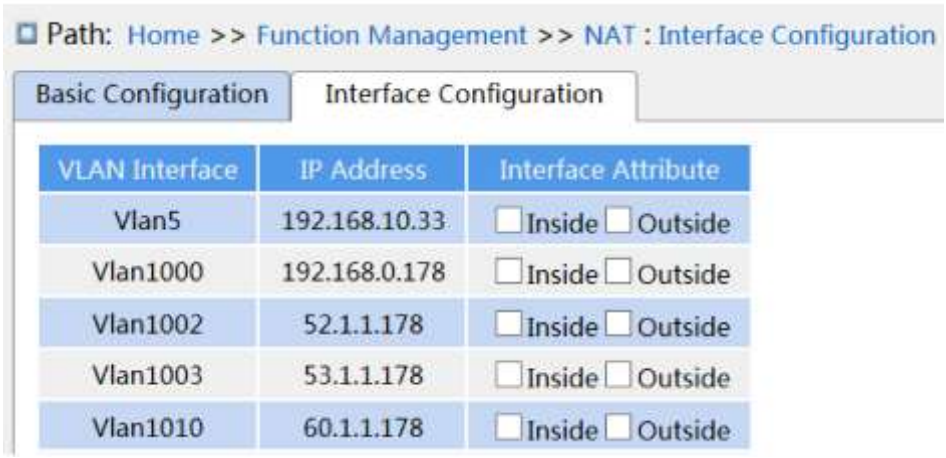


Рисунок 233 – Настройка интерфейса NAT

VLAN Interface

Функция: просмотр всех созданных интерфейсов уровня 3 устройства (исключая VLAN 1; VLAN 1 не поддерживает трансляцию NAT).

IP Address

Функция: отображение основного IP-адреса всех интерфейсов уровня 3 на устройстве (исключая VLAN 1).

Interface Attribute

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: настройка роли интерфейса для трансляции NAT (внутренний/внешний).

2. Базовая конфигурация NAT

В дереве навигации выберите [Function Management] → [NAT] → [Basic Configuration], чтобы войти в интерфейс базовой настройки NAT, как показано ниже.

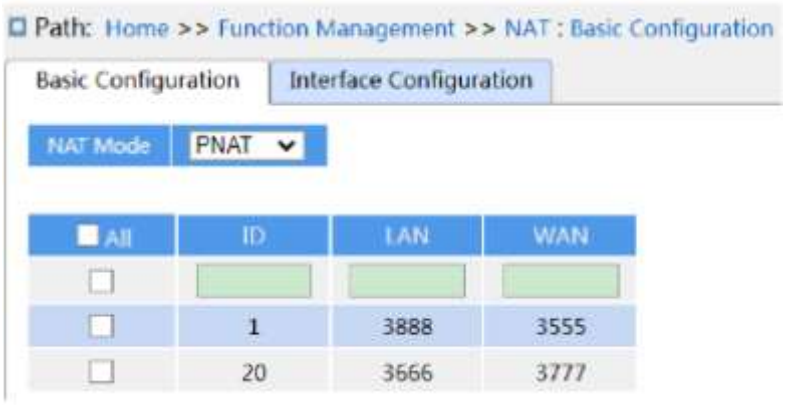


Рисунок 234 – Базовая конфигурация NAT

NAT Mode PNAT

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включает/отключает функцию PNAT, которая работает на основе VLAN-портов, позволяя преобразовывать адреса между внутренней (LAN) и внешней (WAN) сетями.

ID

Диапазон: 1–100

Функция: настройка номера идентификатора правила PNAT.

LAN

Диапазон: 2–4093

Функция: задает VLAN ID, который будет использоваться как внутренняя сторона интерфейса PNAT. Значение VLAN должно соответствовать локальной сети (внутренняя сеть).

WAN

Диапазон: 2–4093

Функция: задает VLAN ID, который будет использоваться как внешняя сторона интерфейса PNAT. Значение VLAN должно соответствовать внешней сети (интернет или другой внешний сегмент).

7.14.4 Пример типовой настройки

После преобразования адреса FTP-клиента внутренней сети с помощью NAT DUT1, можно получить доступ к FTP-серверу внешней сети.

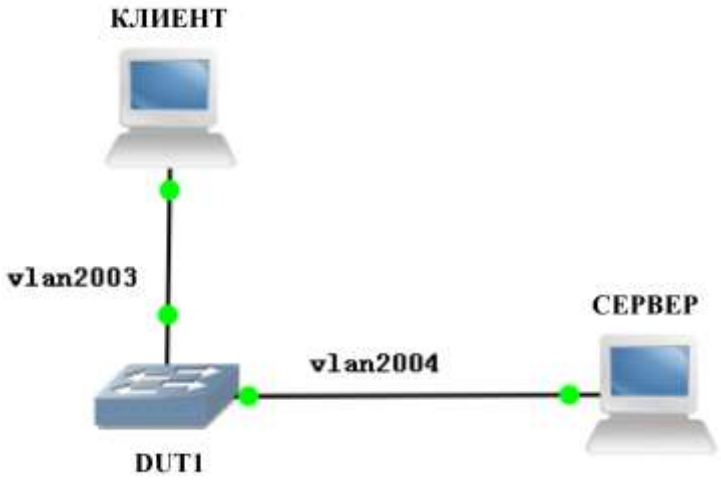


Рисунок 235 – Типовая конфигурация NAT

1. Настройте параметры IP интерфейса VLAN 2003: адрес 113.1.1.176, маска подсети 255.0.0.0. Настройте параметры IP интерфейса VLAN 2004: адрес 104.1.1.176, маска подсети: 255.0.0.0.

2. IP-адрес на стороне Клиента – 113.1.1.100/8, адрес шлюза – 113.1.1.176, а IP-адрес на стороне Сервера – 104.1.1.100/8.

3. Интерфейсы VLAN 2003 и VLAN 2004 на DUT1 являются соответственно внутренней и внешней сетью, как показано на рисунке 233.

4. Включите NAT на DUT1 и настройте правила PNAT для преобразования VLAN 2003 на стороне LAN в VLAN 2004 на стороне WAN, как показано на рисунке 234.

7.15 PIM

PIM (Protocol Independent Multicast) – это протокол независимой многоадресной рассылки, выполняющий проверку обратного пути передачи (Reverse Path Forwarding, RPF) для мультимедийных пакетов, используя существующую таблицу маршрутизации для одноадресных пакетов. Эта проверка помогает создавать записи многоадресной маршрутизации и строить дерево передачи мультимедийного трафика.

PIM поддерживает два режима работы:

PIM-DM (PIM Dense Mode) – режим плотного распространения, где трафик изначально распространяется во все сегменты сети и затем отбрасывается там, где не нужен;

PIM-SM (PIM Sparse Mode) – режим разреженного распространения, где трафик передается только в те участки сети, где есть получатели, что более эффективно при большом числе получателей, разбросанных по сети.

- К понятию «маршрутизатор», или «роутер» в этой главе относятся коммутаторы 3-го уровня.
- Протокол PIM поддерживается только в коммутаторах 3-го уровня серии SEWM3GX28P.

7.15.1 Настройка PIM-SM

7.15.1.1 Введение

PIM-SM использует режим «pull» (вытягивания), при котором дерево передачи мультимедийных данных строится на основе запросов от получателей. Это значит, что трафик направляется только туда, где есть заинтересованные получатели.

Построение дерева передачи в PIM-SM происходит в два этапа.

Первый этап: создается дерево передачи, состоящее из двух частей – дерева Rendezvous Point Tree (RPT) и дерева Shortest Path Tree (SPT). Центром этого дерева является Rendezvous Point (RP) – специальный узел, к которому присоединяются получатели и источники мультимедийного трафика.

Второй этап: после установления начального дерева происходит переключение на дерево SPT, которое напрямую соединяет получателей с источником мультимедийных данных по кратчайшему пути.

При работе PIM-SM источник мультимедийного трафика сначала отправляет данные на RP по дереву SPT, а RP затем пересылает эти данные получателям по дереву RPT.

7.15.1.2 Основные понятия

RP – это ключевой маршрутизатор в дереве передачи PIM-SM. Он собирает и обрабатывает сообщения типа Join и Prune от получателей, а также принимает мультимедийные данные от источников.

RPT – это дерево передачи, которое устанавливается между получателями и RP. Его иногда называют деревом RPT.

Для распространения информации о расположении RP и связанных с ним данных в сети используется специальный маршрутизатор Bootstrap Router (BSR). BSR распространяет сведения о RP среди всех маршрутизаторов в сети.

Сетевые администраторы могут настроить несколько кандидатов на роль BSR (Candidate BSR, C-BSR) и кандидатов на роль RP (Candidate RP, C-RP). Из всех кандидатов BSR с наивысшим приоритетом выбирается один, который становится настоящим (аутентичным) BSR.

7.15.1.3 Принцип работы

1. Обнаружение соседей

В домене PIM маршрутизаторы периодически отправляют специальные сообщения PIM Hello (далее – Hello-пакеты) на мультикаст-адрес 224.0.0.13. Это необходимо для обнаружения соседних PIM-маршрутизаторов и поддержания связи с ними. Обнаружение и поддержание соседних маршрутизаторов важно для построения и поддержания дерева кратчайшего пути (SPT).

2. Выбор главного маршрутизатора

С помощью Hello-пакетов также происходит выбор главного маршрутизатора (Designated Router, DR) для общих сетей (например, Ethernet). Этот DR становится единственным маршрутизатором, который пересылает мультимедийные данные в данной общей сети. Выбор DR необходим как на стороне сети, где находится источник мультимедиа, так и на стороне сети с получателями.

DR на стороне получателей отвечает за отправку сообщений Join к RP, чтобы присоединиться к мультимедийной группе.

DR на стороне источника отправляет регистрационные сообщения RP, информируя его о наличии источника мультимедийного трафика.

Процесс выбора DR происходит следующим образом:

Каждый маршрутизатор в общей сети периодически отправляет Hello-пакеты, в которых указывается параметр приоритета DR. Маршрутизатор с самым высоким значением приоритета становится главным маршрутизатором (DR).

Если приоритеты у нескольких маршрутизаторов совпадают или хотя бы один маршрутизатор в сети не поддерживает параметр приоритета DR в Hello-пакетах, то выбор DR производится на основе IP-адресов. В этом случае маршрутизатор с наибольшим IP-адресом становится DR.

Если текущий DR выходит из строя и другие маршрутизаторы перестают получать от него Hello-пакеты в течение заданного таймаута, запускается новый процесс выбора DR.

3. Обнаружение RP

RP – это ключевой маршрутизатор в домене PIM-SM. В небольших и простых сетях объем мультимедийной информации невелик, и для передачи многоадресного трафика достаточно одного RP. В таких случаях RP можно задать статически на каждом маршрутизаторе в домене PIM-SM. В более крупных и сложных сетях объем многоадресного трафика значительно увеличивается, и один RP может стать узким местом. Чтобы разгрузить RP и оптимизировать топологию дерева RPT, в домене PIM-SM можно настроить несколько кандидатов в RP (C-RP). Выбор настоящих RP среди кандидатов выполняется динамически с помощью механизма Bootstrap. Для работы этого механизма в сети конфигурируется специальный маршрутизатор – BootStrap Router (BSR). BSR управляет информацией о RP и распространяет ее по всему домену PIM-SM. В домене может быть только один активный BSR, однако можно настроить несколько кандидатов в BSR (C-BSR). Если текущий BSR выходит из строя, один из кандидатов автоматически становится новым BSR, что обеспечивает непрерывность работы мультикаст-сервиса.

BSR отвечает за сбор сообщений объявлений, отправляемых кандидатами в RP (C-RP) в сети. Каждое такое объявление содержит IP-адрес C-RP, его приоритет и диапазон мультимедийных групп, за которые он отвечает.

BSR собирает всю эту информацию и формирует специальный набор – RP-Set (множество RP), представляющий собой сопоставления между мультимедийными группами и назначенными RP. Затем BSR распространяет этот RP-Set по всему домену PIM-SM через Bootstrap-сообщения.

Каждый маршрутизатор в сети выбирает свой соответствующий RP для определенной группы многоадресной рассылки из нескольких C-RP на основе информации, предоставленной в RP-Set, руководствуясь следующими правилами:

Сначала сравниваются приоритеты C-RP – выбирается RP с наивысшим приоритетом.

Если приоритеты совпадают, то для выбора используется значение хэша, вычисляемое специальной хеш-функцией. Выбирается C-RP с большим хеш-значением.

Если и приоритет, и хеш-значение совпадают, то побеждает C-RP с большим IP-адресом.

4. Построение дерева RPT

Когда приемник хочет присоединиться к мультимедийной группе G, он отправляет сообщение IGMP своему ближайшему маршрутизатору DR.

Получив информацию о новом приемнике группы G, DR начинает поэтапно отправлять сообщения Join в сторону RP, соответствующего этой группе.

Все маршрутизаторы на пути от DR до RP формируют ветвь дерева RPT. В их таблицах маршрутизации создаются записи вида (∗, G), где символ «*» означает, что трафик может поступать от любого источника. В таком дереве корнем является RP, а листьями – DR, подключенные к приемникам.

Когда мультимедийные данные для группы G поступают на RP, они передаются по дереву RPT к соответствующим DR, а затем к конечным приемникам.

Если приемник больше не хочет получать данные группы G, его ближайший DR отправляет сообщения Prune (обрезки) по тому же пути к RP. Каждый маршрутизатор, получивший Prune, удаляет из своей таблицы интерфейс, ведущий к этому приемнику, и проверяет, есть ли еще другие приемники группы G в этом направлении. Если приемников нет, сообщение Prune пересылается дальше вверх по дереву к RP.

5. Механизм регистрации источника многоадресной рассылки

Поскольку маршрутизатор BSR распространяет информацию о местоположении маршрутизатора RP всей сети PIM-SM в многоадресном режиме, источники многоадресной рассылки также знают местоположение RP. Когда источник мультимедиа собирается начать передачу данных, он инкапсулирует эти данные в сообщения регистрации (Registration) и отправляет их в режиме одноадресной передачи непосредственно на RP, который соответствует группе, в которой он участвует. RP принимает эти регистрационные пакеты, декапсулирует из них полезные мультикаст-данные и пересылает их дальше в сеть, к подписчикам группы.

После получения регистрации от источника RP инициирует отправку Join (S, G) – запроса установления маршрута от RP к источнику S для многоадресной группы G. Этот запрос

проходит через маршрутизаторы по пути назад к источнику, и каждый узел создает запись (S, G), строя таким образом дерево кратчайшего пути. После установления SPT-дерева источник начинает напрямую отправлять многоадресные данные на RP по построенному маршруту.

Когда RP получает мультикаст-данные напрямую по SPT-дереву, он отправляет регистрирующему источнику специальный пакет – Registration Stop. Этот пакет уведомляет источник о том, что дальнейшая инкапсуляция данных в регистрационные сообщения не требуется, и источник может отправлять данные напрямую. Этот процесс называется механизмом остановки регистрации.

6. Механизм переключения на SPT

Когда источник многоадресной рассылки находится далеко от RP, но близко к получателю, маршрутизация через RP может привести к ненужным задержкам, так как данные проходят длинный путь через RP, что увеличивает время доставки до получателя. Механизм переключения на SPT помогает решить эту проблему.

Маршрутизатор DR отправляет команду Join (S, G) – запрос на установление прямого маршрута от получателя к источнику S для группы G. По мере прохождения этого Join-запроса по сети каждый маршрутизатор на пути создает запись (S, G), формируя дерево кратчайшего пути (SPT) между источником и получателем. Когда Join-запрос достигает источника S, устанавливается SPT-дерево, по которому данные будут передаваться напрямую от DR источника к получателю, минуя RP.

После того как получатель начинает принимать данные через SPT-дерево, маршрутизатор DR отправляет Prune-сообщение на RP. Это сообщение уведомляет RP о том, что данные теперь идут напрямую по SPT, и RP может прекратить пересылку этих данных по своему RPT-маршруту. Маршрутизаторы, получающие Prune, удаляют интерфейсы, по которым данные передавались через RP, обновляют записи (*, G) и (S, G), тем самым оптимизируя маршрутизацию.

Переключение на SPT не является обязательным. Мультикаст-роутеры могут выбирать, использовать ли SPT (прямой маршрут от источника к получателю) или продолжать передачу через RPT (маршрут через RP), в зависимости от политики и условий сети.

7. Механизм Assert:

В сетевом сегменте может находиться несколько маршрутизаторов многоадресных данных, которые получают один и тот же мультикаст-пакет и пытаются переслать его дальше по одному и тому же локальному сегменту. Это приводит к дублированию пакетов и избыточному трафику. Чтобы избежать такой ситуации, используется механизм Assert, который выбирает единственного распространителя мультимедиа – маршрутизатор forwarder – для пересылки мультикаст-пакетов в данном сегменте.

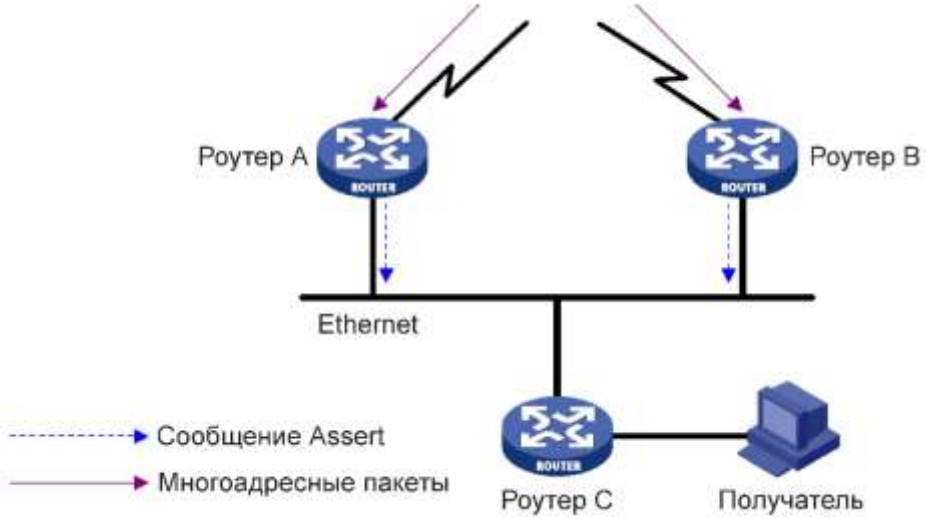


Рисунок 236 – Схема работы механизма Assert

Как показано на рисунке выше, роутеры A и B подключены к одному локальному сегменту и оба получают мультикаст-пакеты (S, G) от вышестоящего узла. Оба маршрутизатора начинают пересылать эти пакеты в локальную сеть. В результате, конечный узел C получает дубликаты одного и того же пакета. Роутеры A и B получают мультикаст-пакеты, которые были отправлены друг другом по интерфейсу в локальной сети. Это сигнализирует о том, что в сегменте есть несколько потенциальных распространителей одинаковых пакетов. Чтобы решить, какой из маршрутизаторов будет пересылать пакеты, A и B отправляют специальные Assert-сообщения на адрес 224.0.0.13 (мультикастовый адрес PIM), содержащие следующую информацию:

- адрес источника многоадресной рассылки S;
- адрес мультикаст-группы G;
- приоритет одноадресного маршрута к источнику;
- метрику одноадресного маршрута к источнику;
- IP-адрес локального интерфейса.

После обмена Assert-сообщениями маршрутизаторы сравнивают свои параметры по следующим правилам:

- Побеждает роутер с более высоким маршрутизатор одноадресного маршрута к источнику.
- Если приоритеты равны, побеждает маршрутизатор с меньшей метрикой одноадресного маршрута к источнику.
- Если метрики тоже равны, побеждает маршрутизатор с большим IP-адресом локального интерфейса.

Маршрутизатор-победитель становится единственным транслятором мультикаст-пакетов (S, G) в данном локальном сегменте. Остальные маршрутизаторы прекращают пересылать эти пакеты, тем самым устраняя дублирование.

7.15.1.4 Настройка с помощью WEB-интерфейса

1. Ниже показана базовая конфигурация PIM-SM.

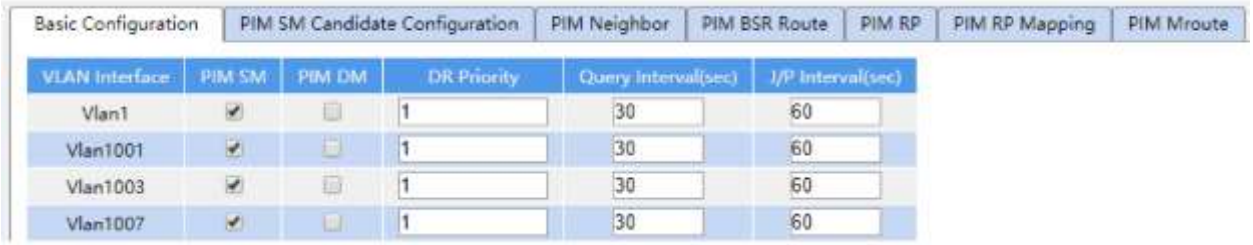


Рисунок 237 – Базовая конфигурация PIM-SM

VLAN Interface

Варианты настройки: созданные интерфейсы VLAN уровня 3

PIM-SM

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение и отключение ли функции PIM-SM на интерфейсе уровня 3.

DR Priority

Диапазон: 0–4294967294

По умолчанию: 1

Функция: настройка приоритета интерфейса VLAN уровня 3.

Query-Interval (sec)

Диапазон: 1–18724 с

По умолчанию: 30 с

Функция: настройка интервала отправки Hello-пакетов на интерфейсе уровня 3 для обнаружения соседних маршрутизаторов PIM.

J/P Interval (sec)

Диапазон: 1–65535 с

По умолчанию: 60 с

Функция: настройка интервала, с которым интерфейс уровня 3 отправляет сообщения Join и Prune.

2. Ниже показана настройка кандидатов PIM SM.

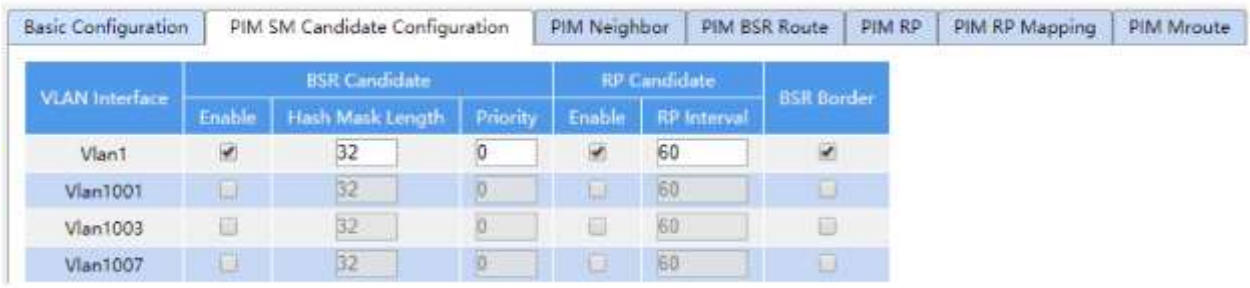


Рисунок 238 – Настройка кандидатов PIM SM

VLAN Interface

Варианты настройки: созданные интерфейсы VLAN уровня 3

BSR Candidate-Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: настройка IP-адреса интерфейса VLAN уровня 3 в качестве адреса C-BSR. Этот роутер будет отправлять BSR-сообщения всем соседям PIM.

BSR Candidate-Hash Mask Length

Диапазон: 0–32

По умолчанию: 32

Функция: определяет, сколько старших битов IP-адреса многоадресной группы участвуют в вычислении хэша, который используется для выбора RP.

BSR Candidate-Priority

Диапазон: 0–255

По умолчанию: 0

Функция: задает приоритет для выбора BSR среди нескольких кандидатов. Чем выше значение, тем выше приоритет.

RP Candidate-Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: настройка IP-адреса интерфейса VLAN уровня 3 в качестве адреса C-RP. Этот адрес будет использоваться для приема регистрационных пакетов, сообщений Join/Prune и построения дерева многоадресной передачи.

RP Candidate-RP Interval

Диапазон: 1–16383 с

По умолчанию: 60 с

Функция: определяет периодичность, с которой C-RP отправляет уведомления BSR о своей кандидатуре.

BSR Border

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: позволяет пометить интерфейс VLAN уровня 3 как границу области BSR. Это означает, что данный интерфейс служит границей для распространения BSR сообщений.

3. Просмотрите информацию о соседних устройствах PIM, как показано ниже.

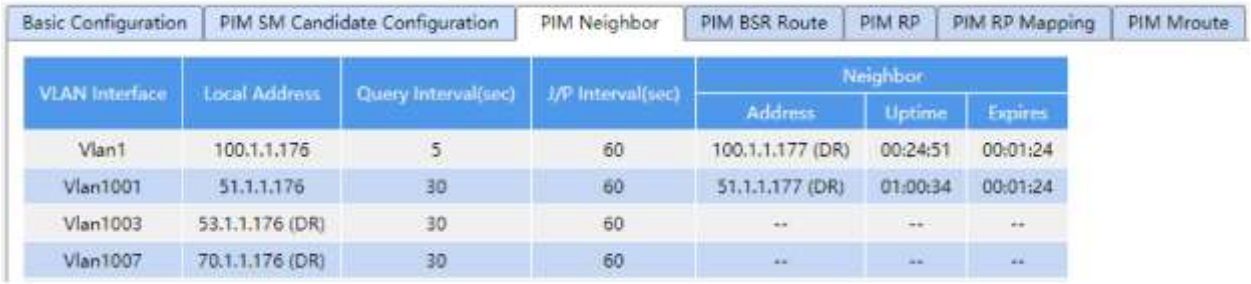


Рисунок 239 – Информация о соседях PIM

Поля отображаемой информации описаны в следующей таблице.

Таблица 12 – Описание параметров соседей PIM

Параметр	Описание
VLAN Interface	Порт VLAN уровня 3 коммутатора, через который происходит маршрутизация многоадресного трафика и установление PIM-соседства
Local Address	IP-адрес интерфейса коммутатора, который участвует в PIM
Query Interval (sec)	Интервал (в секундах), с которым интерфейс отправляет Hello-пакеты PIM
J/P Interval (sec)	Интервал (в секундах), с которым интерфейс отправляет сообщения Join/Prune
Neighbor Address	IP-адрес PIM-соседа, то есть другого маршрутизатора или коммутатора, с которым установлен соседский статус PIM
Neighbor Uptime	Время, в течение которого PIM-соседство с этим соседом активно и поддерживается. Формат – часы:минуты:секунды
Neighbor Expires	Время, оставшееся до истечения срока действия соседства, если не поступят новые Hello-пакеты от соседа. Формат – часы:минуты:секунды

4. Просмотрите информацию о PIM BSR, как показано ниже.

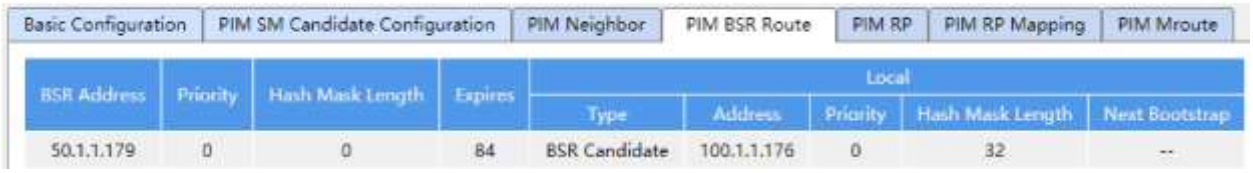


Рисунок 240 – Информация о PIM BSR

Поля отображаемой информации описаны в следующей таблице.

Таблица 13 – Описание параметров PIM BSR

Параметр	Описание
BSR Address	Текущий сетевой адрес BSR
Priority	Приоритет BSR
Hash Mask Length	Длина хэш-маски BSR
Expires	Время истечения срока действия BSR (секунды)
Local Type	Статус кандидата BSR (BSR/BSR Candidate) на этой машине
Local Address	Адрес C-BSR на этой машине. Если кандидат выбран в качестве BSR, информация не отображается
Local Priority	Приоритет C-BSR на локальном устройстве. Если кандидат выбран в качестве BSR, информация не отображается
Local Hash Mask Length	Длина хэш-маски C-BSR на этой машине. Если кандидат выбран в качестве BSR, информация не отображается
Local Next Bootstrap	Интервал отправки следующего пакета Bootstrap маршрутизатором BSR на локальном устройстве. Если это кандидат BSR, информация отображается.

5. Просмотрите информацию о PIM RP, как показано ниже.

Рисунок 241 – Информация о PIM RP

Поля отображаемой информации описаны в следующей таблице.

Таблица 14 – Описание параметров PIM RP

Параметр	Описание
Group	Групповой адрес
Valid	Показывает, актуален RP или нет
RP	RP, соответствующий групповому адресу

6. Просмотрите информацию о маппинге PIM RP, как показано ниже.

Рисунок 242 – Маппинг PIM RP

Поля отображаемой информации описаны в следующей таблице.

Таблица 15 – Описание параметров PIM RP

Параметр	Описание
Group	Групповой адрес
C-RP	C-RP, соответствующий групповому адресу
Timeout	Тайм-аут C-RP, отображается в формате «часы:минуты:секунды»

6. Просмотрите информацию о маршрутах PIM, как показано ниже.

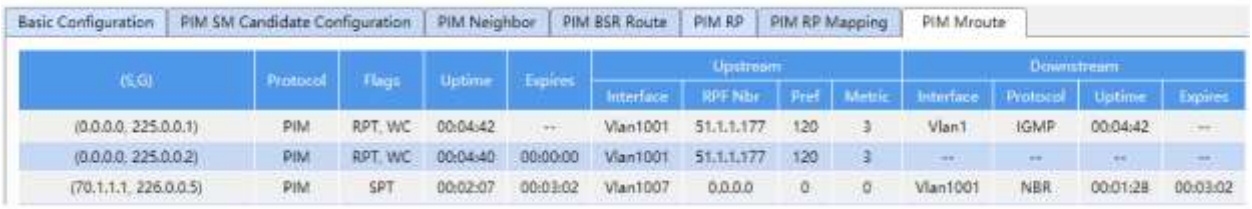


Рисунок 243 – Маршруты PIM

Поля отображаемой информации описаны в следующей таблице.

Таблица 16 – Маршруты PIM

Параметр	Описание
(S, G)	Записи (*, G) или (S, G), созданные приемником или многоадресным потоком
Protocol	Текущий запущенный протокол
Flags	Флаги записей (S, G) или (*, G) в таблице маршрутизации PIM
Uptime	Время активности (*, G) или (S, G)
Expires	Через какое время истекает срок действия записей (*, G) или (S, G)
Upstream-Interface	Входной интерфейс, связанный с конкретной записью (S, G) или (*, G) в таблице маршрутов PIM-SM Для (*, G) – интерфейс, по которому мультикастовые пакеты направляются к RP Для (S, G) – это интерфейс, по которому пакеты поступают от источника
Upstream-RPF Nbr	Сосед по обратному пути (RPF), связанный с конкретной записью в таблице маршрутов PIM-SM Для (*, G) – это соседний интерфейс, который «смотрит» на RP Для (S, G) – это соседний интерфейс, который «смотрит» на источник Если устройство само является RP для группы G, то запись (*, G) у него не имеет Upstream-соседа, так как оно – конечная точка RP. В этом случае RPF Nbr обозначается как 0.0.0.0 (нет следующего хопа) Если устройство напрямую подключено к источнику S, то для записи (S, G) RPF Nbr тоже будет 0.0.0.0, так как источник подключен напрямую и нет промежуточного соседа
Upstream-Pref	Административная дистанция маршрута, который используется при определении RPF-соседа для записи (S, G) или (*, G) в таблице маршрутизации PIM
Upstream-Metric	Метрика маршрута, по которому определяется RPF-сосед для записи (S, G) или (*, G). Метрика – это числовое значение, отражающее «стоимость» маршрута. Чем меньше метрика, тем предпочтительнее маршрут

Downstream-Interface	Выходной интерфейс, через который коммутатор отправляет трафик для (S, G) или (*, G)
Downstream-Protocol	Тип протокола, используемого на выходном интерфейсе для передачи многоадресного трафика
Downstream-Uptime	Время существования выходного интерфейса, которое показывает, как долго интерфейс был активен и использовался для передачи многоадресного трафика
Downstream-Expires	Таймаут для выходного интерфейса, который показывает, сколько времени осталось до окончания активности

7.15.1.5 Пример типовой настройки

Как показано ниже, маршрутизаторы Router1, Router2, Router3, Router4 могут поддерживать протокол PIM-SM; S означает источник, а R означает получателей.

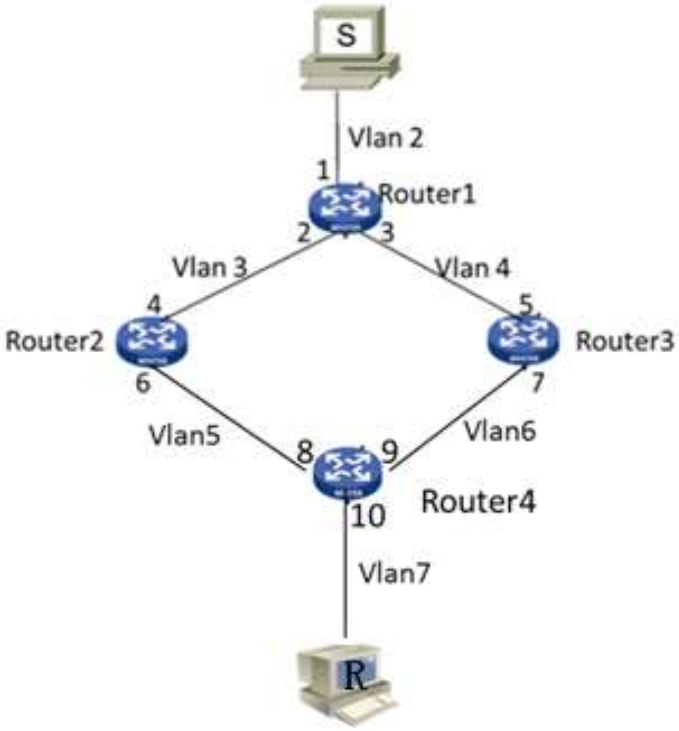


Рисунок 244 – Пример PIM SM

1. Настройте идентификаторы маршрутизаторов и включите протокол Open Shortest Path First (OSPF). Подробный процесс настройки см. в разделе 7.17.3 «OSPF».

2. Настройка Router1:

- Создайте VLAN 2, VLAN 3 и VLAN 4 и добавьте порт 1 к VLAN 2, порт 2 к VLAN 3 и порт 3 к VLAN 4. Подробный процесс настройки см. в разделе 7.2 «VLAN».

- Настройте интерфейсы уровня 3 со следующими адресами: порт 1 – 20.0.0.2, порт 2 – 30.0.0.2 и порт 3 – 40.0.0.4. Подробный процесс настройки см. в разделе 7.3.
- Включите PIM-SM на каждом созданном интерфейсе VLAN уровня 3 и настройте интервал запроса пакетов, как показано на рисунке 237.

3. Настройка Router2:

- Создайте VLAN 3, VLAN 5 и добавьте порт 4 к VLAN 3, порт 6 к VLAN 5.
- Настройте интерфейсы уровня 3 со следующими адресами: порт 4 – 30.0.0.4, порт 6 – 50.0.0.4.
- Включите PIM-SM на каждом созданном интерфейсе VLAN уровня 3 и настройте интервал запроса пакетов, как показано на рисунке 237.

4. Настройка Router3:

- Создайте VLAN 4, VLAN 6 и добавьте порт 5 к VLAN 4, порт 7 к VLAN 6.
- Настройте интерфейсы уровня 3 со следующими адресами: порт 5 – 30.0.0.4, порт 7 – 60.0.0.4.
- Включите PIM-SM на каждом созданном интерфейсе VLAN уровня 3 и настройте интервал запроса пакетов, как показано на рисунке 237.

5. Настройка Router4:

- Создайте VLAN 5, VLAN 6 и VLAN 7 и добавьте порт 8 к VLAN 5, порт 9 к VLAN 6 и порт 10 к VLAN 7.
- Настройте интерфейсы уровня 3 со следующими адресами: порт 8 – 50.0.0.8, порт 9 – 60.0.0.9, порт 10 –70.0.0.10.
- Включите PIM-SM на каждом созданном интерфейсе VLAN уровня 3 и настройте интервал запроса пакетов, как показано на рисунке 237.

6. Настройте границу BSR (необязательно): отметьте интерфейс уровня 3 в качестве границы BSR PIM-SM, как показано на рисунке 238.

7. Настройте C-BSR как показано на рисунке 238: отметьте порт 2 маршрутизатора Router1 как BSR Candidate со значением «Priority» 0 и значением «Hash Mask Length» 0.

8. Настройте C-RP как показано на рисунке 238: отметьте порт 4 маршрутизатора Router4 и порт 5 маршрутизатора Router3 как RP Candidate со значением «RP Interval» 60.

9. Просмотрите конфигурацию, как описано выше в этой главе.

- Router1, Router2 и Router3 могут быть настроены как C-BSR. Аутентичный BSR может быть определен посредством выборов, или указан вручную.
- После настройки интерфейса как границы BSR, он будет блокировать прием или передачу BSR-сообщений. Поэтому границу надо настраивать на интерфейсе, за пределы которого BSR-сообщения распространяться не должны. Эту функцию не нужно настраивать для всех маршрутизаторов.

7.15.2 Настройка PIM-DM

7.15.2.1 Введение

PIM-DM использует режим «push» (проталкивания) для передачи многоадресных данных и обычно применяется в сетях с относительно плотным распределением участников многоадресных групп.

Основные принципы работы PIM-DM следующие:

PIM-DM предполагает, что в каждой подсети сети присутствует хотя бы один участник многоадресной группы, поэтому многоадресные данные изначально распространяются (flooding) на все узлы сети. Затем происходит процесс отсечения ветвей (pruning), по которым нет получателей многоадресного трафика. Оставляются только те ветви, где находятся получатели. Этот цикл «flooding-pruning» повторяется периодически, а ранее отсеченные ветви также могут периодически восстанавливаться для передачи трафика.

Если на узле, который был отсечен, появляется участник многоадресной группы, PIM-DM использует механизм «graft» – активное восстановление передачи многоадресных данных, что позволяет сократить время восстановления передачи на этом узле.

Как правило, путь передачи данных в режиме плотного распространения формируется в виде Source Tree – дерева с корнем в источнике многоадресного трафика и листьями в виде участников группы. Поскольку Source Tree строится по кратчайшему пути от источника к получателю, его также называют Shortest Path Tree (SPT).

7.15.2.2 Принцип работы

1. Обнаружение соседей

PIM-DM использует механизм обнаружения соседей, аналогичный PIM-SM, подробности см. в разделе 7.15.1.3.

2. Построение SPT

Процесс построения SPT в PIM-DM представляет собой циклическое чередование двух основных этапов: флудинг (flooding) и отсечение (pruning).

Когда источник многоадресного трафика S начинает передачу данных в многоадресную группу G, маршрутизаторы в домене PIM-DM сначала распространяют пакет на все интерфейсы, кроме интерфейса, с которого пакет был получен (RPF-интерфейс). После прохождения проверки RPF маршрутизатор создает запись (S, G) в своей таблице многоадресной маршрутизации и пересылает пакет на все свои выходные интерфейсы. В результате флудинга запись (S, G) появляется на каждом маршрутизаторе в домене PIM-DM.

После флудинга маршрутизаторы, которые не имеют локальных получателей многоадресной группы G, инициируют процесс отсечения. Такие маршрутизаторы отправляют Prune-сообщения своим вышестоящим маршрутизаторам, чтобы уведомить их удалить соответствующий интерфейс из списка выходных интерфейсов для записи (S, G). Это приводит к прекращению пересылки многоадресного трафика по этим интерфейсам.

Процесс отсечения начинается с листовых маршрутизаторов (например, непосредственно подключенных к хостам без подписки на группу) и распространяется вверх по дереву, пока не останутся только необходимые ветви, ведущие к реальным получателям. Эти ветви формируют дерево кратчайшего пути – SPT.

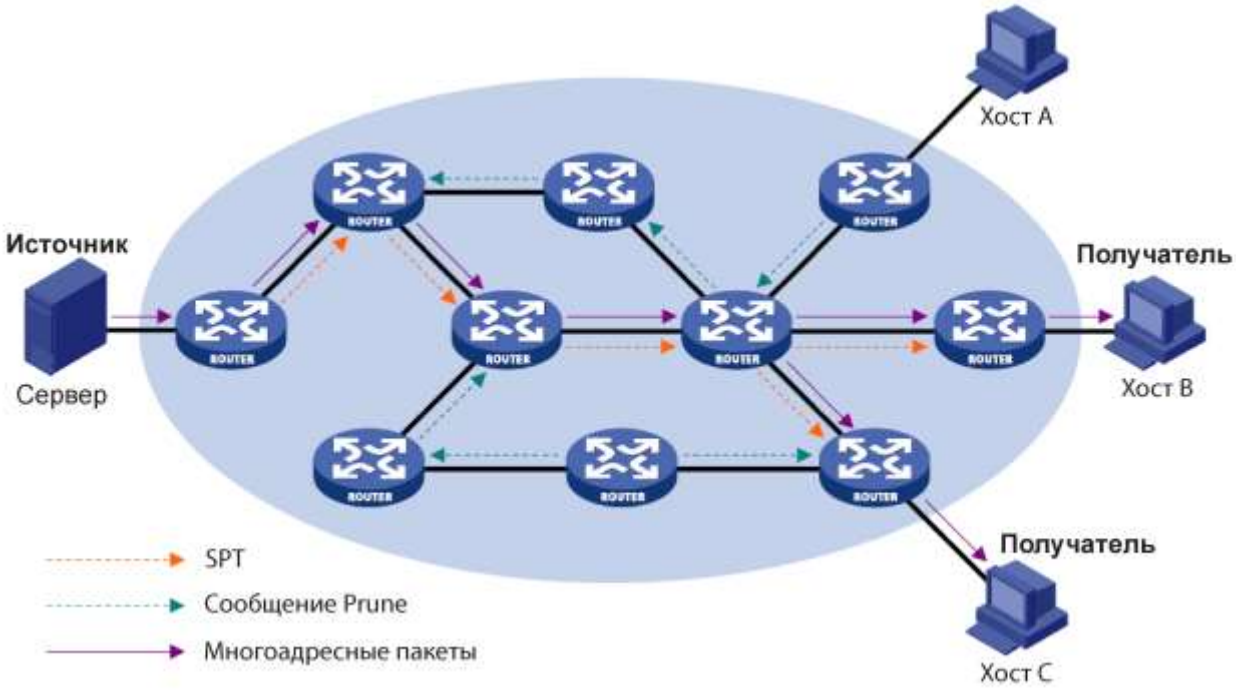


Рисунок 245 – Принципиальная схема построения SPT в PIM-DM

Процесс «flooding-pruning» повторяется периодически, чтобы обеспечить актуальность маршрутов и учесть изменения в составе группы.

Каждый отсеченный интерфейс имеет таймаут: по истечении времени таймаута происходит повторное распространение трафика по этому интерфейсу, что позволяет восстановить доставку мультимедиа в случае появления новых получателей.

3. Механизм Graft

Когда на узле, ранее отсеченном от передачи многоадресного трафика, появляется новый участник многоадресной группы, для ускоренного восстановления передачи данных используется механизм Graft – активное повторное присоединение к дереву передачи. Процесс состоит из следующих этапов:

Узел, на котором появился новый получатель, отправляет своему вышестоящему маршрутизатору Graft-сообщение с запросом на повторное включение в SPT и возобновление пересылки многоадресного трафика.

Получив Graft-сообщение, вышестоящий маршрутизатор восстанавливает состояние передачи для соответствующего интерфейса (восстанавливает его в списке выходных интерфейсов для записи (S, G)) и начинает пересылать трафик на нижестоящий узел. После этого он отправляет сообщение Graft-Ack в подтверждение успешного восстановления.

Если нижестоящий маршрутизатор не получает Graft-Ack в течение заданного времени, он повторно отправляет Graft-сообщение до тех пор, пока не получит подтверждение.

7. Механизм Assert

PIM-DM использует механизм Assert, аналогичный PIM-SM, подробности см. в разделе 7.15.1.3.

7.15.2.3 Настройка с помощью WEB-интерфейса

1. Ниже показана базовая конфигурация PIM-DM.

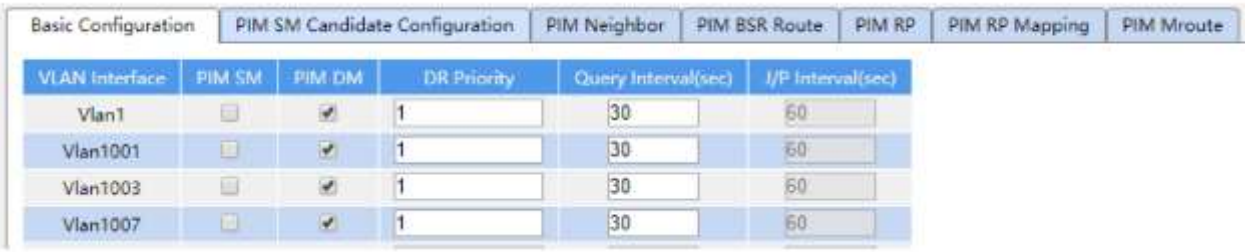


Рисунок 246 – Базовая конфигурация PIM-DM

VLAN Interface

Варианты настройки: созданные интерфейсы VLAN уровня 3

PIM-DM

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение и отключение ли функции PIM-DM на интерфейсе уровня 3.

DR Priority

Диапазон: 0–4294967294

По умолчанию: 1

Функция: настройка приоритета интерфейса VLAN уровня 3.

Query-Interval (sec)

Диапазон: 1–18724 с

По умолчанию: 30 с

Функция: настройка интервала отправки Hello-пакетов на интерфейсе уровня 3 для обнаружения соседних маршрутизаторов PIM.

2. Просмотр информации о соседних устройствах PIM

Аналогично PIM-SM, см. раздел 7.15.1.4.

3. Просмотр информации о маршрутах PIM

Аналогично PIM-SM, см. раздел 7.15.1.4.

7.15.2.4 Пример типовой настройки

Как показано ниже, маршрутизаторы Router1, Router2, Router3, Router4 могут поддерживать протокол PIM-DM; S означает источник, а R означает получателей.

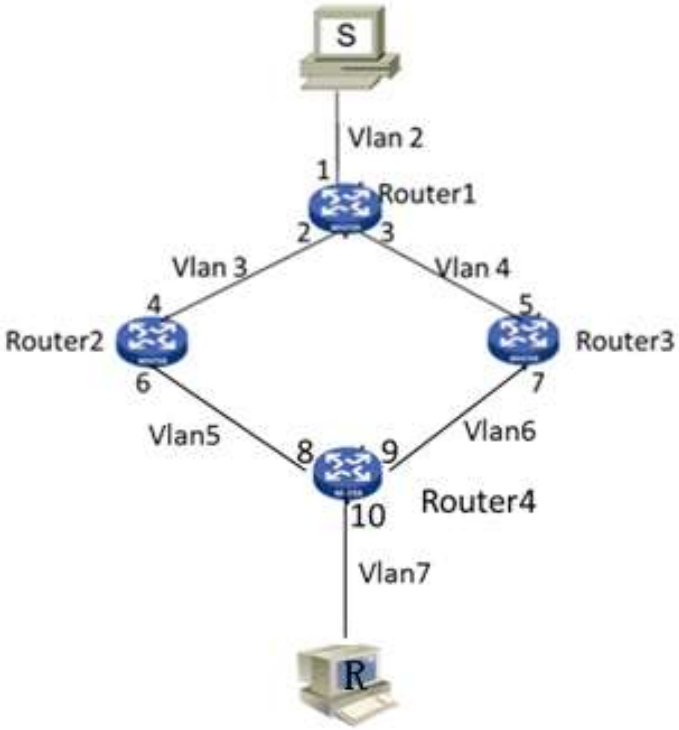


Рисунок 247 – Пример PIM DM

1. Настройте идентификаторы маршрутизаторов и включите протокол Open Shortest Path First (OSPF). Подробный процесс настройки см. в разделе 7.17.3 «OSPF».
2. Настройка Router1:

- Создайте VLAN 2, VLAN 3 и VLAN 4 и добавьте порт 1 к VLAN 2, порт 2 к VLAN 3 и порт 3 к VLAN 4. Подробный процесс настройки см. в разделе 7.2 «VLAN».
- Настройте интерфейсы уровня 3 со следующими адресами: порт 1 – 20.0.0.2, порт 2 – 30.0.0.2 и порт 3 – 40.0.0.4. Подробный процесс настройки см. в разделе 7.3 «Конфигурация IP».
- Включите PIM-DM на каждом созданном интерфейсе VLAN уровня 3 и настройте интервал запроса пакетов, как показано на рисунке 246.

3. Настройка Router2:

- Создайте VLAN 3, VLAN 5 и добавьте порт 4 к VLAN 3, порт 6 к VLAN 5.
- Настройте интерфейсы уровня 3 со следующими адресами: порт 4 – 30.0.0.4, порт 6 – 50.0.0.4.
- Включите PIM-DM на каждом созданном интерфейсе VLAN уровня 3 и настройте интервал запроса пакетов, как показано на рисунке 246.

4. Настройка Router3:

- Создайте VLAN 4, VLAN 6 и добавьте порт 5 к VLAN 4, порт 7 к VLAN 6.
- Настройте интерфейсы уровня 3 со следующими адресами: порт 5 – 30.0.0.4, порт 7 – 60.0.0.4.
- Включите PIM-DM на каждом созданном интерфейсе VLAN уровня 3 и настройте интервал запроса пакетов, как показано на рисунке 246.

5. Настройка Router4:

- Создайте VLAN 5, VLAN 6 и VLAN 7 и добавьте порт 8 к VLAN 5, порт 9 к VLAN 6 и порт 10 к VLAN 7.
- Настройте интерфейсы уровня 3 со следующими адресами: порт 8 – 50.0.0.8, порт 9 – 60.0.0.9, порт 10 –70.0.0.10.
- Включите PIM-DM на каждом созданном интерфейсе VLAN уровня 3 и настройте интервал запроса пакетов, как показано на рисунке 246.

6. Просмотрите соседние устройства PIM и таблицу маршрутизации, как описано в разделе 7.15.1.4.

7.16 IGMP

7.16.1 Введение

IGMP – это протокол, предназначенный для управления членством в группах многоадресной рассылки. Он работает на конечных устройствах, устанавливая и поддерживая участие в группе многоадресной рассылки между IP-хостами и соседними маршрутизаторами, поддерживающими многоадресную передачу.

Существует три версии IGMP: IGMPv1, IGMPv2 и IGMPv3. Данное устройство не поддерживает IGMPv3.

Основные различия между IGMPv1 и IGMPv2 следующие:

- Выбор запросчика: IGMPv2 использует формальный механизм выбора опрашивающего устройства, который назначает маршрутизатор с наименьшим IP-адресом в качестве опрашивающего. В IGMPv1 такого механизма нет, и различные протоколы маршрутизации могут использовать свои собственные методы выбора.
- Сообщение Leave Group: IGMPv2 добавляет сообщение Leave Group. Когда хост покидает группу, он активно отправляет пакет Leave Group. В IGMPv1 пакет Leave Group не отправляется активно.
- Max Resp Time: в IGMPv2 добавлено новое поле Max Resp Time в пакеты запросов. Это поле указывает максимальное время ответа, установленное запрашивающим. Значение по умолчанию составляет 10 секунд.
- Запросы, специфичные для группы: в IGMPv2 запросчику разрешается выполнять запросы для конкретной группы, а не для всех групп, отправляя сообщение, специфичное только для данной группы.

Понятие «маршрутизаторы» в этой главе относится к коммутаторам третьего уровня.

7.16.2 Принцип работы

Ниже на примере IGMPv2 описан механизм реализации протокола IGMP.

1. Механизм выбора запросчика

Все маршрутизаторы IGMPv2 изначально считают себя опрашивающими (Querier) и отправляют пакет запроса (Query). Если маршрутизатор получает пакет запроса от другого маршрутизатора с IP-адресом, меньшим, чем его собственный, он отказывается от роли запросчика и становится «не-опрашивающим» (Non-querier). В итоге в качестве запросчика выбирается маршрутизатор с наименьшим IP-адресом.

- General Query (общий запрос)

Опрашивающий периодически отправляет общий запрос, чтобы проверить наличие участников в многоадресной группе. Адрес назначения такого пакета всегда 224.0.0.1.

- Membership Report (отчет о членстве)

При получении запроса хост, являющийся участником группы, отправляет пакет отчета. Если хост хочет присоединиться к группе, он активно отправляет IGMP Report опрашивающему для вступления в интересующую многоадресную группу.

2. Механизм подавления отчетов (Member Suppression)

При получении Query-пакета хост запускает таймер задержки ответа со случайным значением от 0 до максимального (D). Если таймер данного хоста истекает раньше, чем у других хостов в том же сегменте, он отправляет Membership Report. Получив такой отчет, остальные хосты отменяют свои таймеры и не отправляют отчеты. Этот процесс называется механизмом подавления отчетов.

3. Механизм выхода из группы (Leave mechanism)

Когда хост намеревается покинуть многоадресную группу, он отправляет пакет Leave Group с адресом назначения 224.0.0.2.

- Group-Specific Query (запрос, специфичный для группы)

После получения Leave Group опрашивающий отправляет запрос, адресованный конкретной группе, чтобы проверить, остался ли еще кто-либо из участников. Если опрашивающий получает отчеты от других участников, он продолжает поддерживать группу. В противном случае он прекращает пересылку данных в эту группу.

4. Параметры запросчика (Querier)

Query Interval – интервал между отправками General Query, по умолчанию 125 секунд.

Last Listener Query Interval – максимальное время ответа (Max Resp Time) в Group-Specific Query, то есть интервал ожидания ответа, по умолчанию 1 секунда.

Query Response Interval – максимальное время ответа (Max Resp Time) в General Query, по умолчанию 10 секунд. Хост, получивший General Query, должен ответить в течение этого интервала. Значение должно быть меньше Query Interval.

7.16.3 Настройка с помощью WEB-интерфейса

1. Настройте основные параметры IGMP, как показано ниже.

Рисунок 248 – Базовая конфигурация IGMP

VLAN Interface

Варианты настройки: созданные интерфейсы VLAN уровня 3

Version

Варианты настройки: V1/V2

По умолчанию: V2

Функция: выбор версии IGMP для запуска на данном интерфейсе.

Query-Interval (sec)

Диапазон: 1–65535 с

По умолчанию: 125 с

Функция: настройка интервала отправки пакета запроса IGMP-запросчиком.

Query Timeout (sec)

Диапазон: 60–300 с

По умолчанию: 265 с

Функция: настройка времени ожидания пакетов запроса IGMP для интерфейса.

Описание: если не-опрашивающее устройство не может получить пакет Query от запросчика в течение настроенного интервала, интерфейс на нем автоматически становится запрашивающим. Этот интервал называется временем ожидания, или тайм-аутом. В общем случае время ожидания в два раза больше интервала запроса плюс максимальное время ответа.

Max Query Response Time (sec)

Диапазон: 1–25 с

По умолчанию: 10 с

Функция: настройка максимального времени, в течение которого интерфейс должен ответить на запросы IGMP.

Описание: когда хост желает присоединиться к многоадресной группе, он должен отправить пакет Membership Report в ответ на Query-пакет от запросчика не позднее, чем через заданное максимальное время ответа. Это время определяет максимальный интервал ожидания ответа на запрос. Если хост не успевает отправить отчет в течение этого времени, опрашивающий считает, что в соответствующем сегменте сети отсутствуют участники данной многоадресной группы, и может выполнить отсечение (pruning) этого сегмента, прекратив пересылку трафика для группы по данному ответвлению.

3. Настройте статическую группу IGMP, как показано ниже.

Рисунок 249 – Настройка статической группы IGMP

Vlan ID

Варианты настройки: созданные интерфейсы VLAN уровня 3

По умолчанию: Vlan1

Функция: выбор интерфейса уровня 3 для настройки.

Group Address

Формат: A.B.C.D

Функция: указывает IP-адрес группы многоадресной рассылки, к которой необходимо статически добавить интерфейс уровня 3 коммутатора. Подразумевает, что интерфейс уровня 3 коммутатора заранее задан для конкретной многоадресной группы, и эта связь является фиксированной.

4. Настройте группу присоединения IGMP, как показано ниже.

Рисунок 250 – Настройка группы присоединения IGMP

Vlan ID

Варианты настройки: созданные интерфейсы VLAN уровня 3

По умолчанию: Vlan1

Функция: выбор интерфейса уровня 3 для настройки.

Group Address

Формат: A.B.C.D

Функция: указывает IP-адрес многоадресной группы, к которой коммутатор должен быть добавлен, и добавляет интерфейс уровня 3 коммутатора в многоадресную группу с этим адресом. По умолчанию для многоадресной группы не определен ни один участник. Эта настройка позволяет динамически добавлять интерфейс уровня 3 коммутатора в многоадресную группу, что означает, что участники могут изменяться в зависимости от состояния сети.

5. Удалите группу IGMP, как показано ниже.

Рисунок 251 – Удаление IGMP-группы

Clear Type

Варианты настройки: By Interface / By Group Address

По умолчанию: By Interface

Функция: настройка метода очистки информации о динамической группе IGMP на основе интерфейса или группового адреса.

Vlan Interface

Варианты настройки: созданные интерфейсы VLAN уровня 3

По умолчанию: не задано

Функция: настройка интерфейса VLAN для очистки информации о динамической группе IGMP.

Group Address

Формат: A.B.C.D

Функция: адрес группы IGMP, которую необходимо удалить.

6. Ниже показано отображение информации об интерфейсах IGMP.

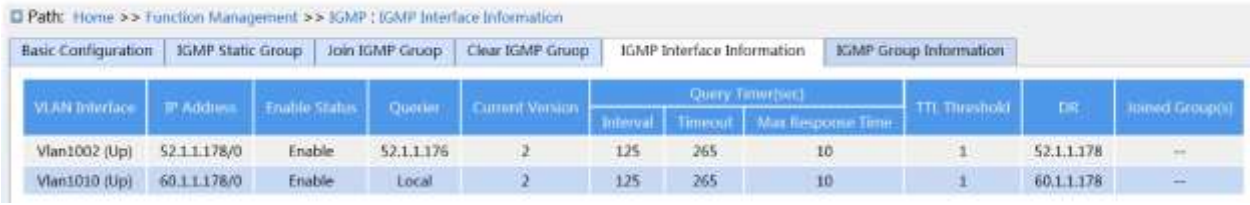


Рисунок 252 – Информация об интерфейсах IGMP

Поля отображаемой информации описаны в следующей таблице.

Таблица 17 – Информация об интерфейсе IGMP

Параметр	Описание
VLAN Interface	L3-интерфейс VLAN, на котором включен IGMP и который находится в активном состоянии
IP Address	IP-адрес, назначенный этому VLAN-интерфейсу
Enable Status	Статус включения IGMP на данном VLAN-интерфейсе (включен или выключен)
Querier	IP-адрес устройства, выполняющего функцию запросчика. Формат – «A.B.C.D». Если указано «Local» – значит, этот коммутатор сам является IGMP-запросчиком на данной VLAN
Current Version	Версия протокола IGMP, используемая на данном интерфейсе VLAN
Query Timer(s)-Interval	Интервал между отправками IGMP-запросов (Query) на данном интерфейсе VLAN (в секундах)
Query Timer(s)-Timeout	Время ожидания ответа на IGMP-запрос на данном интерфейсе VLAN, после которого считается, что участник группы отсутствует
Query Timer(s)-Max Response Time	Максимальное время, в течение которого клиенты должны ответить на IGMP-запрос
TTL Threshold	Порог TTL (Time To Live) для IGMP-сообщений на этом интерфейсе VLAN. Пакеты с TTL меньше этого значения игнорируются
DR	IP-адрес назначенного маршрутизатора (DR) для данного VLAN. DR отвечает за маршрутизацию многоадресного трафика
Joined Group(s)	Список многоадресных групп, на которые подписан данный VLAN-интерфейс

6. Ниже показано отображение информации о группах IGMP.

Рисунок 253 – Информация о группах IGMP

Поля отображаемой информации описаны в следующей таблице.

Таблица 18 – Информация о группах IGMP

Параметр	Описание
VLAN Interface	L-3 интерфейс VLAN коммутатора, через который осуществляется доступ к соответствующей многоадресной группе. Т.е. интерфейс VLAN, на котором зарегистрирована эта группа
Group Address	IP-адрес многоадресной группы
Uptime	Время, в течение которого данная многоадресная группа активна на данном VLAN-интерфейсе. Отображается в формате «часы:минуты:секунды»
Expires	Время, оставшееся до истечения таймера группы (т.е. до того момента, когда группа будет удалена, если не поступят новые сообщения от участников). Формат – «часы:минуты:секунды». Если указано «stopped», значит таймер не работает, и группа не будет автоматически удалена
Last Reporter	IP-адрес последнего хоста (участника), который присоединился к многоадресной группе или отправлял IGMP-сообщения для этой группы. Это последний известный источник информации о членстве в группе

7.17 Настройка маршрутизации

Чтобы получить доступ к удаленному узлу в Интернете, хост должен выбрать соответствующий маршрут с помощью маршрутизаторов или коммутаторов 3-го уровня. В процессе выбора пути каждый коммутатор 3-го уровня выбирает путь к следующему коммутатору 3-го уровня в соответствии с адресом получателя пакета до тех пор, пока последний коммутатор не отправит пакет узлу-получателю. Путь, который выбирает каждый коммутатор 3-го уровня, называется маршрутом. Маршруты делятся на следующие типы:

Прямой – маршрут, обнаруженный протоколом канального уровня.

Статический – маршрут, настроенный сетевым администратором вручную.

Динамический – маршрут, обнаруженный протоколом маршрутизации.

В данной серии коммутаторов протоколы маршрутизации поддерживают модели SEWM3GX28P.

7.17.1 Статическая маршрутизация

7.17.1.1 Введение

Статические маршруты настраиваются вручную. Если топология сети достаточно проста, вам нужно всего лишь настроить статические маршруты для сети, чтобы она работала соответствующим образом. Статические маршруты просты в настройке и стабильны. Они могут быть использованы для достижения балансировки нагрузки и резервирования маршрутов, предотвращая неправомерные изменения маршрута. Недостатком использования статических маршрутов является то, что они не могут приспособиться к изменениям сетевой топологии. Если в сети появится неисправность или произойдет изменение топологии, соответствующие маршруты будет недоступны, что приведет к прерываниям передачи данных. Когда это происходит, сетевой администратор должен изменить статические маршруты вручную.

7.17.1.2 Таблица маршрутизации

Каждый коммутатор 3-го уровня содержит таблицу маршрутизации, где прописаны все маршруты, которые используются маршрутизатором. Каждая запись в таблице определяет, какой из пакетов VLAN, предназначенный для определенной подсети или хоста, должен быть отправлен к следующему маршрутизатору или напрямую подключенному к маршрутизатору адресату.

Запись маршрута включает в себя следующие пункты:

Назначение (Destination Network): указывает IP адрес получателя или сети.

Маска подсети (Subnet Mask): определяет, какая часть IP-адреса коммутатора 3-го уровня относится к адресу сети, а какая к адресу самого узла в этой сети. Логическая операция AND между адресом назначения и маской подсети дает адрес сети назначения. Например, если адрес получателя 129.102.8.10 и маска 255.255.0.0, адрес сети назначения будет 129.102.0.0. Маска подсети состоит из определенного числа последовательных битов. Это значение может быть выражено как десятичном формате, так и количеством битов.

Выход (Out Interface): определяет порт, через который соответствующий пакет IP должен быть отправлен.

IP адрес следующего коммутатора 3-го уровня (Next Hop): указывает новый маршрутизатор, через который будет пропущен пакет IP.

Приоритет: маршруты для одной и той же точки назначения, но имеющие различные следующие хопы, могут иметь разный уровень приоритета и определяются различными

протоколами маршрутизации или конфигурируются вручную. Оптимальным маршрутом является маршрут с наивысшим приоритетом.

7.17.1.3 Маршрут по умолчанию

Для ограничения слишком большого количества записей в таблице маршрутизации, вы можете настроить маршрут по умолчанию. Маршрут по умолчанию является статическим маршрутом. Если пакету данных не удается найти соответствие в таблице маршрутизации, он передается в согласно маршруту по умолчанию. В таблице маршрутизации маршрутом по умолчанию является маршрут с адресом назначения и маской 0.0.0.0. Если пакет не соответствует ни одной записи в таблице маршрутизации и маршрут по умолчанию не настроен, маршрутизатор отбрасывает пакет и возвращает пакет ICMP с информацией о том, что адрес назначения или сеть недостижимы.

7.17.1.4 Настройка с помощью WEB-интерфейса

1. Ниже показана настройка статической маршрутизации.

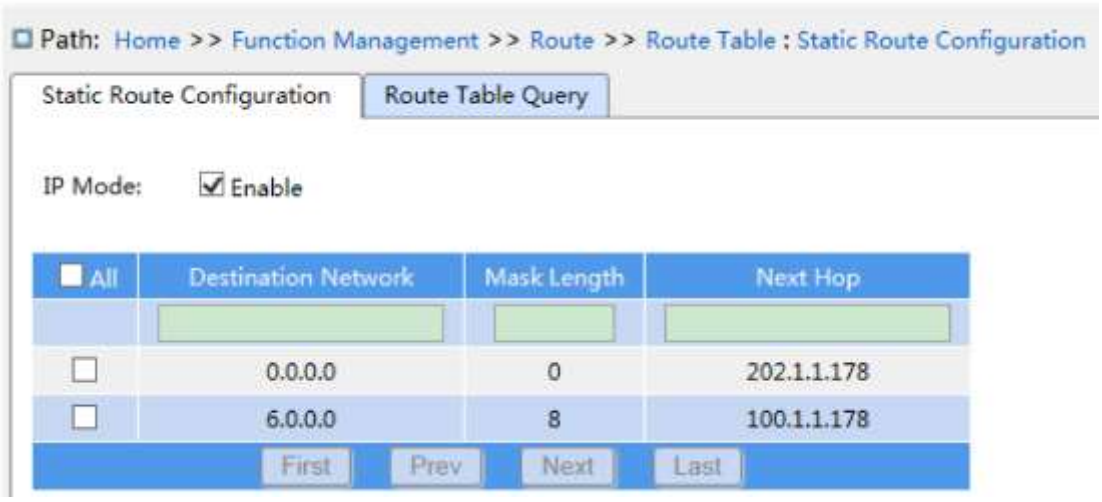


Рисунок 254 – Настройка статической маршрутизации

IP Mode

Варианты настройки: включено/выключено

По умолчанию: для устройств уровня 3 по умолчанию включено. Для устройств уровня 2 по умолчанию выключено.

Функция: включение/отключение IP-режима.

Destination Network

Формат конфигурации: A.B.C.D

Функция: указывает целевой сетевой адрес в таблице статической маршрутизации.

Mask Length

Функция: маска подсети – это 32-битное число, состоящее из последовательности единиц и нулей. Единицы обозначают часть адреса, отвечающую за номер сети и подсети, а нули – часть, выделенную под номера хостов. Длина маски – это количество единиц в ней.

Next Hop

Формат конфигурации: A.B.C.D

Функция: настройка IP-адреса следующего перехода.

2. Запрос таблицы маршрутизации. Просмотрите информацию таблицы маршрутизации устройства, включая статические и динамические маршруты, как показано ниже.

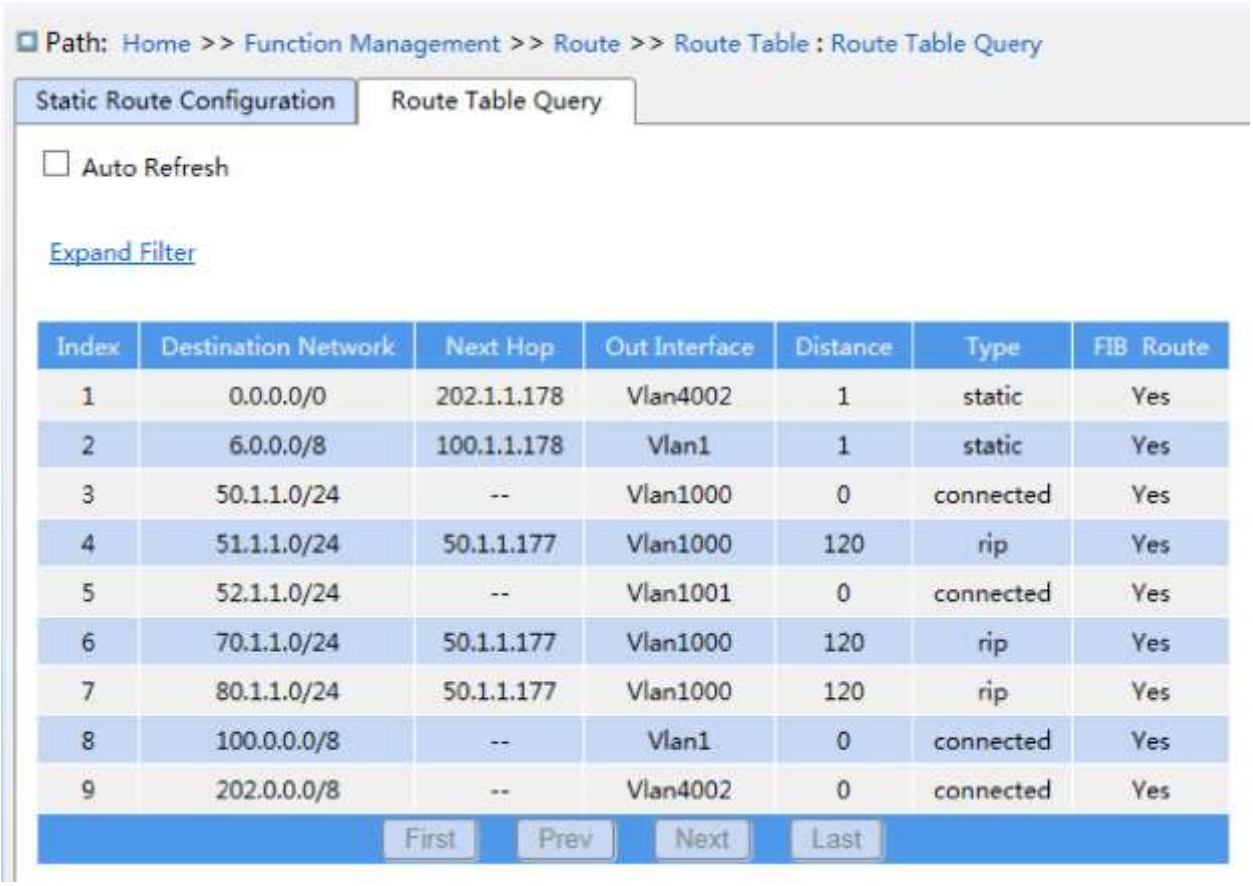


Рисунок 255 – Таблица маршрутизации

7.17.1.5 Пример типовой настройки

Как показано на рисунке 256, маска подсети всех коммутаторов 3-го уровня и компьютеров в сети – 255.255.255.0. Требуется настроить статические маршруты, чтобы любые из хостов могли общаться друг с другом.

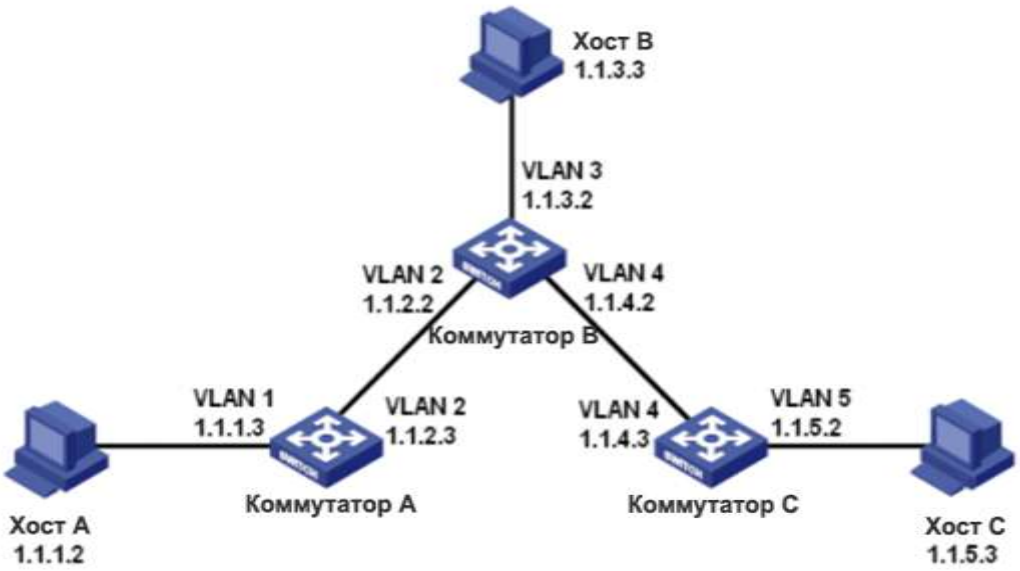


Рисунок 256 – Пример для настройки статических маршрутов

Настройка коммутатора A:

1. Задайте IP-адреса для интерфейсов VLAN.
2. Настройте статический маршрут со следующими параметрами:

IP-адрес назначения: 1.1.3.0; маска сети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.2.2; приоритет: 1, как показано на рисунке 254.

IP-адрес назначения: 1.1.5.0; маска сети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.2.2; приоритет: 1, как показано на рисунке 254.

Настройка коммутатора B:

3. Задайте IP-адреса для интерфейсов VLAN.
4. Настройте статический маршрут со следующими параметрами:

IP-адрес назначения: 1.1.1.0; маска сети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.2.3; приоритет: 1, как показано на рисунке 254.

IP-адрес назначения: 1.1.5.0; маска сети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.4.3; приоритет: 1, как показано на рисунке 254.

Настройка коммутатора C:

5. Задайте IP-адреса для интерфейсов VLAN.
6. Настройте статический маршрут со следующими параметрами:

IP-адрес назначения: 0.0.0.0; маска сети назначения: 0.0.0.0; шлюз по умолчанию: 1.1.4.2; приоритет: 1, как показано на рисунке 254.

7. Настройте шлюзы по умолчанию для хоста A, хоста B и хоста C как 1.1.1.3, 1.1.3.2 и 1.1.5.2 соответственно.

7.17.2 RIP

7.17.2.1 Введение

Понятие «маршрутизаторы» в этой главе относится к коммутаторам третьего уровня.

RIP (Routing Information Protocol) – это внутренний протокол маршрутизации дистанционно-векторного типа, использующий пакеты UDP для обмена информацией через порт 520. Каждый коммутатор 3-го уровня, на котором работает RIP, имеет базу данных маршрутизации. База данных содержит записи маршрутизации ко всем доступным пунктам назначения этого коммутатора, на основе которых создается таблица маршрутизации. Когда коммутатор 3-го уровня, использующий RIP, отправляет пакет обновления маршрута своим соседним устройствам, этот пакет содержит всю таблицу маршрутизации, установленную коммутатором на основе базы данных маршрутизации. Следовательно, в крупномасштабной сети каждый коммутатор 3-го уровня должен передавать и обрабатывать большой объем данных маршрутизации, что снижает общую производительность сети. RIP позволяет вносить в таблицу информацию, обнаруженную другими протоколами маршрутизации.

RIP имеет две версии: RIP-1 и RIP-2. RIP-1 использует для сообщений только широковещательную рассылку, не поддерживает маску подсети и аутентификацию. Некоторые поля в сообщении RIP-1 должны быть заполнены нулями. Эти поля называются нулевыми, их следует проверять при получении сообщения RIP-1. Если такое поле содержит ненулевое значение, сообщение RIP-1 не будет обработано. RIP-2 – усовершенствованная версия на основе RIP-1. В RIP-2 пакеты протокола отправляются в многоадресном режиме, а адрес назначения – 224.0.0.9. Кроме того, в RIP-2 добавлены домен маски подсети и домен проверки RIP (поддерживается простой текстовый пароль и проверка пароля MD5), а также поддерживаются маски подсети переменной длины (VLSM). RIP-2 сохраняет часть нулевых доменов в RIP-1, и поэтому нет необходимости проверять все нулевые домены. По умолчанию коммутатор 3-го уровня передает сообщение RIP-2 в многоадресном режиме, а принимает сообщения RIP-1 и RIP-2.

Для измерения расстояния до пункта назначения RIP использует количество переходов (хопов). Количество хопов от маршрутизатора к сети с прямым подключением равно 0. Количество переходов от маршрутизатора к маршрутизатору с прямым подключением равно 1. Чтобы ограничить время конвергенции, диапазон значений метрики RIP составляет от 0 до 15. Значение метрики 16 и более считается бесконечным, и это означает, что сеть назначения недоступна. Именно поэтому RIP подходит только для сетей небольшого размера.

7.17.2.2 Предотвращение петель маршрутизации

В сети с протоколом RIP, когда маршрут RIP становится недоступным, коммутатор 3-го уровня не будет отправлять пакет обновления маршрута немедленно, пока не истечет интервал обновления маршрута (30 с). Если соседний коммутатор отправляет пакет, содержащий информацию о его собственной таблице маршрутизации до того, как будет получен пакет обновления маршрута, произойдет бесконечный подсчет. То есть, метрика для выбора маршрута к недостижимому коммутатору 3-го уровня постепенно увеличивается. Это заметно влияет на время маршрутизации и время агрегации маршрутов.
Чтобы избежать бесконечного подсчета и образования циклического маршрута (петли), RIP предоставляет механизмы расщепления горизонта и триггерного обновления. Расщепление горизонта (split horizon) направлено на то, чтобы избежать отправки маршрутов на шлюз, из которого они были получены. Технология включает в себя простое расщепление горизонта и расщепление горизонта с «отравлением» обратного маршрута (poisoned reverse). Простое расщепление горизонта удаляет маршруты, которые должны быть отправлены на соседний шлюз, от которого эти маршруты были получены. Расщепление горизонта с отравлением обратного маршрута удаляет предыдущие маршруты из пакета обновления и устанавливает метрики этих маршрутов на 16. В механизме триггерного обновления всякий раз, когда шлюз изменяет метрику маршрута, пакет обновления маршрута будет передан немедленно, без учета состояния 30-секундного таймера обновления.

7.17.2.3 Принцип работы

1. После включения RIP маршрутизатор отправляет сообщения-запросы соседним маршрутизаторам. Соседние маршрутизаторы возвращают ответные сообщения, включая информацию о своих таблицах маршрутизации.

2. Получив такую информацию, маршрутизатор обновляет свою локальную таблицу маршрутизации и отправляет триггерные сообщения об обновлении соседним узлам. Все маршрутизаторы в сети делают то же самое, чтобы сохранить самую последнюю информацию о маршрутизации.

3. По умолчанию локальная таблица маршрутизации будет отправляться на соседние маршрутизаторы с интервалом в 30 секунд. После получения пакета, содержащего эту таблицу маршрутизации, соседние маршрутизаторы, использующие протокол RIP, будут поддерживать свои собственные локальные маршруты, выбирать оптимальный маршрут и отправлять сообщение об обновлении своим соответствующим соседним узлам, чтобы обновленный маршрут стал глобальным. Кроме того, RIP использует механизм истечения срока действия для обработки устаревших маршрутов. В частности, если коммутатор 3-го уровня не получает информацию об обновлении маршрута от соседнего коммутатора в течение указанного интервала времени (значение invalid timer), все маршруты от этого соседа будут считаться недопустимыми и перейдут в состояние подавления. Такие маршруты имеют срок действия (значение таймера удержания) в таблице маршрутизации. Если в течение этого периода от соседнего узла не будет получена информация об обновлении, эти маршруты удаляются из таблицы маршрутизации.

7.17.2.4 Настройка с помощью WEB-интерфейса

1. Ниже показана базовая настройка RIP.

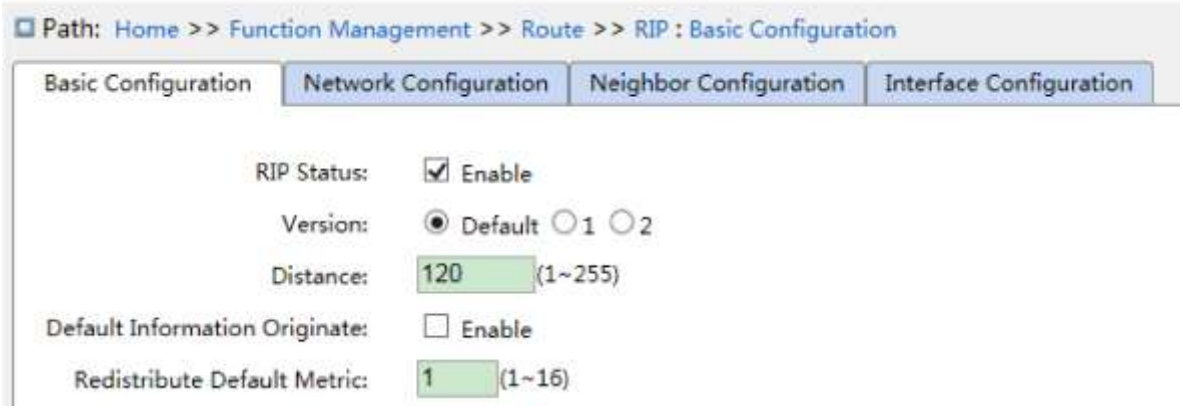


Рисунок 257 – Базовая конфигурация RIP

RIP Status

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение RIP.

Version

Варианты настройки: Default/1/2

По умолчанию: Default

Функция: выбор версии протокола RIP. По умолчанию отправляется RIP-2 и принимаются RIP-1 и RIP-2. Конфигурация 1 указывает, что все интерфейсы коммутатора 3-го уровня отправляют и принимают пакеты RIP-1. Конфигурация 2 указывает, что все интерфейсы отправляют и принимают пакеты RIP-2.

Distance

Диапазон: 1–255

По умолчанию: 120

Функция: определяет предпочтение маршрутов, получаемых с помощью протокола RIP. Чем меньше значение, тем выше приоритет маршрута. Это значение влияет на выбор маршрутов в таблице маршрутизации, где более низкие значения указывают на более предпочтительные маршруты.

Default Information Originate

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включает или отключает широковещательную рассылку маршрута по умолчанию.

Redistribute Default Metric

Диапазон: 1–16

По умолчанию: 1

Функция: используется для настройки метрики по умолчанию при импорте внешних маршрутов в протокол RIP. Когда маршруты из других протоколов маршрутизации (например, OSPF) перераспределяются в RIP, им присваивается метрика, определяемая этим параметром.

2. Ниже показана настройка перераспределения маршрутов.

Redistribute		
Protocol	Enable	Metric
Connected	☐	(1~16)
Static	☐	(1~16)
OSPF	☐	(1~16)

Рисунок 258 – Настройка перераспределения маршрутов

Protocol

Варианты настройки: Connected/Static/OSPF

Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: маршруты, сгенерированные другими протоколами, перераспределяются в RIP. Импортировать можно только маршруты с активным статусом.

Metric

Диапазон: 1–16

По умолчанию: не задано

Функция: настройка метрики импортируемого маршрута. Этот параметр не является обязательным. Если он не настроен, метрика перераспределенного маршрута будет назначена согласно конфигурации «Redistribute Default Metric» (см. пункт 1).

3. Ниже показана настройка временных параметров.

Timer		
Routing Table Update	30	(5~86400Second(s))
Routing Information Timeout	180	(5~86400Second(s))
Garbage Collection	120	(5~86400Second(s))

Рисунок 259 – Таймеры RIP

Routing Table Update

Диапазон: 5–2147483647 с

По умолчанию: 30 с

Функция: настройка интервала, с которым RIP отправляет пакеты обновления.

Routing Information Timeout

Диапазон: 5–2147483647 с

По умолчанию: 180 с

Функция: настройка периода времени ожидания маршрута RIP. Если в течение этого периода от соседа не получено никакой информации об обновлении таблицы маршрутизации, все маршруты с устройства считаются недействительными, и маршрут переходит в состояние подавления. Время, установленное для этого параметра должно быть больше времени обновления информации о маршрутах.

Garbage Collection

Диапазон: 5–2147483647 с

По умолчанию: 120 с

Функция: настройка времени нахождения маршрута RIP в состоянии подавления. Если устройство не получает информацию об обновлении, такие маршруты удаляются из таблицы маршрутизации. Время, установленное для этого параметра должно быть больше времени обновления информации о маршрутах.

4. Ниже показаны сетевые настройки RIP.

Рисунок 260 – Сетевые настройки

IP Address

Формат конфигурации: A.B.C.D

Функция: объявление о запуске протокола RIP в сегменте сети.

Mask

Формат конфигурации: A.B.C.D

Функция: маска подсети – это 32-битное число, состоящее из последовательности единиц и нулей. Единицы обозначают часть адреса, отвечающую за номер сети и подсети, а нули – часть, выделенную под номера хостов. Длина маски – это количество единиц в ней.

5. Ниже показана настройка информации о соседних устройствах.

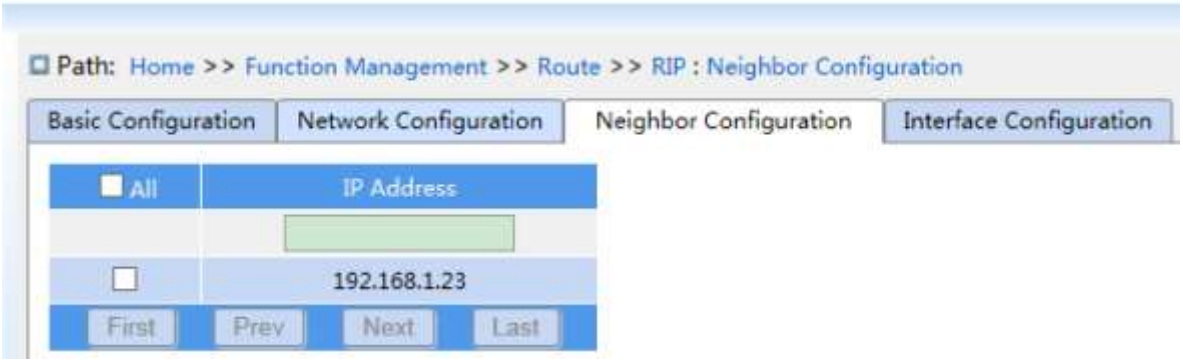


Рисунок 261 – Информация о соседних устройствах

IP Address

Формат конфигурации: A.B.C.D

Функция: IP-адрес соседнего устройства.

6. Ниже показана настройка RIP на интерфейсах.

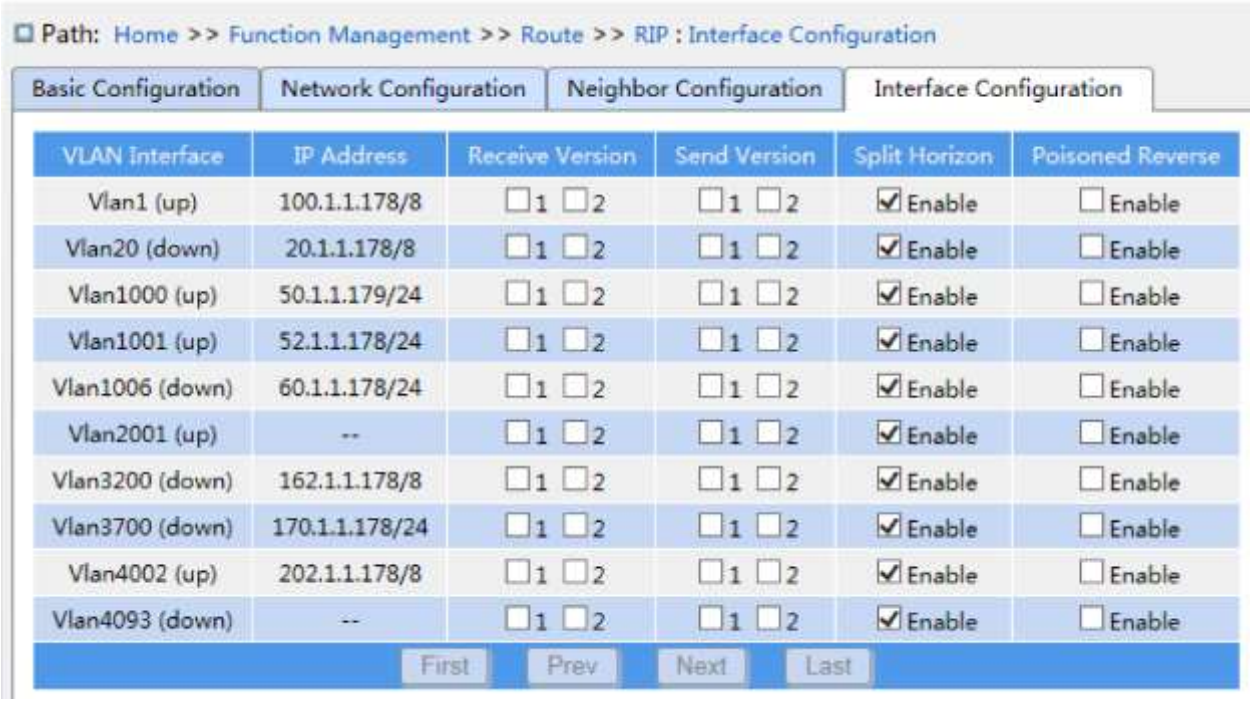


Рисунок 262 – Интерфейсы RIP

VLAN Interface

Варианты настройки: все интерфейсы VLAN на коммутаторе

IP address

Формат конфигурации: A.B.C.D

Функция: IP-адрес интерфейса

Receive Version

Варианты настройки: 1/2

По умолчанию: не задано

Функция: настройка интерфейса для получения пакетов RIP указанной версии. «1» означает прием сообщений RIP-1; «2» означает прием сообщений RIP-2. Если ни одного значения не выбрано, по умолчанию принимаются сообщения RIP-1 и RIP-2.

Send Version

Варианты настройки: 1/2

По умолчанию: нет

Функция: настройка интерфейса для отправки пакетов RIP указанной версии. «1» означает отправку сообщений RIP-1; «2» означает отправку сообщений RIP-2. Если ни одного значения не выбрано, по умолчанию отправляются сообщения RIP-2.

Split Horizon

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение или отключение расщепления горизонта. Этот механизм запрещает интерфейсу отправлять обратно маршруты, которые были получены с этого же интерфейса. Например, если коммутатор получил маршрут через интерфейс Vlan20, он не будет отправлять этот маршрут обратно через тот же интерфейс.

Poisoned Reverse

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение или отключение отравления обратного маршрута. При включении, если интерфейс получил маршрут через соседний интерфейс, он отправляет обратно этот же маршрут с метрикой 16 (что означает «недостижимый» в RIP), чтобы сообщить соседу, что этот маршрут больше не действителен через данный интерфейс. Это дополнительный механизм для предотвращения петель маршрутизации

7.17.2.5 Пример типовой настройки

Как показано на рисунке 215, коммутатор B подключен к коммутатору A через интерфейс VLAN 2 и к коммутатору C через интерфейс VLAN 4. Все три коммутатора работают по протоколу маршрутизации RIP. Маска подсети у всех коммутаторов — 255.255.255.0.

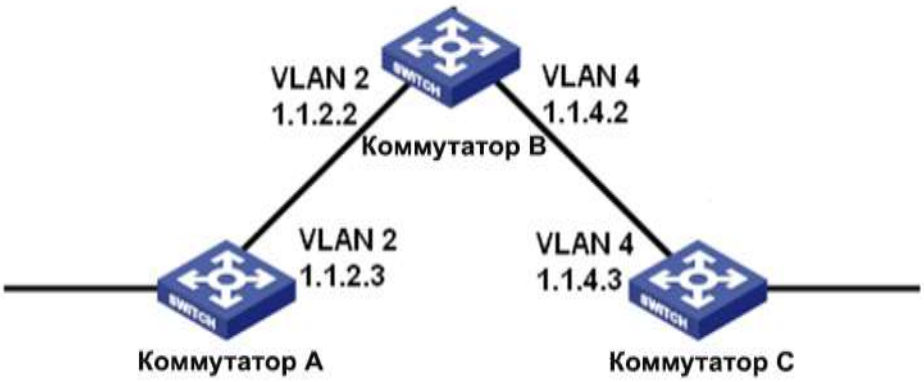


Рисунок 263 – Пример конфигурации RIP

Настройка коммутатора A:

1. Установите IP-адрес для интерфейса VLAN 2.
2. Включите протокол RIP, как показано на рисунке 257.
3. Настройте интерфейс VLAN 2 для передачи/приема сообщения RIP, как показано на рисунке 262.

Настройка коммутатора B:

1. Установите IP-адреса для интерфейсов VLAN 2 и VLAN 4.
2. Включите протокол RIP, как показано на рисунке 257.
3. Настройте интерфейсы VLAN 2 и VLAN 4 для передачи/приема сообщения RIP, как показано на рисунке 262.

Настройка коммутатора C:

1. Установите IP-адрес для интерфейса VLAN 4.
2. Включите протокол RIP, как показано на рисунке 257.
3. Настройте интерфейс VLAN 4 для передачи/приема сообщения RIP, как показано на рисунке 262.

7.17.3 OSPF

7.17.3.1 Введение

OSPF (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала. Коммутаторы 3-го уровня обмениваются информацией о состоянии канала с базой данных LSDB (Link State Database), содержащей список всех записей о состоянии каналов. Затем каждый из коммутаторов использует

алгоритм SPF (Shortest Path First), базирующийся на LSDB, для генерации таблицы маршрутизации. Данная серия коммутаторов поддерживает OSPF версии 2.

Понятие «маршрутизаторы» в этой главе относится к коммутаторам третьего уровня.

7.17.3.2 Основные понятия

1. AS (автономная система)

Автономная система (AS) включает в себя группу маршрутизаторов, которые работают, используя один и тот же протокол маршрутизации.

2. Router ID (идентификатор маршрутизатора)

ID маршрутизатора (RID): маршрутизатор с включенным протоколом OSPF должен иметь свой собственный ID, который является уникальным идентификатором маршрутизатора в AS. При этом RID может быть настроен как вручную, так и автоматически. Автоматически созданным RID является основной IP-адрес порта VLAN с самым маленьким ID на коммутаторе.

3. Пакеты OSPF

- Hello: периодическая отправка к соседним узлам пакета, содержащего значения некоторых таймеров, а также информацию о выделенном маршрутизаторе (DR), резервном выделенном маршрутизаторе (BDR) и известных соседних узлах.
- Database description (DD): показывает справочную информацию о всех LSA (Link State Advertisement) в LSDB, передаваемых между двумя маршрутизаторами для синхронизации данных.
- Link state request (LSR): после обмена пакетами DD, два маршрутизатора знают, какие LSA соседних узлов исчезли из их LSDB. Затем они передают пакет LSR друг другу с запросом о потерянных LSA.
- Link state update (LSU): в ответ на LSR пакеты отправляются LSU-пакеты, которые содержат полные описания недостающих LSA.
- Link state acknowledgment (LSAck): подтверждает принятые пакеты LSU. Содержит заголовки принятых пакетов LSA (один пакет LSAck может подтвердить несколько пакетов LSA).

4. Соседние и смежные узлы

- Соседний узел – это маршрутизатор, который установил связь с другим маршрутизатором OSPF. Когда маршрутизатор OSPF запускается, он отправляет пакет Hello через интерфейс, на котором включен протокол OSPF. При получении пакета Hello другой маршрутизатор проверяет параметры, содержащиеся в пакете (например, идентификаторы маршрутизаторов, параметры сети и т.д.). Если параметры совпадают и соответствуют критериям соседства, маршрутизаторы становятся соседними.

Соседние узлы могут обмениваться информацией о маршрутах и о состоянии интерфейсов.

- Смежный узел – это специальный тип соседнего узла, который участвует в процессе обмена информацией о маршрутах и синхронизации баз данных маршрутов (LSDB). Два соседних маршрутизатора могут установить смежные отношения только после успешного обмена пакетами Hello и подтверждения их параметров. Смежные узлы обмениваются сообщениями LSA для обновления и синхронизации своих баз данных. Без этого обмена информацией о состоянии сети соседние узлы не могут установить полноценные смежные отношения.

Таким образом, различие между соседними и смежными узлами в OSPF заключается в том, что все смежные узлы являются соседними, но не все соседние узлы являются смежными. Смежность подразумевает активный обмен информацией о маршрутах и синхронизацию баз данных, в то время как соседство может быть установлено на основании обмена пакетами Hello.

5. Типы LSA

LSA (Link State Advertisement) – это сообщения, с помощью которых маршрутизаторы OSPF обмениваются информацией о топологии сети. LSA распространяются по области с помощью механизма flooding и хранятся в базе данных LSDB. На основе LSDB маршрутизаторы вычисляют кратчайшие пути с помощью алгоритма SPF.

- Router LSA (Type 1): генерируется каждым маршрутизатором внутри своей области. Он описывает состояние интерфейсов маршрутизатора, его связи с соседними маршрутизаторами в пределах этой области и стоимость.
- Network LSA (Type 2): генерируется выделенным маршрутизатором DR на многодоступном сегменте (например, Ethernet). Содержит информацию о всех маршрутизаторах, подключенных к этому сегменту внутри области. Не распространяется за пределы области.
- Summary LSA (Type 3): генерируется на граничном маршрутизаторе ABR для объявления маршрутов из одной области в другую. Распространяется в смежные области, описывает подсети внутри области, известные ABR.
- ASBR Summary LSA (Type 4): генерируется на граничном маршрутизаторе ABR для указания маршрутов к граничному маршрутизатору автономной системы ASBR внутри области. Распространяется в смежных зонах, помогая другим областям узнать, как добраться до ASBR.
- AS External LSA (Type 5): генерируется на ASBR для объявления маршрутов к внешним сетям вне автономной системы OSPF. Распространяется по всей AS, кроме stub и NSSA областей
- NSSA External LSA (Type 7): используется для распространения внешних маршрутов, но только внутри области типа NSSA. Создается внутри NSSA маршрутизаторами, которые хотят объявить внешние маршруты.

7.17.3.3 Область и маршрутизатор

1. Разделение областей.

OSPF делит AS на несколько зон, или областей, которые идентифицируются посредством ID. Области классифицируют маршрутизаторы в сети по нескольким логическим группам, как показано на рисунке 264. Между областями OSPF обмен происходит не полными маршрутами, а сводной информацией о маршрутах, которая позволяет эффективно и масштабируемо распространять данные о доступных сетях между областями.

Область 0, известная как магистральная область, является центральной областью сети OSPF. Все остальные области (немагистральные) должны быть подключены к ней напрямую или через виртуальные каналы. Магистральная область отвечает за пересылку маршрутной информации между немагистральными областями, выступая в качестве транзитной зоны для межобластной маршрутизации.

Для уменьшения размера базы данных топологии LSDB в OSPF области могут быть сконфигурированы как тупиковые (stub-области). В таких областях запрещен вход LSA типов 4 (ASBR Summary) и 5 (External). Для обеспечения доступности маршрутов в другие области автономной системы или в другие автономные системы, граничный маршрутизатор области (ABR) формирует и распространяет среди маршрутизаторов stub-области маршрут по умолчанию (0.0.0.0/0). Также может быть настроена область NSSA, отличающаяся от stub тем, что позволяет ограниченно распространять внешние маршруты через LSA 7-го типа.

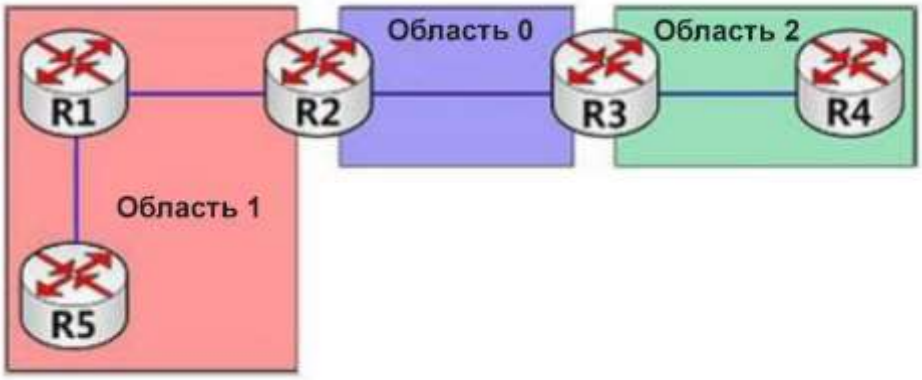


Рисунок 264 – Разделение областей

Принадлежность маршрутизатора к области определяется конфигурацией его интерфейсов. Маршрутизатор с несколькими интерфейсами может одновременно принадлежать к нескольким областям, однако каждый интерфейс может быть назначен только одной области.

Все маршрутизаторы в одной области поддерживают общую базу LSDB, отражающую топологию данной области. Маршрутизатор, принадлежащий к нескольким областям, хранит отдельную LSDB для каждой области. Деление сети на области дает следующие преимущества:

- Маршрутизаторы каждой области хранят только LSDB своей области, а не всей OSPF-сети целиком, что снижает требования к памяти и нагрузку на процессор.

- Изменения топологии, ограниченные одной областью, не влияют на всю сеть OSPF и не вызывают перерасчета SPF во всех областях, что уменьшает частоту вычислений маршрутов.
- Ограничение распространения LSA в пределах области снижает объем передаваемой информации и нагрузку на сеть.

2. Типы маршрутизаторов.

В зависимости от роли маршрутизатора в автономной системе он может быть внутренним маршрутизатором, ABR, маршрутизатором магистрали или ASBR, как показано на рисунке 265.

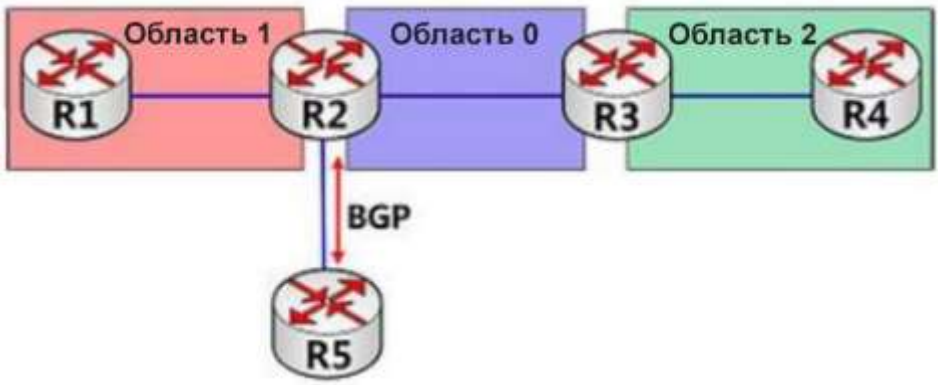


Рисунок 265 – Типы маршрутизаторов OSPF

- Внутренний маршрутизатор: все интерфейсы внутреннего маршрутизатора принадлежат одной OSPF-области и не могут соединять разные области.
- ABR: граничный маршрутизатор. Соединяет одну или несколько областей с магистральной областью (область 0). На ABR хотя бы один интерфейс должен принадлежать магистральной области.
- Маршрутизатор магистрали: хотя бы один интерфейс маршрутизатора магистрали должен находиться в магистральной области. Все ABR и внутренние маршрутизаторы в области 0 являются маршрутизаторами магистрали.
- ASBR: граничный маршрутизатор автономной системы, который обменивается маршрутной информацией с другой автономной системой и может использовать внешние маршруты.

Один маршрутизатор может выполнять несколько ролей одновременно. Например, R2 на рисунке 265 – это и магистральный маршрутизатор, и ABR, и ASBR.

3. Виртуальный канал.

Если немагистральные области, не могут подключиться к магистральной из-за определенных ограничений, логические связи между ними можно создать при помощи виртуальных каналов OSPF.

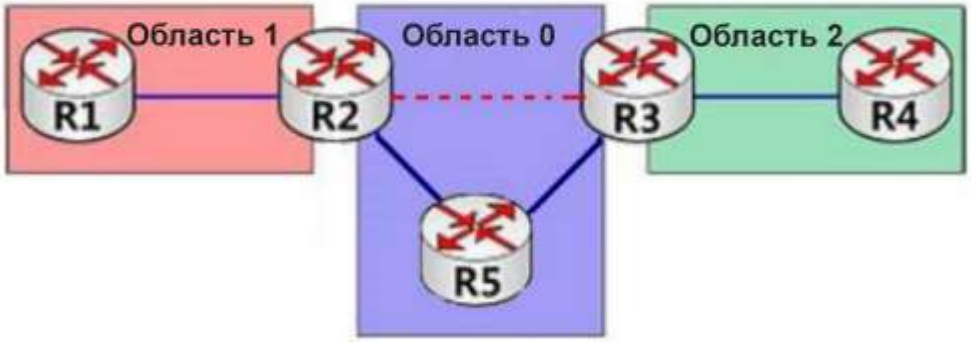


Рисунок 266 – Виртуальный канал

Виртуальный канал, настроенный на обоих маршрутизаторах ABR, представляет собой логическое соединение, которое устанавливается между двумя маршрутизаторами ABR через область, не являющуюся магистральной. Такая область называется транзитной зоной. Например, красная пунктирная линия на рисунке 266 – это виртуальный канал, а область 1 – транзитная зона для виртуального канала.

4. Типы маршрутов.

В OSPF маршруты классифицируются по четырем типам с различным уровнем предпочтительности (в порядке убывания приоритета):

- Внутриобластные маршруты (intra-area): маршруты к сетям, находящимся в той же OSPF-области, что и маршрутизатор. Они имеют наивысший приоритет и отражают топологию внутри одной области.
- Межобластные маршруты (inter-area): маршруты к сетям, расположенным в других областях той же автономной системы. Эти маршруты распространяются между областями через ABR.
- Внешние маршруты 1-го типа (E1): маршруты, импортированные из внешних автономных систем, для которых стоимость маршрута считается как сумма стоимости маршрута до ASBR и стоимости внешнего маршрута.
- Внешние маршруты 2-го типа (E2): маршруты, импортированные из внешних автономных систем, для которых стоимость маршрута определяется только стоимостью внешнего маршрута, а стоимость пути до ASBR не учитывается.

Таким образом, OSPF отдает предпочтение маршрутам внутри AS (внутриобластным и межобластным), а затем внешним маршрутам, при этом маршруты 1-го типа предпочтительнее маршрутов 2-го типа.

7.17.3.4 DR и BDR

В сетях NBMA любые два маршрутизаторы обмениваются маршрутной информацией друг с другом. В результате генерируется много ненужных пакетов LSA. Выделенный маршрутизатор (DR) был применен для решения именно этой проблемы. Все остальные маршрутизаторы устанавливают смежную связь и обмениваются информацией о маршрутизации с DR-маршрутизатором. DR извещает о состоянии каналов сети другие

маршрутизаторы. Для предотвращения одиночных, точечных отказов, вызванных неисправностью DR, OSPF определяет резервный выделенный маршрутизатор (BDR). BDR-маршрутизаторы также устанавливают смежную связь с другими маршрутизаторами. BDR является резервной копией DR. Когда DR неисправен, BRD начинает выполнять функции DR. Поскольку с другими маршрутизаторами были установлены смежные связи, отказ DR-маршрутизатора оказывает минимальное влияние на работу сети.

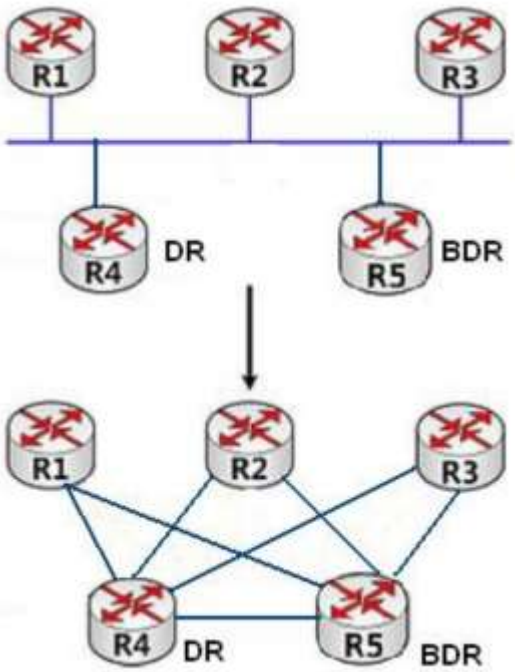


Рисунок 267 – DR и BDR.

Верхняя часть рисунка 267 показывает физические соединения Ethernet, а нижняя – установленные смежные отношения. После определения DR и BDR для пяти маршрутизаторов требуется только семь смежных связей.

Правила для выбора DR/BDR следующие:

- Маршрутизатор с приоритетом 0 не может стать DR или BDR.
- Маршрутизатор с наивысшим приоритетом сегмента сети становится DR, а маршрутизатор со вторым по значимости после наивысшего становится BDR.
- Если несколько маршрутизаторов имеют одинаковый приоритет, в качестве DR-маршрутизатора выбирается маршрутизатор с наибольшим RID.
- Когда происходит отказ DR-маршрутизатора, BDR-маршрутизатор берет на себя роль DR-маршрутизатора, при этом другой маршрутизатор будет выбран в качестве BDR.
- Понятия DR и BDR определяются для каждого сетевого сегмента. Выбор DR и BDR происходит отдельно для каждого сегмента на основе состояния интерфейсов и приоритетов маршрутизаторов, подключенных к этому сегменту. Таким образом, один и тот же маршрутизатор может быть DR на одном сетевом сегменте (интерфейсе), BDR на другом и обычным маршрутизатором на третьем.

- Если маршрутизатор с наивысшим приоритетом добавляется в сети после того, как DR/BDR уже выбраны, он не заменит существующие DR или BDR, чтобы стать новым DR или BDR.

7.17.3.5 Настройка с помощью WEB-интерфейса

1. Базовая конфигурация OSPF

Нажмите [Function Management] → [Route] → [OSPF] → [Basic Configuration], чтобы войти в интерфейс базовой конфигурации OSPF, как показано ниже.

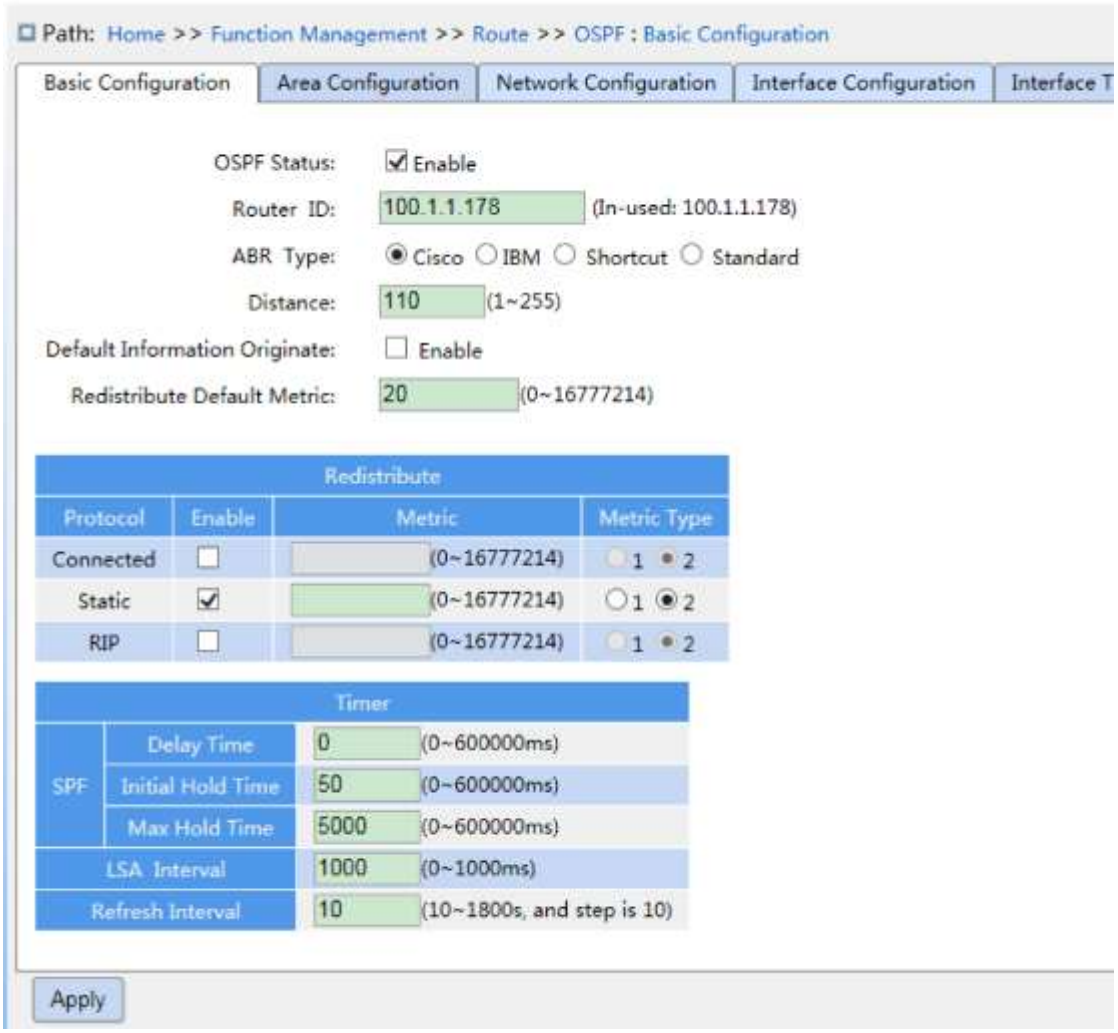


Рисунок 268 – Базовая конфигурация OSPF

OSPF Status

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение/отключение OSPF.

Router ID

Формат конфигурации: A.B.C.D

По умолчанию: наименьший из всех настроенных IP-адресов коммутатора.

Функция: настройка RID коммутатора OSPF. Каждый коммутатор, на котором работает OSPF, имеет уникальный идентификатор RID в AS.

Изменения RID вступают в силу только после перезапуска процесса OSPF.

Router ID (In-Used)

Функция: отображение текущего фактического RID.

ABR Type

Варианты настройки: Cisco/IBM/Shortcut/Standard

По умолчанию: Cisco

Функция: настройка типа ABR маршрутизатора.

Описание:

Cisco: необходимо настроить минимум две области, каждая из которых содержит хотя бы один интерфейс в активном состоянии. При этом одна из областей обязательно должна быть областью 0. Такой маршрутизатор считается ABR типа Cisco.

IBM: маршрутизатор считается ABR типа IBM, если настроено не менее двух областей, каждая с хотя бы одним активным интерфейсом. При этом область 0 должна быть настроена и может содержать интерфейс в любом состоянии (up или down). Кроме того, область 0 учитывается как одна из двух областей с активными интерфейсами.

Shortcut/Standard: для ABR типа Shortcut или Standard достаточно настроить не менее двух областей с хотя бы одним активным интерфейсом в каждой. При этом наличие области 0 не обязательно. Такой тип ABR рассматривается как стандартный или оптимизированный для кратчайшего пути.

Distance

Диапазон: 1–255

По умолчанию: 110

Функция: настройка административной дистанции маршрутов OSPF.

Default Information Originate

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: разрешение широковещательной передачи маршрута по умолчанию 0.0.0.0 в домен OSPF. Эта функция вступает в силу только в том случае, если маршрут 0.0.0.0 существует в локальной таблице маршрутизации.

Redistribute-Default Metric

Диапазон: 0–16777214

По умолчанию: 20

Функция: настройка метрики по умолчанию для импортированных внешних маршрутов.

Redistribute-Protocol

Тип протокола: Connected/Static/RIP

Функция: указывает тип протокола, маршруты которого будут перераспределяться в OSPF как внешние маршруты.

Описание:

Connected – перераспределяются напрямую подключенные маршруты.

Static – перераспределяются статические маршруты.

RIP – перераспределяются маршруты, полученные протоколом RIP

Redistribute-Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение или отключение перераспределения внешних маршрутов указанного типа.

Redistribute-Metric

Диапазон: 0–16777214

По умолчанию: не задано

Функция: задает стоимость (метрику) маршрутов, перераспределяемых в OSPF. Значение данной метрики имеет приоритет над глобальной метрикой по умолчанию при перераспределении.

Redistribute-Metric Type

Варианты настройки: 1/2

По умолчанию: 2

Функция: выбор типа по умолчанию для внешних маршрутов OSPF при перераспределении.

Описание:

1 (E1) – стоимость внешнего маршрута равна сумме стоимости маршрута от маршрутизатора к ASBR и стоимости маршрута от ASBR до пункта назначения.

2 (E2) – стоимость внешнего маршрута равна стоимости маршрута от ASBR до пункта назначения (стоимость до ASBR не учитывается).

SPF Delay Time

Диапазон: 0–600000 мс

По умолчанию: 0

Функция: минимальный интервал между запусками алгоритма SPF для расчета маршрутов OSPF. Позволяет избежать слишком частого повторного вычисления маршрутов при постоянных изменениях топологии.

SPF Initial Hold Time

Диапазон: 0–600000 мс

По умолчанию: 50 мс

Функция: начальный интервал ожидания перед повторным запуском алгоритма SPF после первого изменения топологии.

SPF Max Hold Time

Диапазон: 0–600000 мс

По умолчанию: 5000 мс

Функция: максимальный интервал ожидания между запусками алгоритма SPF при последовательных изменениях топологии.

LSA Interval

Диапазон: 0–1000 мс

По умолчанию: 1000 мс

Функция: минимальный интервал между обработками входящих пакетов LSA. Используется для сглаживания и предотвращения избыточной обработки LSA.

Refresh Interval

Диапазон: 10–1800 с, шаг – 10 с

По умолчанию: 10

Функция: интервал, с которым маршрутизатор обновляет свои LSA в базе данных OSPF.

2. Настройка областей Stub и NSSA

Нажмите [Function Management] → [Route] → [OSPF] → [Area Configuration], чтобы войти в интерфейс настройки областей OSPF, как показано ниже.

Рисунок 269 – Конфигурация областей OSPF

Area ID

Формат конфигурации: A.B.C.D

Диапазон: 0.0.0.0 – 255.255.255.255

Функция: задает идентификатор области OSPF в формате IPv4-адреса.

Type

Варианты настройки: Stub/NSSA

По умолчанию: Stub

Функция: определяет тип области OSPF. Stub – область без внешних маршрутов, NSSA – область, позволяющая ограниченно распространять внешние маршруты через LSA 7-го типа.

Translate

Варианты настройки: Candidate/Never/Always

По умолчанию: Candidate

Функция: настраивает правила преобразования LSA типа 7 в LSA типа 5 на ABR в NSSA.

Описание:

Candidate: ABR выбирается на основе RID, и только выбранный ABR выполняет преобразование LSA из типа 7 в тип 5. RID имеет приоритет при выборе.

Never: ABR в NSSA никогда не выполняет преобразование LSA.

Always: ABR в NSSA всегда выполняет преобразование LSA.

No Summary

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: определяет, является ли область полным Stub/NSSA. Если включено, то запрещается инжекция LSA типа 3 (маршрутов межобластного суммирования) в эту область.

3. Сетевые настройки

Нажмите [Function Management] → [Route] → [OSPF] → [Network Configuration], чтобы войти в интерфейс настройки сети OSPF, как показано ниже.

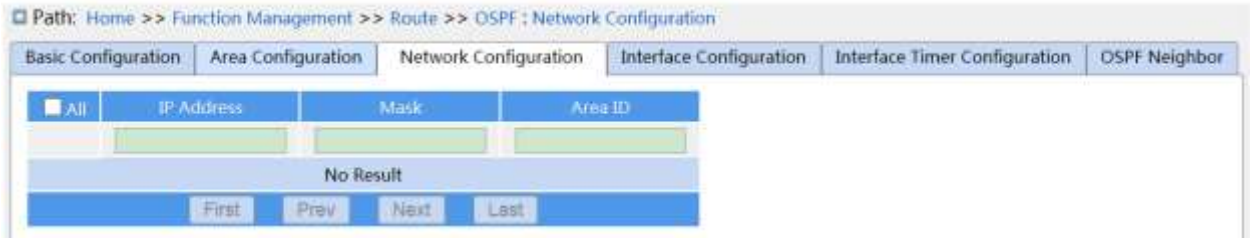


Рисунок 270 – Сетевые настройки OSPF

IP Address

Формат конфигурации: A.B.C.D

Функция: настройка сетевого IP-адреса.

Mask

Функция: настройка маски подсети сети.

Описание: маска и сетевой адрес вместе определяют сетевой диапазон.

Area ID

Формат конфигурации: A.B.C.D

Диапазон: 0.0.0.0 – 255.255.255.255

Функция: настройка общесетевого региона

Описание: после добавления сети в область все внутренние маршруты сети больше не транслируются независимо в другие области, а транслируется только сводная информация всего общесетевого маршрута.

4. Настройка интерфейсов

Нажмите [Function Management] → [Route] → [OSPF] → [Interface Configuration], чтобы открыть страницу настройки интерфейсов OSPF, как показано ниже.

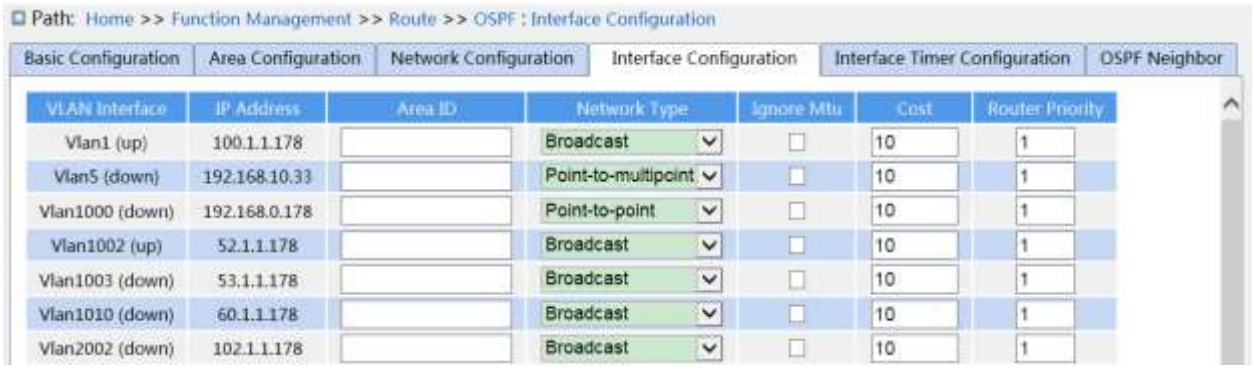


Рисунок 271 – Настройка областей и параметров интерфейсов VLAN

Area ID

Формат конфигурации: A.B.C.D

Диапазон: 0.0.0.0 – 255.255.255.255

Функция: настройка области, к которой принадлежит интерфейс VLAN.

Описание: добавление интерфейса VLAN в область OSPF означает включение протокола OSPF для данного интерфейса.

Network Type

Варианты настройки: Broadcast/Point to multipoint/Point to point

По умолчанию: Broadcast

Функция: настройка типа сети OSPF для выбранного интерфейса.

Ignore Mtu

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: определяет, будет ли интерфейс проверять соответствие значения MTU в получаемых пакетах DD (Database Description) от соседних маршрутизаторов при установлении смежности OSPF.

Описание: если проверка MTU активна (по умолчанию), и значение MTU в сообщении DD соседа не совпадает с локальным MTU, смежность не формируется. Если параметр «Ignore MTU» включен, проверка MTU игнорируется, и смежность устанавливается даже при несовпадении значений.

Cost

Диапазон: 1–65535

По умолчанию: 10

Функция: настройка стоимости пути интерфейса OSPF.

Router priority

Диапазон: 0–255

По умолчанию: 1

Функция: настройка приоритета интерфейса VLAN для запуска OSPF.

Описание: когда в сегменте сети определяются DR и BDR, в качестве DR выбирается устройство с наивысшим значением приоритета.

5. Настройка таймеров интерфейса

Нажмите [Function Management] → [Route] → [OSPF] → [Interface Timer Configuration], чтобы открыть страницу настройки таймеров интерфейсов OSPF, как показано ниже.

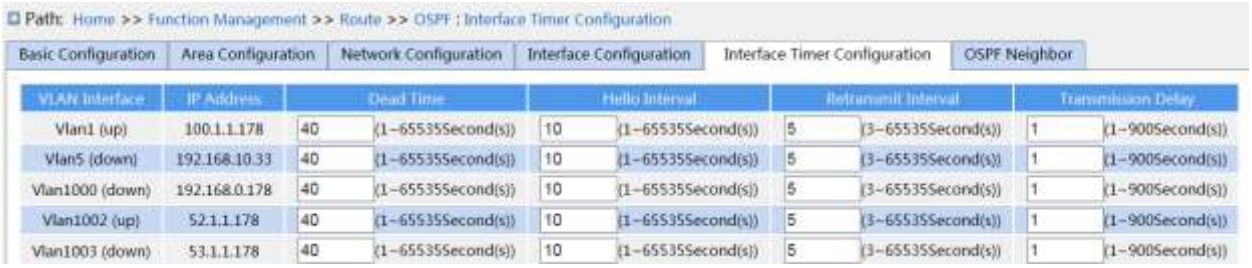


Рисунок 272 – Настройка временных параметров OSPF

Dead Time

Диапазон: 1–65535 с

По умолчанию: 40 с

Функция: настройка времени ожидания информации соседнего коммутатора на указанном интерфейсе.

Описание: когда коммутатор не получает пакет Hello, отправленный соседним устройством в течение указанного временного диапазона, считается, что соседнее устройство недоступно и недействительно.

Hello Interval

Диапазон: 1–65535 с

По умолчанию: 10 с

Функция: настройка интервала отправки пакетов Hello указанным интерфейсом.

Описание: коммутатор периодически отправляет пакеты Hello соседним устройствам для обнаружения, поддержания смежности и выбора DR/ BDR.

Retransmit Interval

Диапазон: 3–65535 с

По умолчанию: 5 с

Функция: указывает интервал повторной передачи LSA – время ожидания подтверждения (LSAck) от соседнего устройства после отправки LSA на выбранном интерфейсе. Если подтверждение в течение этого интервала не получено, LSA передается повторно.

Transmission Delay

Диапазон: 1–900 с

По умолчанию: 1 с

Функция: настройка задержки между последовательными передачами LSA на указанном интерфейсе.

Для обеспечения нормальной работы OSPF параметры таймеров соседей OSPF должны быть согласованы.

---

6. Информация о соседях

Нажмите [Function Management] → [Route] → [OSPF] → [OSPF Neighbor], чтобы просмотреть информацию о соседних устройствах OSPF, как показано ниже.

Рисунок 273 – Соседние устройства OSPF

7.17.3.6 Пример типовой настройки

R1 и R2 используют OSPF. R1 импортирует внешние статические маршруты в область OSPF.

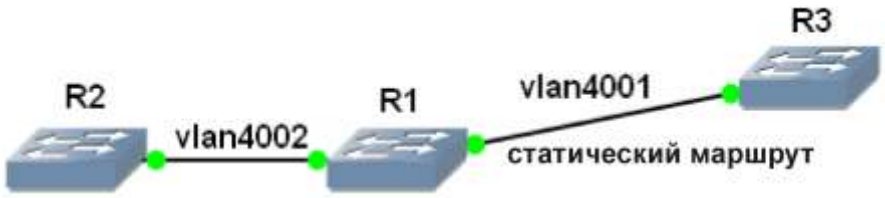


Рисунок 274 – Пример конфигурации OSPF

Настройка R1:

1. Укажите IP-адрес интерфейса VLAN 4002: 202.1.1.178, маску подсети: 255.0.0.0. Укажите IP-адрес интерфейса VLAN 4001: 201.1.1.178, маску подсети: 255.0.0.0;
2. Установите статический маршрут с адресом назначения 6.0.0.0/8 и следующим переходом 201.1.1.176.
3. Задайте идентификатор маршрутизатора 100.1.1.178, как показано на рисунке 268.
4. Запустите протокол OSPF, как показано на рисунке 268.
5. Установите область 0 интерфейса VLAN 4002, как показано на рисунке 269.
6. Настройте OSPF для перераспределения статических маршрутов, как показано на рисунке 270.

Настройка R2:

1. Укажите IP-адрес интерфейса VLAN 4002: 202.1.1.177, маску подсети: 255.0.0.0;
2. Задайте идентификатор маршрутизатора 100.1.1.177.
3. Запустите протокол OSPF.
4. Установите область 0 интерфейса VLAN 4002.

Настройка R3:

1. Укажите IP-адрес интерфейса VLAN 4001: 201.1.1.178, маску подсети: 255.0.0.0.

На этом этапе соседские отношения успешно устанавливаются на R1, как показано на рисунке 273.

7.18 QoS

7.18.1 Введение

Quality of Service (QoS) позволяет дифференцировать сервисы, в зависимости от разных требований в условиях ограниченной пропускной способности путем контроля трафика и изменения его движения в IP-сетях. QoS пытается оптимизировать передачу данных

различных сервисов, снизить задержки передачи и минимизировать их эффект в зависимости от приоритета сервиса.

Основная задача QoS – идентификация сервисов, управление перегрузкой при передаче данных и ее предотвращение.

Классификация трафика, контроль трафика, формирование трафика, управление перегрузками и предотвращение перегрузок – основные концепции внедрения QoS (качества обслуживания). Они выполняют следующие ключевые функции:

Классификация трафика: определение объекта на основе заданных правил сопоставления. Является основой и необходимым условием для реализации QoS.

Контроль трафика (полисинг): контролирует скорость передачи пакетов, направляемых на устройство. Если скорость трафика превышает заданный предел, устройство применяет ограничительные или штрафные меры для защиты сетевых ресурсов от перегрузок. Контроль трафика может быть на основе портов (port-based) и на основе очередей (queue-based).

Формирование трафика (шейпинг): проактивно регулирует скорость выхода трафика. Цель – адаптировать трафик под доступные сетевые ресурсы конечного устройства, чтобы предотвратить излишнее отбрасывание пакетов и возникновение перегрузок. Шейпинг также подразделяется на port-based и queue-based.

Управление перегрузками: обязательная функция для решения проблемы конкуренции за ресурсы. Управление перегрузками осуществляет буферизацию пакетов в очередях и определяет порядок их передачи на основе заданного алгоритма планирования, обеспечивая приоритетную обработку ключевых сервисов.

Предотвращение перегрузок: избыточная перегрузка может привести к повреждению сетевых ресурсов. Эта функция контролирует использование ресурсов сети и при обнаружении нарастающей перегрузки проактивно отбрасывает пакеты и регулирует объем трафика для устранения перегрузки.

Полисинг, шейпинг, управление перегрузками и их предотвращение обеспечивают регулирование сетевого трафика и выделенных ресурсов с разных сторон. Эти методы являются конкретным воплощением концепции QoS.

Например, коммутатор контролирует пакеты, передаваемые в сеть, на основе гарантированной скорости передачи. Перед отправкой пакетов коммутатор выполняет их формирование (шейпинг). В случае возникновения перегрузки осуществляется управление очередями с помощью алгоритмов планирования, а при усилении перегрузки применяются меры по ее предотвращению.

7.18.2 Принцип работы

Каждый порт коммутатора имеет 8 очередей для кэшированных данных, от 0 до 7 в порядке возрастания приоритета.

При поступлении кадра на порт коммутатор определяет очередь для данного кадра на основе информации кадра и порта. Данная серия коммутаторов поддерживает классификацию трафика с использованием следующих режимов сопоставления очередей,

расположенных по возрастанию приоритета: порт, информация заголовка 802.1Q, поле Differentiated Services Code Point (DSCP) и список управления QoS (QCL).

При передаче данных порт использует режим планирования для организации очередности обработки данных в 8 очередях и распределения пропускной способности каждой очереди. В данной серии коммутаторов поддерживаются два режима планирования: «6 очередей с взвешенным распределением» (6 Queues Weighted) и строгий приоритет (Strict Priority, SP).

Режим WRR (Weighted Round Robin) планирует потоки данных на основе весовых коэффициентов. Каждая очередь получает пропускную способность пропорционально своему весу. WRR обеспечивает приоритетное обслуживание очередей с более высоким весом, выделяя им большую часть пропускной способности.

Режим SP обеспечивает приоритетную передачу пакетов с высоким приоритетом, что особенно важно для чувствительных к задержкам сигналов. Если кадр попадает в очередь высокого приоритета, коммутатор приостанавливает обработку очередей с низким приоритетом и начинает обработку данных в очереди высокого приоритета. После опустошения очереди высокого приоритета коммутатор возобновляет обработку данных очередей с более низким приоритетом.

Режим «6 очередей с взвешенным распределением» предусматривает, что очереди 6 и 7 работают по режиму строгого приоритета (SP), а очереди с 0 по 5 – по режиму WRR. При этом данные из очереди 7 обрабатываются в первую очередь, затем очередь 6. Если очереди 7 и 6 пусты, данные из очередей 0–5 обрабатываются согласно весовым коэффициентам.

7.18.3 Настройка с помощью WEB-интерфейса

1. Настройте режим сопоставления очередей на основе портов, как показано ниже.

Рисунок 275 – Маппинг на основе портов

CoS

Диапазон: 0–7

По умолчанию: 0

Функция: настройка значения COS по умолчанию для порта.

Описание: значение CoS определяет очередь хранения сообщения и соответствует очередям с номером от 0 до 7. При поступлении сообщения в коммутатор ему присваивается значение CoS. Если сообщение является тегированным, но при этом отключена классификация по тегам, либо если сообщение нетегированное, то значением CoS для данного сообщения считается значение CoS по умолчанию, установленное для принимающего порта.

DPL

Диапазон: 0–1

По умолчанию: 0

Функция: настройка значения DPL (Drop Priority Level) по умолчанию для порта

Описание: указанное значение DPL используется в качестве значения приоритета сброса по умолчанию для порта при поступлении в коммутатор нетегированных сообщений или тегированных сообщений при отключенной классификации по тегам.

PCP

Диапазон: 0–1

По умолчанию: 0

Функция: настройка значения PCP (Priority Code Point) по умолчанию для порта

Описание: при поступлении на коммутатор нетегированного сообщения и последующем добавлении тега, значение приоритета в этом теге устанавливается равным значению PCP по умолчанию, заданному для порта.

DEI

Диапазон: 0–1

По умолчанию: 0

Функция: настройка значения DEI (Drop Eligible Indicator) по умолчанию для порта.

Описание: при поступлении на коммутатор нетегированного сообщения и последующем добавлении тега, значение поля CFI в этом теге устанавливается равным значению DEI по умолчанию, заданному для порта.

2. Настройте режим сопоставления очередей на основе информации заголовка 802.1Q.

Как показано на рисунке 275, отметьте «Tag Class» для порта и нажмите <Details Configuration> в столбце «(PCP, DEI) to (QOS, DPL) Mapping» Введите соответствующие значения для сопоставления на основе информации заголовка 802.1q, как показано ниже.

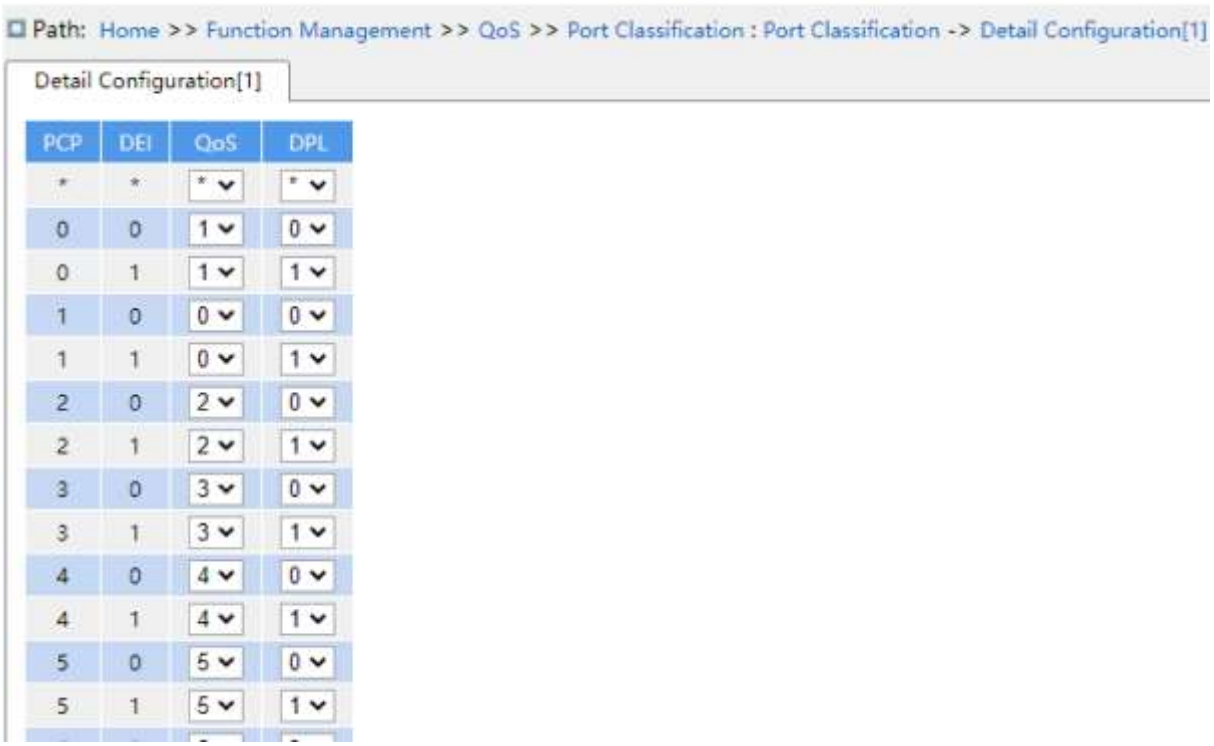


Рисунок 276 – Маппинг на основе информации заголовка 802.1Q

Режим сопоставления очередей, основанный на информации заголовка 802.1Q, подходит только для полученных сообщений с тегом.

Сопоставление (PCP, DEI) → (класс QoS, уровень DP)

Диапазон: класс QoS: 0–7; уровень DP: 0–1

По умолчанию: значения PCP 0, 1, 2, 3, 4, 5, 6, 7 соответствуют классам QoS 1, 0, 2, 3, 4, 5, 6, 7 соответственно; значения DEI 0, 1 соответствуют уровням DP 0, 1 соответственно.

Функция: настройка сопоставления значений PCP и DEI сообщения со значениями CoS и DPL.

Описание: класс QoS равен значению CoS, которое определяет очередь хранения сообщения и соответствует очередям с номерами от 0 до 7. При поступлении сообщения на коммутатор ему присваиваются значения CoS и DPL. Если сообщение является тегированным и включена классификация по тегам (Tag Class), значения CoS и DPL для сообщения определяются по заданному сопоставлению (PCP, DEI) → (CoS, DPL).

3. Настройте перемаркировку 802.1p, как показано ниже.

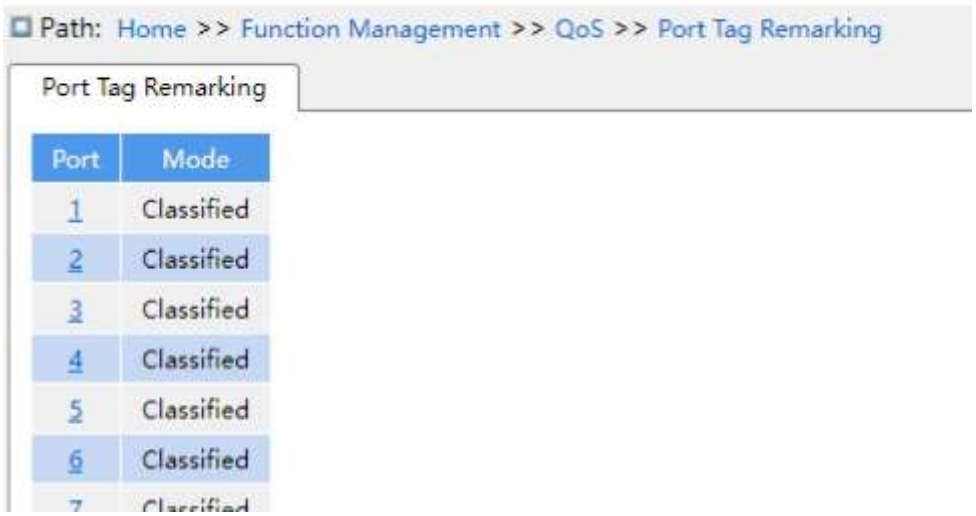


Рисунок 277 – Перемаркировка 802.1p

Нажмите кнопку <Port> и войдите на страницу настройки режима перемаркировки 802.1p, как показано на рисунке 278. Перемаркировка 802.1p – это процесс изменения (перезаписи) значений полей PCP и DEI в VLAN-теге Ethernet-кадра при его прохождении через порт коммутатора. Такая перезапись позволяет адаптировать приоритеты трафика в зависимости от политики QoS, принятой в сети, например, повысить или понизить приоритет сообщения. Режим перезаписи определяет, как именно будут изменяться значения PCP и DEI в кадрах при их пересылке через порт.

Рисунок 278 – Выбор режима перемаркировки для порта

Если в сообщении, обрабатываемом на порту, нет тега, настройка перемаркировки будет недействительна.

- Настройка перемаркировки 802.1p «Classified»

Tag Remarking Mode

Варианты настройки: Classified/Mapped/Default

По умолчанию: Classified

Функция: настройка режима перемаркировки 802.1p. В режиме «Classified» значения PCP и DEI в сообщении не обновляются, когда выходной порт пересылает сообщение.

- Настройка перемаркировки 802.1p «Default»

Рисунок 279 – Настройка режима «Default» для выбранного порта

Tag Remarking Mode

Варианты настройки: Classified/Mapped/Default

По умолчанию: Classified

Функция: настройка режима перемаркировки 802.1p. В режиме «Default» установленные значения PCP и DEI будут значениями по умолчанию для выходного порта.

Default PCP

Диапазон: 0–7

По умолчанию: 0

Функция: настройка значения PCP по умолчанию для выходного порта.

Default DEI

Диапазон: 0–7

По умолчанию: 0

Функция: настройка значения DEI по умолчанию для выходного порта.

- Настройка перемаркировки 802.1p «Mapped»

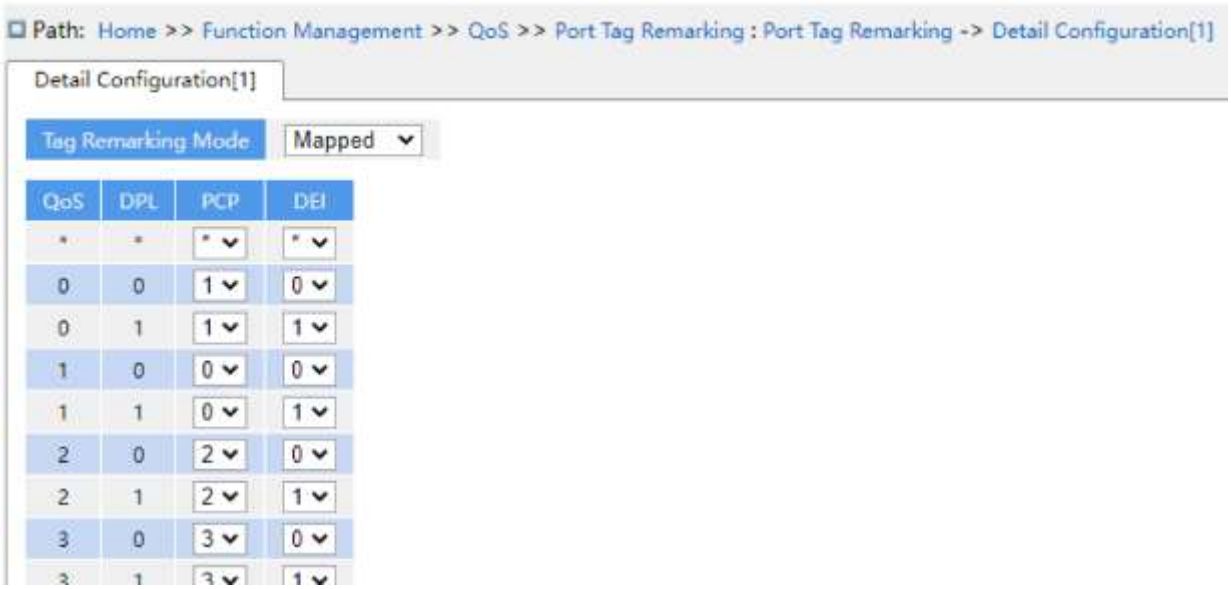


Рисунок 280 – Настройка режима «Mapped» для выбранного порта

Tag Remarking Mode

Варианты настройки: Classified/Mapped/Default

По умолчанию: Classified

Функция: настройка режима перемаркировки 802.1p. В режиме «Mapped» при отправке сообщения через порт значения PCP и DEI в VLAN-теге перезаписываются согласно заданному сопоставлению из внутренних параметров QoS – класса QoS (CoS) и уровня приоритета (DPL) – в значения PCP и DEI. Это позволяет согласовать внутренние механизмы приоритизации с внешними тегами 802.1p. Конфигурация сопоставления приведена ниже.

Сопоставление (класс QoS, уровень DP) → (PCP, DEI)

Варианты настройки: 0–7 (PCP), 0–1 (DEI)

По умолчанию: класс QoS 0, 1, 2, 3, 4, 5, 6, 7 сопоставляется со значением PCP 1, 0, 2, 3, 4, 5, 6, 7; уровень DP 0, 1 сопоставляется со значением DEI 0, 1.

Функция: в соответствии со значением CoS и DPL в сообщении настраивается сопоставление (CoS, DPL) → (PCP, DEI).

4. Настройте режим сопоставления очередей на основе DSCP, как показано ниже.

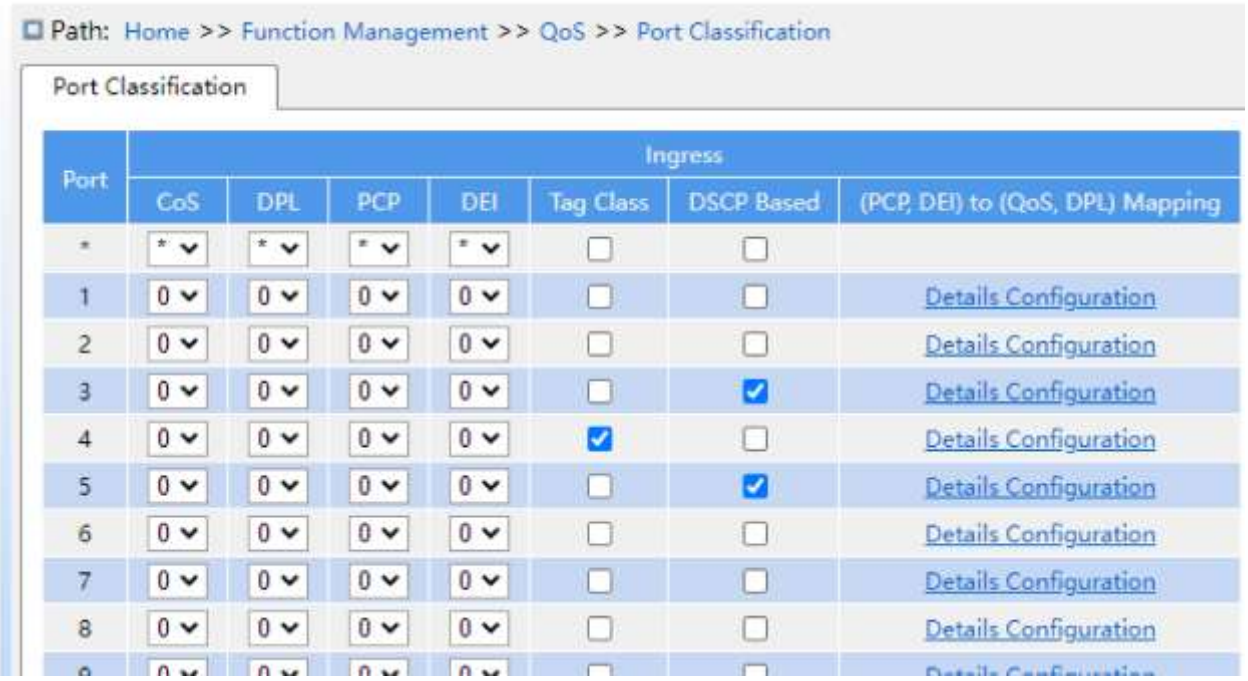


Рисунок 281 – Маппинг на основе DSCP

DSCP Based

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: позволяет включить или отключить использование DSCP для определения очередей QoS, и при включении DSCP приоритеты очередей будут назначаться на основе DSCP, а не только на основе 802.1Q тегов.

5. Включите функцию преобразования DSCP на входном порту и перезаписи на выходном порту, как показано ниже.

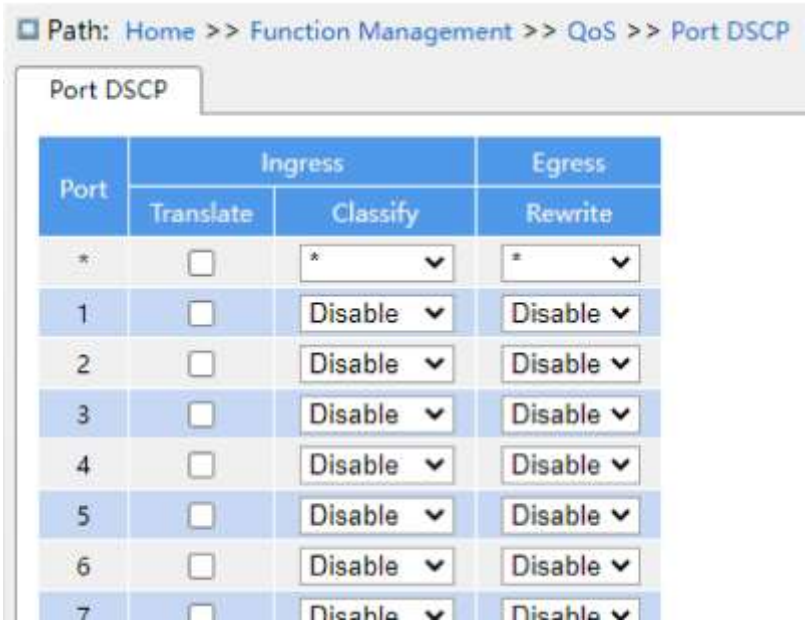


Рисунок 282 – Настройка DSCP портов

Translate

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: определяет, будет ли приемный (ingress) порт выполнять преобразование (трансляцию) значения DSCP в принятом пакете. Если включено, значение DSCP изменяется в соответствии с таблицей трансляции DSCP (столбец «Translate» на рисунке 284).

Classify

Варианты настройки: Disable/DSCP=0/Selected/All

По умолчанию: Disable

Функция: настраивает, для каких пакетов выходной (egress) порт будет переписывать значение DSCP, если режим перезаписи (Rewrite) включен.

Disable: DSCP не переписывается при передаче пакета;

DSCP=0: перезапись происходит только для пакетов с DSCP=0, согласно правилам классификации (см. рисунок 285);

Selected: если стоит галочка в столбце «Classify» (см. рисунок 284), то соответствующее значение DSCP в сообщении перезаписывается согласно правилу классификации (см. рисунок 285);

All: перезапись согласно правилам классификации (см. рисунок 285) происходит для всех пакетов.

Rewrite

Варианты настройки: Disable/Enable/Remap

По умолчанию: Disable

Функция: определяет режим перезаписи значения DSCP при передаче пакета исходящим портом.

Disable: значение DSCP в сообщении не перезаписывается;

Enable: значение DSCP в сообщении перезаписывается в соответствии с настройками классификации;

Remap: DSCP в сообщении переписывается в соответствии с таблицей сопоставления (DSCP, DPL) → DSCP (см. «Remap DP0, DP1» на рисунке 284).

6. Настройте режим сопоставления очередей на основе DSCP, как показано ниже.

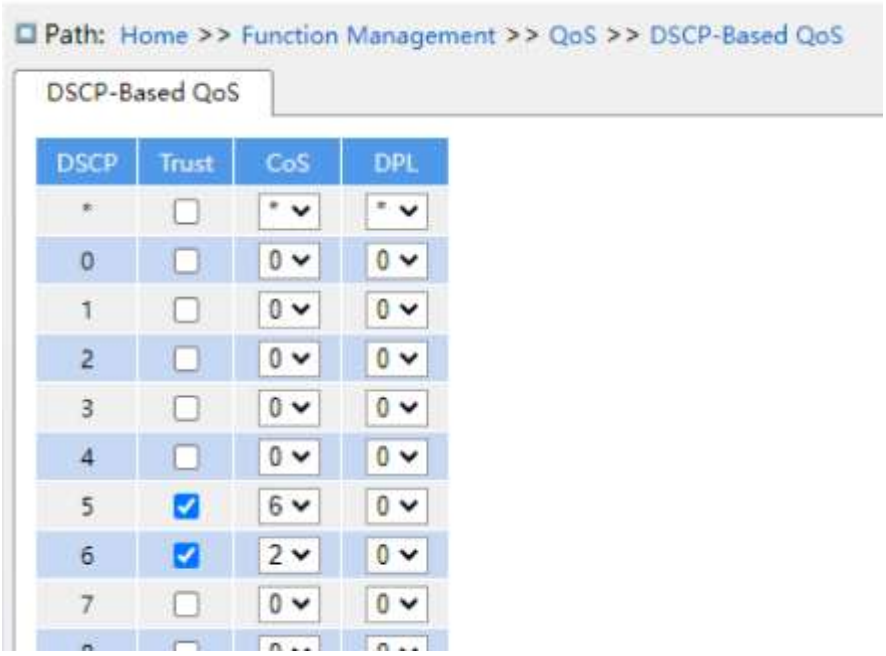


Рисунок 283 – Маппинг на основе DSCP

Trust

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: указывает, следует ли доверять ли значению DSCP.

Режим сопоставления очередей на основе DSCP применяется только к доверенным значениям DSCP в сообщениях, полученных портом.

COS

Диапазон: 0–7

По умолчанию: 0

Функция: настройка сопоставления DSCP и CoS.

Описание: значение CoS определяет, в какую очередь будет помещен пакет при обработке коммутатором. Значения CoS от 0 до 7 соответствуют очередям с номерами от 0 до 7 соответственно. При поступлении пакета с DSCP-значением, которому доверяет устройство (режим Trust), коммутатор назначает этому пакету соответствующее значение CoS согласно заданной карте соответствия DSCP → CoS.

Если на входном порту включено преобразование (функция Translate), коммутатор назначает CoS в соответствии с преобразованным значением DSCP; в противном случае CoS назначается в соответствии с исходным значением DSCP в сообщении.

DPL

Диапазон: 0–1

По умолчанию: 0

Функция: настройка сопоставления DSCP и DPL

Описание: после того, как сообщение с доверенным значением DSCP поступает на коммутатор, коммутатор назначает сообщению DPL согласно заданной карте соответствия DSCP → DPL.

7. Настройте преобразование и перезапись DSCP, как показано ниже.

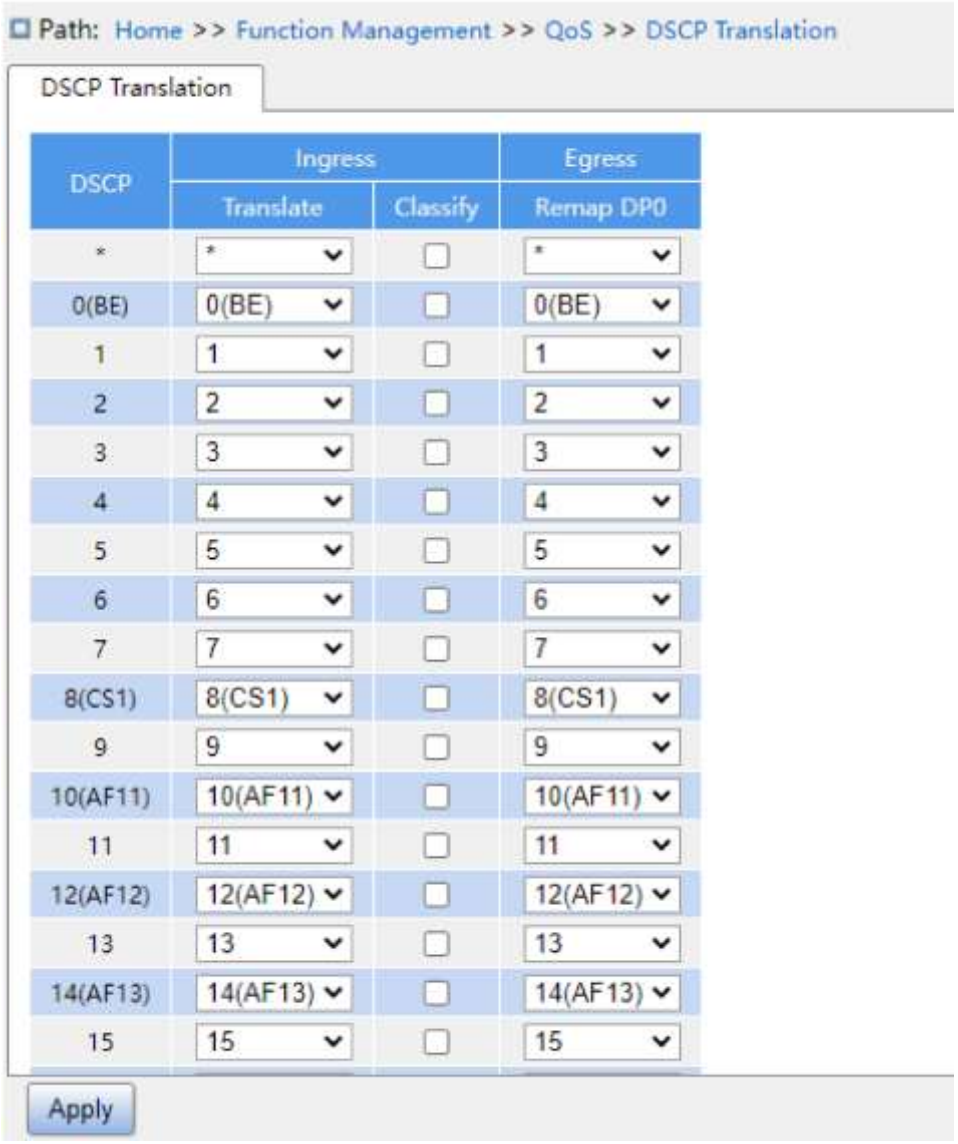


Рисунок 284 – Настройка преобразования и перезаписи DSCP

Translate

Диапазон: 0–63

Функция: настройка таблицы преобразования значений DSCP.

Classify

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: если отмечено галочкой, то при установке параметра «Classify» в режим «Selected» (см. рисунок 282), значение DSCP будет изменяться на выбранное.

Если на входном порту включена функция Translate, то для обработки пакета используется преобразованное значение DSCP. Если функция выключена, то для обработки пакета используется исходное значение DSCP, указанное в IP-заголовке пакета.

Remap DP0

Диапазон: 0–63

Функция: настройка сопоставления (DSCP, DPL) → DSCP.

8. Настройте классификацию на основе DSCP, как показано ниже.

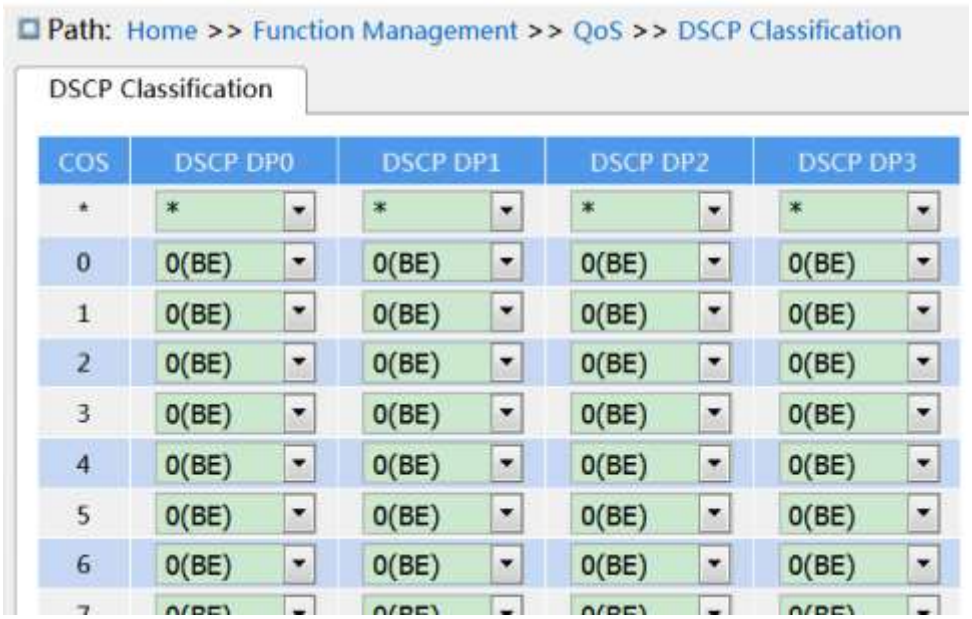


Рисунок 285 – Настройка классификации на основе DSCP

DSCP DP0/DSCP DP1

Диапазон: 0–63

Функция: настройка сопоставления комбинации значений CoS и DPL с соответствующим значением DSCP.

Описание: значение CoS определяет класс обслуживания и соответствует одной из очередей хранения пакетов (очереди с номерами от 0 до 7). При классификации QoS значение CoS используется для выбора очереди, в которую будет помещен пакет. Настройка DSCP DP0 и DSCP DP1 задает, каким образом сочетание CoS и уровня прецедентности отброса (DPL) преобразуется в значение DSCP для маркировки пакета.

9. Настройте элементы таблицы QCL, как показано ниже.

Рисунок 286 – Настройка таблицы QCL

Маппинг сообщений в очереди реализуется посредством сопоставления с таблицей QCL. Каждый элемент таблицы QCL содержит несколько условий, которые связаны логическим оператором «И» – то есть для совпадения пакета с элементом таблицы необходимо, чтобы все условия выполнялись одновременно. Между разными элементами таблицы QCL нет взаимной зависимости.

Если в таблице QCL несколько элементов, устройство последовательно сравнивает пакет с каждым элементом (в порядке сверху вниз). Как только пакет совпадает с первым подходящим элементом, выполняется соответствующее действие, и дальнейшее сравнение прекращается.

Для создания нового элемента таблицы нажмите кнопку «<⊕>». Для редактирования выбранного элемента выделите его и нажмите кнопку <Edit>. Для удаления выбранного элемента выделите его и нажмите кнопку <Del>.

Идентификатор элемента таблицы QCL (QCE) присваивается последовательно в порядке создания элементов.

Port

Функция: выбор активного порта текущего элемента таблицы QCL.

- Настройка параметров таблицы QCL

DMAC

Варианты настройки: Any/Unicast/Multicast/Broadcast

По умолчанию: Any

Функция: конфигурирует условие по MAC-адресу назначения. Условие считается выполненным, если MAC-адрес назначения в принимаемом сообщении соответствует выбранной настройке.

SMAC

Варианты настройки: Any/Specific

По умолчанию: Any

Функция: конфигурирует условие по MAC-адресу источника. При выборе «Specific» необходимо указать конкретный MAC-адрес. Условие считается выполненным, если MAC-адрес источника в принимаемом сообщении соответствует заданному.

Tag

Варианты настройки: Any/Untagged/Tagged

По умолчанию: Any

Функция: конфигурирует условие по наличию VLAN-тега. Условие считается выполненным, если тег сообщения соответствует выбранному параметру.

VID

Варианты настройки: Any / Specific (конкретное значение 1–4093) / Range (диапазон значений 1–4093)

По умолчанию: Any

Функция: конфигурирует условие по VLAN ID. При выборе «Specific» необходимо указать конкретное значение VID, при выборе «Range» – диапазон значений. Условие считается выполненным, если VID в сообщении соответствует заданному значению или диапазону. Если параметр Tag установлен в «Untagged», настройка VID недоступна.

PCP

Варианты настройки: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7

По умолчанию: Any

Функция: конфигурирует условие по полю приоритета PCP VLAN-тега. Условие считается выполненным, если PCP в сообщении соответствует выбранному значению или диапазону. Если параметр Tag установлен в «Untagged», настройка PCP недоступна.

DEI

Варианты настройки: Any/0/1

По умолчанию: Any

Функция: конфигурирует условие по индикатору возможности сброса DEI VLAN-тега. Условие считается выполненным, если DEI в сообщении соответствует выбранному значению. Если параметр Tag установлен в «Untagged», настройка DEI недоступна.

Frame Type

Варианты настройки: Any/EtherType/LLC/SNAP/IPv4

По умолчанию: Any

Функция: позволяет выбрать тип кадра для условия сопоставления.

Для детальной настройки нажмите на поле типа кадра, чтобы перейти в интерфейс расширенной конфигурации.

- Настройка параметров EtherType

Рисунок 287 – Настройка параметров EtherType

Ether Type

Варианты настройки: Any/Specific (конкретный диапазон значений: 0x600–0x7FF, 0x801–0x86DC, 0x86DE–0xFFFF)

По умолчанию: Any

Функция: конфигурирует условие по полю типа Ethernet-кадра. При выборе «Specific» необходимо указать конкретное значение или диапазон значений типа кадра. Условие считается выполненным, если Ethernet-кадр, принятый на порту, соответствует заданному типу.

- Настройка параметров LLC

Рисунок 288 – Настройка параметров LLC

DSAP Address/SSAP Address/Control

Варианты настройки: Any/Specific (конкретное значение в диапазоне 0x00–0xFF)

По умолчанию: Any

Функция: конфигурирует условия по параметрам LLC-кадра: DSAP (Destination Service Access Point), SSAP (Source Service Access Point) и Control. При выборе «Specific» необходимо указать конкретное значение. Условие считается выполненным, если LLC-кадр, принятый на порту, соответствует заданным параметрам.

- Настройка параметров SNAP

Рисунок 289 – Настройка параметров SNAP

PID

Варианты настройки: Any/Specific (конкретное значение в диапазоне 0x0000–0xFFFF)

по умолчанию: Any

Функция: конфигурирует условие по полю PID в SNAP-кадре. При выборе «Specific» необходимо указать конкретное значение PID. Условие считается выполненным, если PID в SNAP-кадре, принятом на порту, соответствует заданному значению.

- Настройка параметров IPv4

Рисунок 290 – Настройка параметров IPv4

Protocol

Варианты настройки: Any/UDP/TCP/Other (числовое значение 0–255)

По умолчанию: Any

Функция: конфигурирует условие по типу протокола IPv4 кадра. При выборе «UDP» или «TCP» необходимо дополнительно указать номера исходного и/или целевого портов. При выборе «Other» требуется указать числовой код протокола (0–255). Условие считается выполненным, если протокол IP-кадра, принятый на порту, соответствует заданной конфигурации.

Sport/Dport

Варианты настройки: Any / Specific (конкретное значение 0–65535) / Range (диапазон значений 0–65535)

По умолчанию: Any

Функция: конфигурирует условие по исходному (Sport) и целевому (Dport) портам TCP/UDP. При выборе «Specific» необходимо указать конкретный номер порта, при выборе «Range» – диапазон портов. Условие считается выполненным, если номер порта в IP-кадре соответствует заданному значению или диапазону.

SIP

Варианты настройки: Any/Specific

По умолчанию: Any

Функция: конфигурирует условие по исходному IP-адресу и маске. При выборе «Specific» необходимо указать IP-адрес и маску подсети. Условие считается выполненным, если IP-адрес источника в IP-кадре соответствует заданному.

IP Fragment

Варианты настройки: Any/Yes/No

По умолчанию: Any

Функция: конфигурирует условие по признаку фрагментации IP-кадра. Условие считается выполненным, если фрагментация в принятом кадре соответствует выбранной настройке.

DSCP

Варианты настройки: Any / Specific (конкретное значение 0–63) / Range (диапазон значений 0–63)

По умолчанию: Any

Функция: конфигурирует условие по значению DSCP в IP-кадре. При выборе «Specific» необходимо указать конкретное значение DSCP, при выборе «Range» – диапазон значений. Условие считается выполненным, если DSCP в принятом кадре соответствует заданному значению или диапазону.

- Настройка правил таблицы QCL (см. рисунок 286)

CoS

Варианты настройки: 0–7/Default

По умолчанию: Default

Функция: при совпадении принятого кадра на порту с записью таблицы QCL, значение CoS кадра изменяется на заданное. Значение CoS определяет очередь, в которую помещается кадр для последующей обработки: CoS 0–7 соответствует очередям с номерами 0–7 соответственно. Значение «Default» означает, что CoS кадра не изменяется.

DPL

Варианты настройки: Default/0/1

По умолчанию: Default

Функция: при совпадении принятого кадра с записью QCL изменяет значение DPL на указанное. Значение Default означает, что DPL кадра остается без изменений.

DSCP

Варианты настройки: Default/0–63

По умолчанию: Default

Функция: при совпадении с записью QCL изменяет значение DSCP в IP-заголовке кадра на заданное. Значение Default означает отсутствие изменений поля DSCP.

PCP

Варианты настройки: Default/0–7

По умолчанию: Default

Функция: при совпадении с записью QCL изменяет значение PCP в VLAN-теге кадра на указанное. Значение Default означает, что PCP не изменяется.

DEI

Варианты настройки: Default/0/1

По умолчанию: Default

Функция: при совпадении с записью QCL изменяет значение DEI в VLAN-теге кадра на указанное. Значение Default означает, что DEI остается без изменений.

- Просмотр элемента таблицы QCL

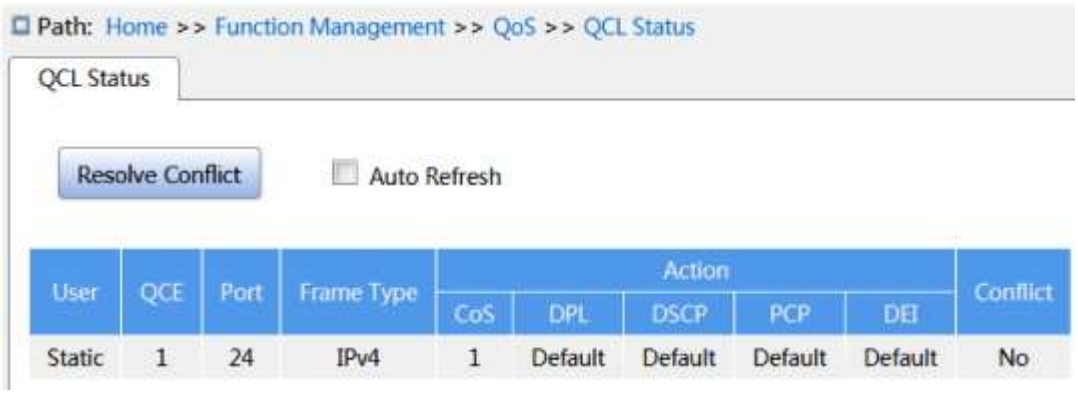


Рисунок 291 – Элемент таблицы QCL

Conflict

Варианты отображения: No/Yes

Описание: отображает состояние конфликта для элемента таблицы QCL. Если для создания данного элемента таблицы QCL недостаточно ресурсов, состояние конфликта устанавливается в «Yes». В противном случае отображается «No».

При нажатии кнопки <Resolve Conflict> освобождаются необходимые ресурсы, занятые конфликтующими элементами таблицы QCL, что позволяет устранить конфликт и успешно создать или применить текущий элемент.

10. Настройте контроль скорости очередей, как показано ниже.

Рисунок 292 – Полисинг на основе очередей

Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включает или отключает функцию контроля скорости очереди. После включения необходимо настроить параметры скорости (Rate) и единицы измерения (Unit).

Rate, Unit

Диапазон: 25–13128147 кбит/с / 1–13128 Мбит/с

По умолчанию: 500 кбит/с

Функция: ограничивает скорость приема кадров в очереди на порту. Если скорость поступающего трафика превышает заданное значение, избыточные кадры будут отброшены.

11. Настройте режим планировщика очередей на портах, как показано на рисунках 293 и 294.

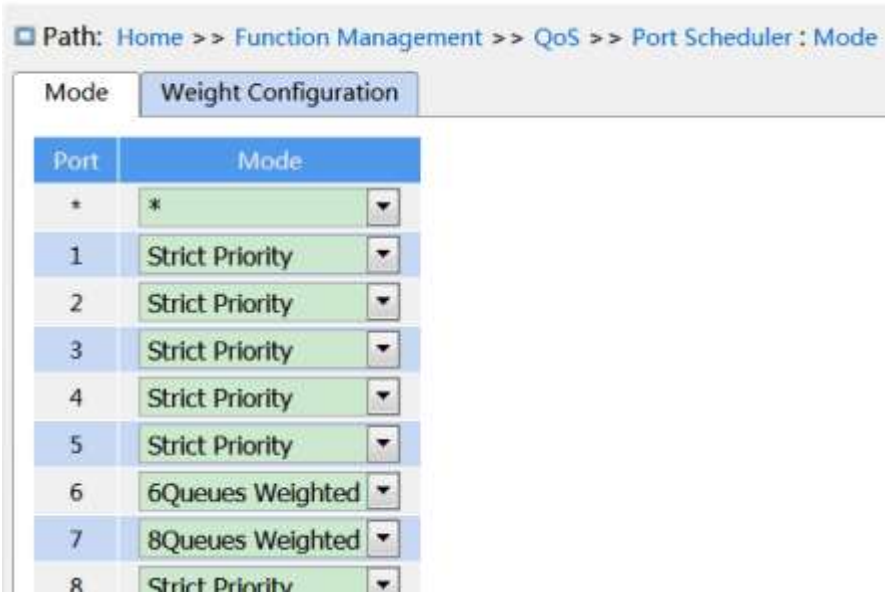


Рисунок 293 – Настройка режима планировщика

Рисунок 294 – Настройка веса очереди

Mode

Варианты настройки: Strict Priority / 2–8 Queues Weighted

По умолчанию: Strict Priority

Функция: определяет режим работы планировщика очередей порта.

Strict Priority: очереди обрабатываются в порядке приоритета, пока не опустеют, без учета весов.

Weighted: очереди обрабатываются по принципу взвешенного перебора, где вес каждой очереди влияет на долю выделяемого ей времени.

Weight

Диапазон: 1–100

По умолчанию: 17

Функция: задает вес очереди при работе в режиме взвешенного планировщика. Чем больше значение веса, тем большую долю времени процессор выделяет данной очереди.

12. Настройте формирование трафика на портах, как показано ниже.

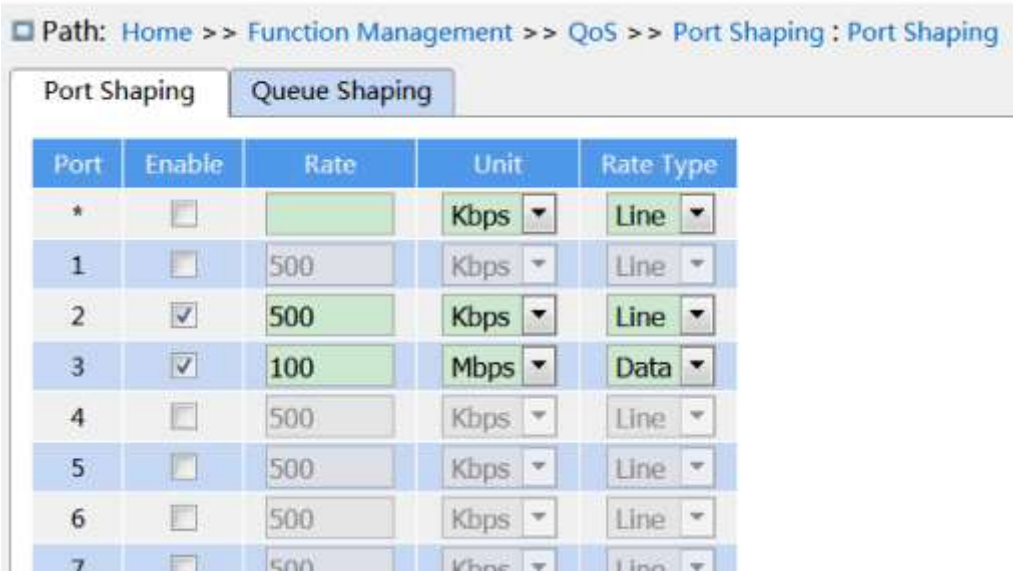


Рисунок 295 – Настройка шейпинга на портах

Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включает или отключает функцию формирования трафика на порту. Формирование трафика реализуется через ограничение скорости передачи данных на порту.

Rate, Unit

Диапазон: 100–13107100 кбит/с / 1–13107 Мбит/с

По умолчанию: 500 кбит/с

Функция: ограничивает скорость передачи кадров через порт. Кадры, превышающие установленный лимит скорости, будут отброшены.

Rate type

Диапазон: Line/Data

По умолчанию: Line

Функция: определяет режим применения ограничения скорости:

Line: ограничение применяется к общей длине кадра (включая заголовки и служебные данные);

Data: ограничение применяется только к полезной нагрузке кадра (без учета заголовков).

13. Настройте формирование трафика в очередях, как показано ниже.

Рисунок 296 – Настройка шейпинга в очередях

Enable

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включает или отключает функцию формирования трафика для конкретной очереди на порту.

Rate, Unit

Диапазон: 100–13107100 кбит/с / 1–13107 Мбит/с

По умолчанию: 500 кбит/с

Функция: ограничивает скорость передачи кадров через указанную очередь на порту. Кадры, превышающие установленный лимит скорости, будут отброшены.

Rate type

Диапазон: Line/Data

По умолчанию: Line

Функция: определяет режим применения ограничения скорости:

Line: ограничение применяется к общей длине кадра (включая заголовки и служебные данные);

Data: ограничение применяется только к полезной нагрузке кадра (без учета заголовков).

7.18.4 Пример типовой настройки

Как показано на рисунке 297, в данной конфигурации пакеты с портов 1–5 направляются на порт 6. При этом:

- Пакеты, получаемые на порту 1, являются нетегированными (Untag) и помещаются в очередь 2.
- Пакеты, получаемые на порту 2, имеют значения PCP=0 и DEI=1 и помещаются в очередь 3.
- Пакеты, получаемые на порту 3, имеют значение DSCP=4 и помещаются в очередь 6.
- Порт 4 направляет все пакеты с исходным MAC-адресом 00-00-00-00-00-23 в очередь 5 и при этом изменяет DSCP в этих пакетах на 9.
- Пакеты, получаемые на порту 5, имеют значение DSCP=5 и помещаются в очередь 2.
- Порт 6 использует режим планирования очередей SP+WRR.

➢ Последовательность настройки:

1. Установить для порта 1 значение CoS=2 (см. рисунок 275).

2. Включить на порту 2 классификацию по тегам (Tag Class) и сопоставить (PCP=0, DEI=1) с CoS=3 (см. рисунки 275, 276).

3. Включить на портах 3 и 5 классификацию по DSCP (DSCP Based) (см. рисунок 281).

4. Доверять значениям DSCP 4 и 5 и сопоставить DSCP=4 с очередью 6, DSCP=5 – с очередью 2 (см. рисунок 283).

5. Создать запись QCL для порта 4 с исходным MAC-адресом 00-00-00-00-00-23, установить действие записи: CoS=5 и DSCP=9 (см. рисунок 286).

6. Настроить режим планирования очередей порта 6 на 6 очередей с взвешенным перебором (Weighted), веса очередей Q0–Q5: 20, 40, 40, 20, 20, 20 (см. рисунки 293, 294).

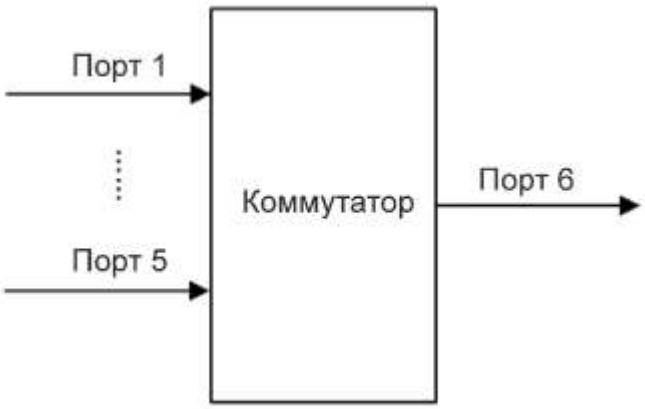


Рисунок 297 – Пример конфигурации QoS

➢ Итоги распределения:

- Пакеты портов 1 и 5 поступают в очередь 2.
- Пакеты порта 2 – в очередь 3.
- Пакеты порта 3 – в очередь 6.
- Пакеты порта 4 – в очередь 5.

➢ Режимы планирования очередей порта 6:

- Очереди 6 и 7 работают в режиме строгого приоритета (Strict Priority).
- Очереди 0–5 работают в режиме взвешенного перебора (WRR).
- Данные из очереди 6 обрабатываются в первую очередь. Если очередь 6 пуста, обслуживание очередей 0–5 происходит согласно весам.

➢ Распределение пропускной способности:

Вес очередей: 20, 40, 40, 20, 20, 20 (для очередей Q0–Q5 соответственно).

- Доля полосы пропускания для пакетов в очереди 2 (порт 1 и порт 5) составляет: 40/(20+40+40+20+20+20)=25%
- Для пакетов в очереди 3 (порт 2): 20/(20+40+40+20+20+20)=12,5%
- Для пакетов в очереди 5 (порт 4): 20/(20+40+40+20+20+20)=12,5%

Пакеты портов 1 и 5, находясь в одной очереди 2, обрабатываются по принципу FIFO (First In, First Out), при этом суммарная пропускная способность для этой очереди составляет 25%.

7.19 VRRP

Понятие «маршрутизаторы» в этой главе относится к коммутаторам третьего уровня.

7.19.1 Введение

VRRP (Virtual Router Redundancy Protocol) добавляет несколько маршрутизаторов, которые могут действовать как сетевые шлюзы, в группу VRRP, которая образует виртуальный маршрутизатор. С помощью механизма выбора VRRP в группе определяется мастер, остальные маршрутизаторы становятся резервными. В случае выхода мастера из строя, среди резервных маршрутизаторов выбирается новый мастер, что обеспечивает бесперебойную передачу данных без изменения конфигурации.

В данной серии коммутаторов VRRP поддерживает SEWM3GX28P

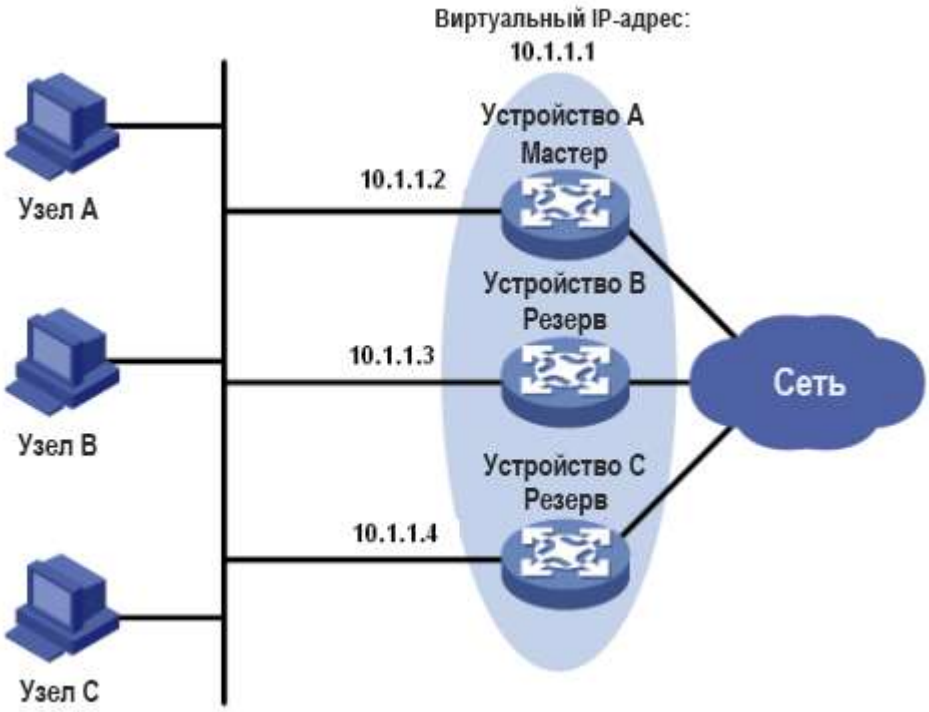


Рисунок 298 – VRRP

Как показано на рисунке 298, устройства A, B и C образуют виртуальный маршрутизатор с IP-адресом. Хосты A, B и C могут взаимодействовать с внешними сетями через виртуальный маршрутизатор только в том случае, если его IP-адрес в их настройках указан как следующий переход (хоп) маршрута по умолчанию. Виртуальный маршрутизатор состоит из одного главного и нескольких резервных коммутаторов. Мастер действует как шлюз. В случае сбоя один из резервных коммутаторов возьмет на себя функции вышедшего из строя мастера и будет выступать в качестве шлюза.

- IP-адрес виртуального маршрутизатора может быть либо неиспользуемым IP-адресом в сегменте, где находится группа VRRP, либо IP-адресом интерфейса маршрутизатора из этой группы.
- Маршрутизатор, IP-адрес интерфейса которого совпадает с адресом виртуального маршрутизатора, является владельцем IP-адреса.
- В каждой группе VRRP может быть только один владелец IP-адреса.

7.19.2 Выбор мастера

1. Маршрутизатор с наивысшим приоритетом в группе VRRP выбирается в качестве мастера. Он периодически отправляет объявления VRRP, чтобы информировать другие маршрутизаторы в группе о том, что он работает корректно.

Приоритет VRRP находится в диапазоне от 0 до 255. Чем больше число, тем выше приоритет. Приоритеты от 1 до 254 настраиваются. Приоритет 0 зарезервирован для специального использования, а приоритет 255 – для владельца IP-адреса.

---

2. Резервные маршрутизаторы получают информацию о приоритетах других маршрутизаторов в группе путем обмена пакетами VRRP.

Если приоритет мастера в объявлении выше его собственного приоритета, маршрутизатор остается резервным.

Если приоритет мастера в объявлении ниже, чем собственный приоритет маршрутизатора, маршрутизатор берет на себя роль мастера в вытесняющем режиме и остается резервным в невытесняющем режиме.

Если в течение определенного периода не было получено объявлений VRRP, маршрутизатор считает, что мастер вышел из строя, и отправляет объявления VRRP, чтобы начать новый выбор мастера.

- Невытесняющий режим: когда маршрутизатор в группе VRRP становится ведущим, он остается ведущим до тех пор, пока работает нормально, даже если резервному маршрутизатору позднее будет присвоен более высокий приоритет.
- Вытесняющий режим: когда резервный маршрутизатор обнаруживает, что его приоритет выше приоритета мастера, он отправляет объявления VRRP, чтобы начать новый выбор мастера в группе.

7.19.3 Мониторинг указанного интерфейса

Если интерфейс восходящей линии связи маршрутизатора в группе VRRP выходит из строя, обычно группа не может знать об отказе такого интерфейса. Если маршрутизатор является мастером, узлы в локальной сети не могут получить доступ к внешним сетям. Эту проблему можно решить, отслеживая указанный интерфейс восходящей линии связи. В случае сбоя интерфейса приоритет ведущего устройства автоматически снижается на установленное, и маршрутизатор с более высоким приоритетом в группе VRRP становится ведущим.

7.19.4 Настройка с помощью WEB-интерфейса

1. Создайте/отредактируйте/удалите группу VRRP, как показано ниже.

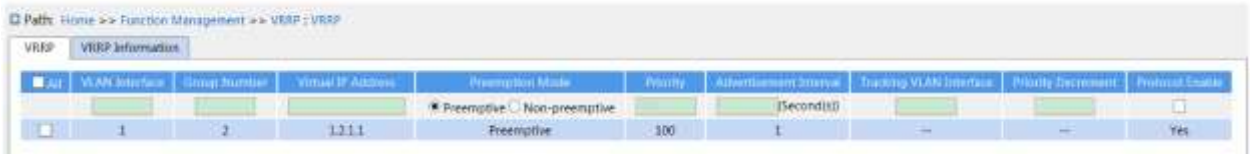


Рисунок 299 – Создание группы VRRP

VLAN Interface

Диапазон: 0–4093

Функция: настройка интерфейса VLAN указанной группы виртуального резервируемого маршрутизатора.

Group Number

Диапазон: 1–255

Функция: настройка идентификатора группы VRRP.

Virtual IP Address

Формат конфигурации: A.B.C.D

Функция: настройка IP-адреса виртуального маршрутизатора.

Примечание: IP-адрес виртуального маршрутизатора должен находиться в том же сегменте сети, что и IP-адрес интерфейса.

Preemption Mode

Варианты настройки: Preemptive/Non-preemptive

Функция: выбор режима работы виртуального маршрутизатора.

Preemptive: режим вытеснения. Если резервный маршрутизатор обнаруживает, что его приоритет выше, чем у текущего главного, он отправляет объявления VRRP группе резервирования, в результате чего в ней происходит выбор нового мастера.

Non-preemptive: не вытесняющий режим. Пока мастер не выйдет из строя, резервный маршрутизатор не станет главным, даже если он настроен с более высоким приоритетом.

Priority

Диапазон: 1–254

По умолчанию: 100 (для не владельцев IP-адресов)

Функция: настройка приоритета маршрутизатора в группе VRRP. Маршрутизатор с наивысшим приоритетом выбирается в качестве мастера.

Advertisement Interval

Диапазон: 1–255 с

По умолчанию: 1 с

Функция: установка интервала отправки VRRP-объявлений главным маршрутизатором.

Интервал отправки VRRP-объявлений должен быть одинаковым для всех участников группы резервирования.

Tracking VLAN Interface

Диапазон: 1–4093

Функция: выбор отслеживаемого интерфейса VLAN.

Priority Decrement

Диапазон: 1–255

Функция: установка значения уменьшения приоритета.

- Владелец IP-адреса виртуального маршрутизатора не может быть настроен как отслеживаемый интерфейс.
- Приоритет главного маршрутизатора после уменьшения должен быть меньше, чем у резервного маршрутизатора.

Protocol Enable

Варианты настройки: включено/выключено

Функция: включает протокол VRRP.

2. Ниже показана страница отображения информации VRRP.

Рисунок 300 – Информация VRRP

7.19.5 Пример типовой настройки

Как показано на рисунке 301, коммутатор A и коммутатор B образуют виртуальный маршрутизатор с IP-адресом 192.168.2.4. Узел A может связываться с узлом B через виртуальный маршрутизатор. Когда коммутатор A работает правильно, он является мастером в группе VRRP. Когда коммутатор A или VLAN 3 выходит из строя, мастером становится коммутатор B.

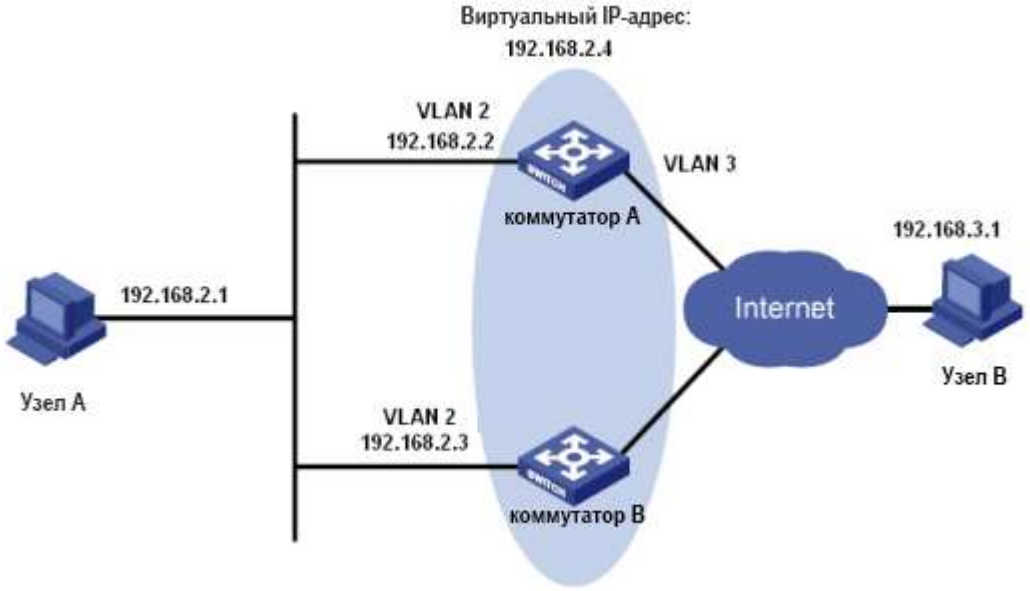


Рисунок 301 – Пример типовой настройки VRRP

Настройка коммутатора A:

1. Установите IP-адрес VLAN 2: 192.168.2.2, маску подсети: 255.255.255.0.
2. Создайте VRRP группу с идентификатором 1 (см. рисунок 299).
3. Задайте виртуальный IP-адрес VRRP-группы 1: 192.168.2.4.
4. Назначьте VLAN 2 в качестве интерфейса уровня 3 для VRRP-группы 1 (см. рисунок 299).
5. Установите приоритет коммутатора A в группе равным 110, режим вытеснения – Non-preemptive (см. рисунок 299).
6. Настройте VLAN 3 как отслеживаемый интерфейс и задайте декремент 30 для уменьшения приоритета при потере связи с этим интерфейсом (см. рисунок 299).
7. Включите протокол VRRP (см. рисунок 299).

Настройка коммутатора B:

1. Установите IP-адрес VLAN 2: 192.168.2.3, маску подсети: 255.255.255.0.
2. Создайте VRRP-группу с идентификатором 1 (см. рисунок 299).
3. Задайте виртуальный IP-адрес VRRP-группы 1: 192.168.2.4.
4. Назначьте VLAN 2 в качестве интерфейса уровня 3 для VRRP группы 1 (см. рисунок 299).
5. Установите приоритет коммутатора B в группе равным 100, режим вытеснения – Non-preemptive (см. рисунок 299).
6. Включите протокол VRRP (см. рисунок 299).

8. Диагностика

8.1 Журналирование

8.1.1 Введение

Функция журналирования (логирования) предназначена для записи информации о состоянии системы, ошибках, отладочных данных, аномалиях и других событиях. При правильной настройке коммутатор может в реальном времени отправлять журналы на сервер, поддерживающий протокол Syslog.

В журнале содержатся сведения о следующих событиях и состояниях:

- сигналы тревоги;
- штормы широковещательного трафика;
- перезагрузки устройства;
- использование памяти;
- действия и операции пользователей.

8.1.2 Настройка с помощью WEB-интерфейса

1. Настройте системный журнал, как показано ниже.

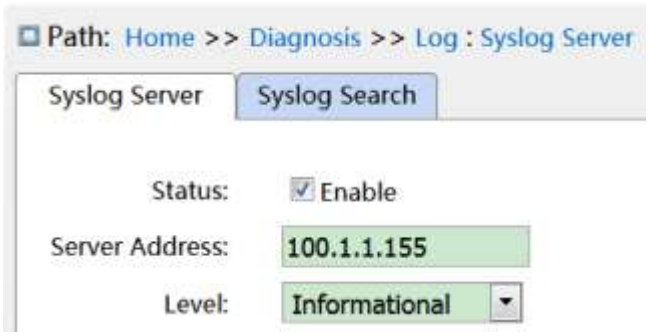


Рисунок 302 – Настройка Syslog-сервера

Status

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение функции передачи журнала на Syslog-сервер.

Server address

Формат конфигурации: A.B.C.D

Функция: IP-адрес Syslog-сервера.

Level

Варианты настройки: Error/Warning/Notice/Information

По умолчанию: Information

Функция: выбор уровня журналирования (ошибка, предупреждение, уведомление, информация).

2. Ниже показан поиск в системном журнале.

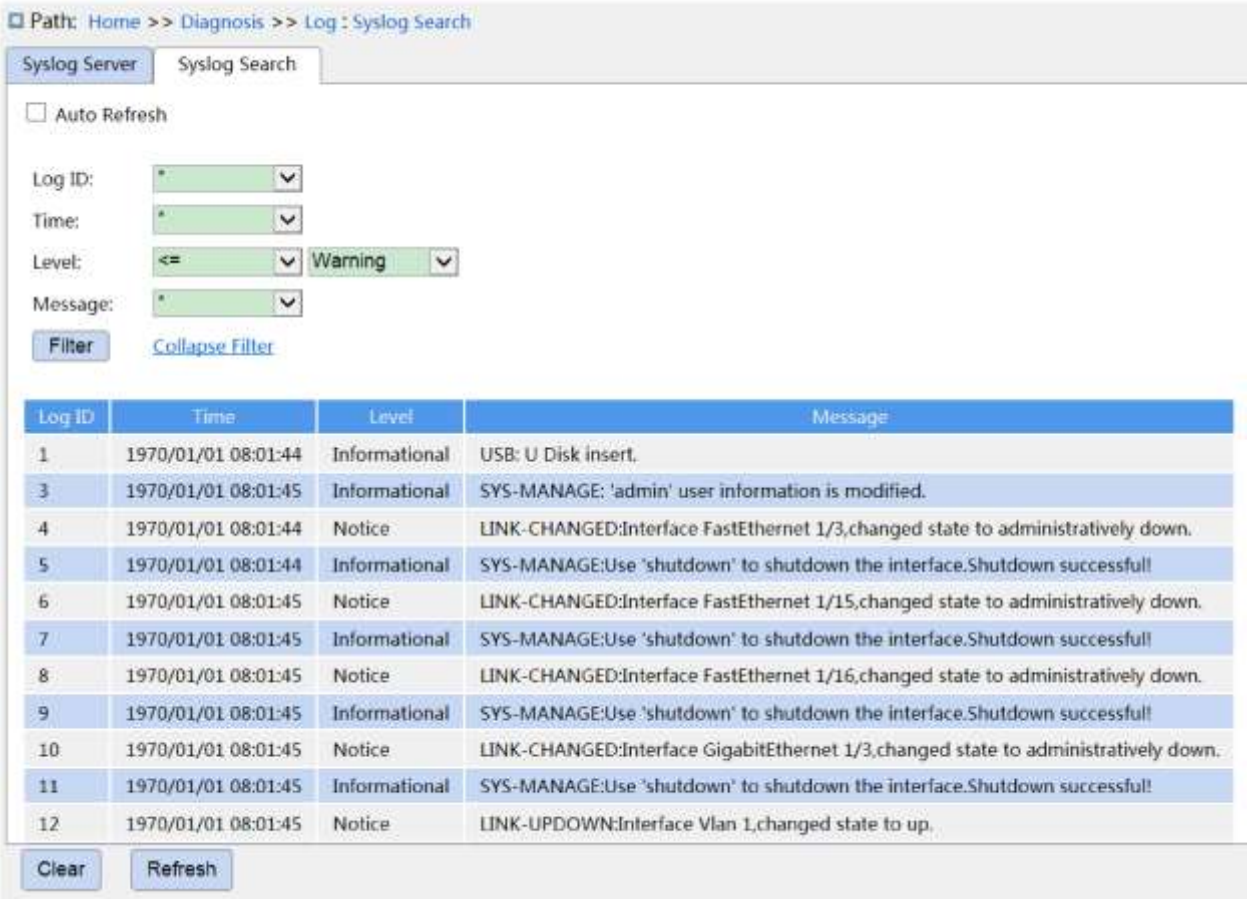


Рисунок 303 – Поиск в системном журнале

Auto Refresh

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение или отключение автоматического обновления списка журналов.

Log ID

Варианты настройки: */>=/<=/select range

По умолчанию: *

Функция: позволяет выбрать записи журнала по идентификатору (ID).

* – все записи;

>= – записи с ID, большим или равным заданному;

<= – записи с ID, меньшим или равным заданному;

select range – ручной ввод диапазона ID.

Time

Варианты настройки: */Start/end/select range

По умолчанию: *

Функция: позволяет выбрать записи журнала за определенный период времени.

* – все записи;

Start – начало временного диапазона;

End – конец временного диапазона;

select range – ручной ввод временного интервала.

Level

Варианты настройки: */>=/<=/ select range

По умолчанию: *

Функция: позволяет выбрать записи журнала по уровню важности. Доступны следующие уровни: ошибка (Error), предупреждение (Warning), уведомление (Notice), информация (Information).

* – все уровни;

>= – записи с уровнем, большим или равным заданному;

<= – записи с уровнем, меньшим или равным заданному;

выбор диапазона – ручной ввод диапазона уровней.

Message

Варианты настройки: */include/not include

По умолчанию: *

Функция: позволяет фильтровать записи журнала по содержимому сообщений.

* – все записи;

include – включить записи, содержащие указанные поля;

not include – исключить записи с указанными полями.

3. Очистите записи журнала, как показано ниже.

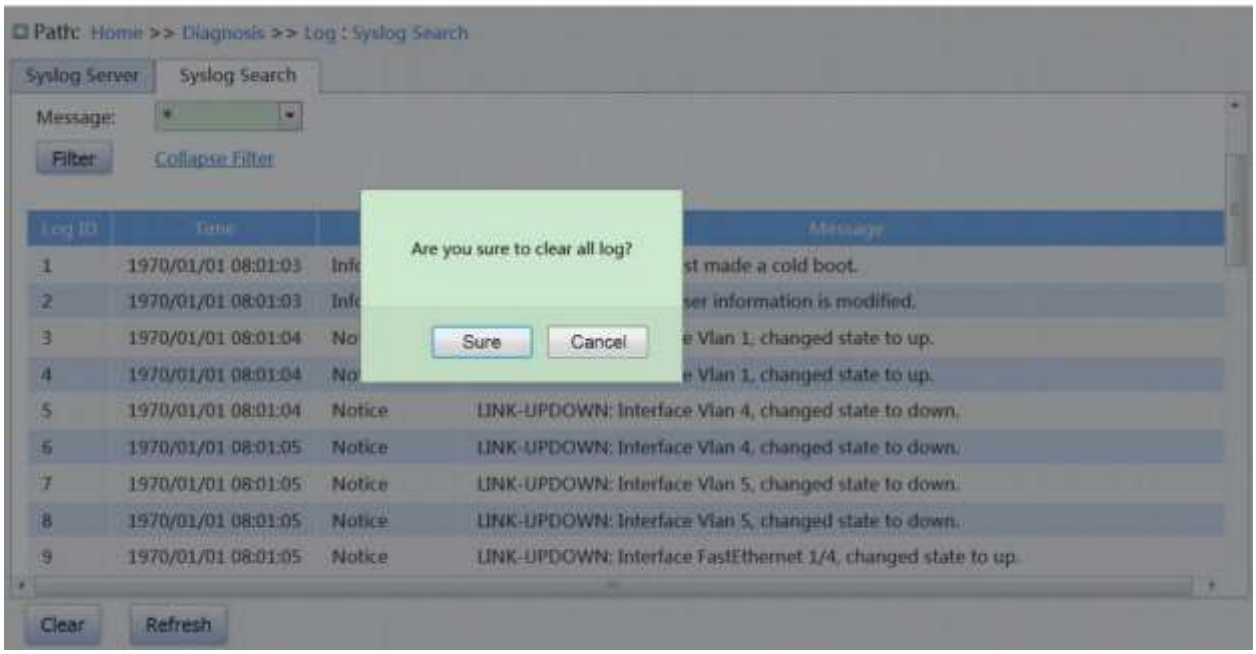


Рисунок 304 – Очистка записей журнала

После завершения поиска по журналу нажмите кнопку <Clear> в левом нижнем углу для удаления текущих записей журнала.

Для приема и просмотра журналов по протоколу Syslog на ПК можно установить программное обеспечение, поддерживающее функцию Syslog-сервера, например, Tftp32. Получаемая информация журнала будет отображаться в режиме реального времени, как показано ниже.

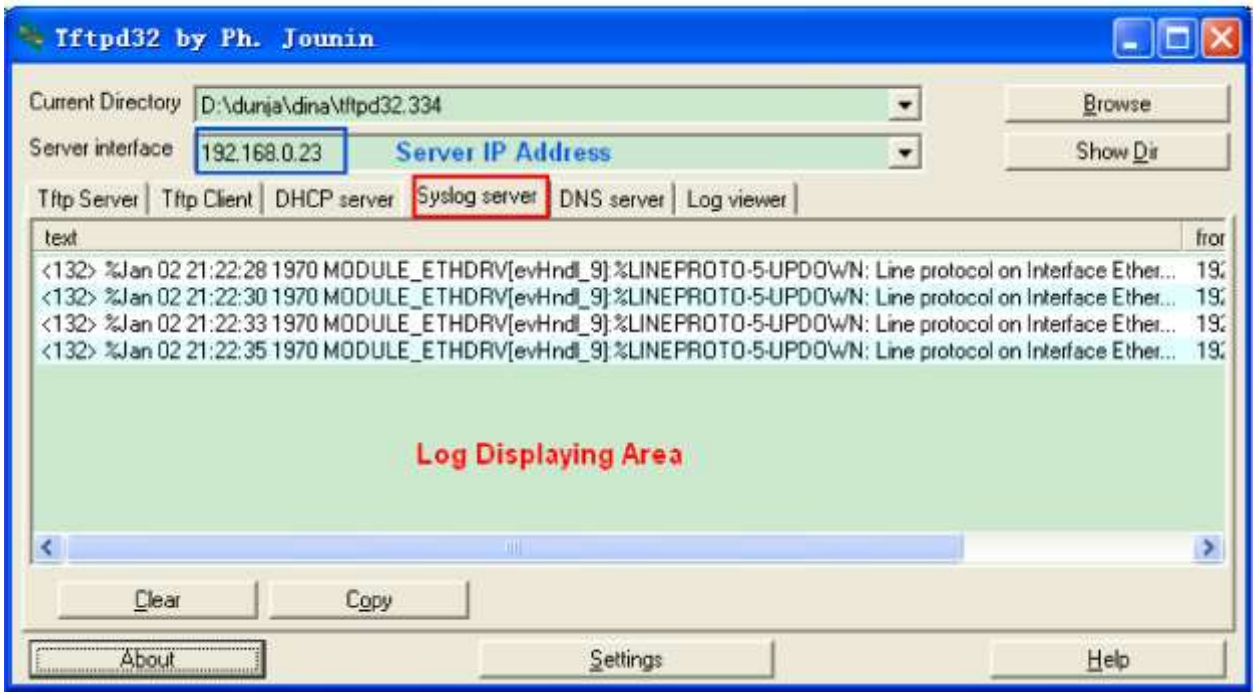


Рисунок 305 – Загрузка журнала в режиме реального времени

8.2 Зеркалирование портов

8.2.1 Введение

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

8.2.2 Описание

Коммутатор поддерживает только один порт назначения для зеркалирования, но несколько портов-источников.

Порты, данные которых зеркалируются, могут быть в одной сети VLAN или в разных. При этом, порты источника и назначения зеркалирования также могут быть в одной или в разных VLAN.

Один и тот же порт нельзя настроить как исходный и целевой одновременно.

На порту назначения должно быть отключено динамическое изучение MAC-адресов.

8.2.3 Настройка с помощью WEB-интерфейса

1. Настройте функцию зеркалирования на портах, как показано ниже.

Рисунок 306 – Настройка зеркалирования на портах

ALL

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: выбор группы зеркалирования для редактирования и изменения.

Status

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение функции зеркалирования.

Destination Port

Варианты настройки: NULL/номер порта

По умолчанию: NULL

Функция: выбор порта назначения для зеркалирования. Разрешен только один порт назначения.

Rx

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение или отключение зеркалирования кадров, принимаемых на исходном порту.

Tx

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: включение или отключение зеркалирования кадров, передаваемых с исходного порта.

2. Настройте функцию удаленного зеркалирования, как показано ниже.

Рисунок 307 – Настройка удаленного зеркалирования

ALL

Варианты настройки: включено/выключено

По умолчанию: выключено

Функция: выбор группы зеркалирования для редактирования и изменения.

Status

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение функции зеркалирования.

Destination Remote

Варианты настройки: NULL/номер порта

По умолчанию: NULL

Функция: включение зеркалирования для удаленного порта назначения. Одновременно нельзя включать удаленное зеркалирование для порта назначения и порта источника.

Destination VLAN ID

Диапазон: 1–4093

Функция: настройка VLAN ID для порта назначения удаленного зеркалирования.

Destination Port

Варианты настройки: NULL/номер порта

По умолчанию: NULL

Функция: указывает порт назначения для удаленного зеркалирования.

Source Remote

Варианты настройки: Enable/Disable

По умолчанию: Disable

Функция: включение удаленного зеркалирования порта источника. Одновременно нельзя включать удаленное зеркалирование для порта источника и порта назначения.

Source VLAN ID

Диапазон: 1–4093

Функция: настройка VLAN ID для удаленного зеркалирования порта источника.

Source Port

Варианты настройки: выключено/RX/TX

По умолчанию: выключено

Функция: если удаленное зеркалирование включено для порта назначения, нужно выбрать, какой трафик с порта источника будет зеркалироваться: входящий (RX) или исходящий (TX). Если же удаленное зеркалирование включено для порта источника, то выбор направления трафика (RX или TX) для порта источника здесь сделать нельзя – эта настройка недоступна.

8.2.4 Пример типовой настройки

Как показано на рисунке 308, порт назначения зеркалирования – это порт 2, а порт источника – порт 1. Как передаваемые, так и принимаемые портом 1 пакеты зеркалируются на порт 2.

Рисунок 308 – Пример зеркалирования портов

Процесс настройки:

1. Включите функцию зеркалирования портов, как показано на рисунке 306.

2. Укажите порт 2 в качестве целевого, порт 1 в качестве исходного. Отметьте режим RX и TX для зеркалирования входящих и исходящих кадров, как показано на рисунке 306.

8.3 LLDP

8.3.1 Введение

LLDP (Link Layer Discovery Protocol) предоставляет стандартный механизм обнаружения второго уровня. Он собирает информацию, такую как возможности устройства, адрес, идентификатор устройства и интерфейса в пакет Link Layer Discovery Protocol Data Unit (LLDPDU), и передает LLDPDU своим непосредственно подключенным соседям. Получив LLDPDU, соседние устройства сохраняют содержащуюся в нем информацию в своей базе управления (MIB), что позволяет системе управления сетью (NMS) выполнять запросы и проверять состояние соединений.

8.3.2 Настройка с помощью WEB-интерфейса

1. Настройте LLDP, как показано ниже.

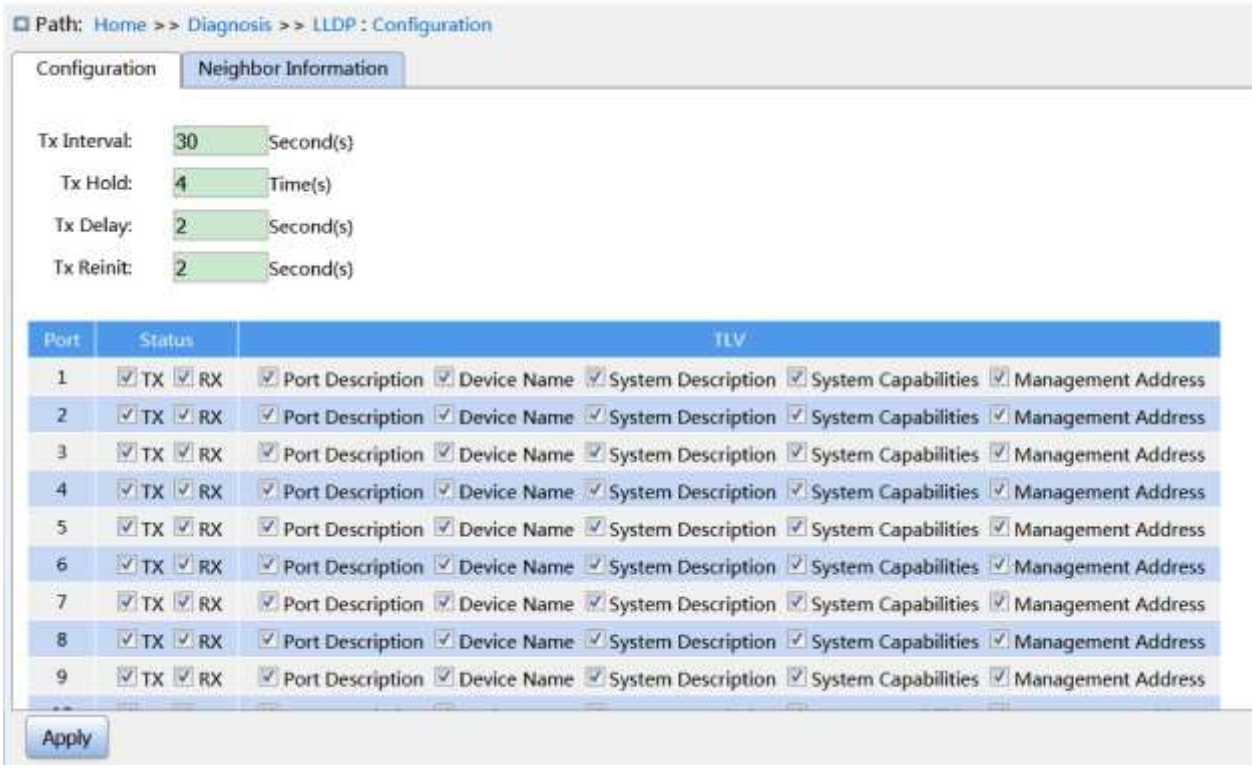


Рисунок 309 – Настройка LLDP

Tx Interval

Диапазон: 5–32768 с

По умолчанию: 30 с

Функция: настройка интервала времени между отправками LLDP-пакетов.

Tx Hold

Диапазон: 2–10 раз

По умолчанию: 4 раза

Функция: количество интервалов передачи, в течение которых LLDP-пакет считается действительным. Эффективное время жизни LLDP-пакета рассчитывается как произведение Tx Interval на Tx Hold.

Tx Delay

Диапазон: 1–8192 с

По умолчанию: 2 с

Функция: задержка между отправкой нового LLDP-пакета и предыдущего после изменения конфигурации. Значение Tx Delay не должно превышать четверть значения Tx Interval.

Tx Reinit

Диапазон: 1–10 с

По умолчанию: 2 с

Функция: интервал между отправкой LLDP shutdown-пакета (при отключении LLDP на порту или перезагрузке коммутатора) и повторной инициализацией передачи LLDP-пакетов.

Status

Параметры настройки: отключено /TX/RX/TX&RX

По умолчанию: TX&RX

Функция: настройка режима работы LLDP:

TX&RX – коммутатор отправляет и принимает LLDP-пакеты;

TX – только отправляет LLDP-пакеты;

RX – только принимает и обрабатывает LLDP-пакеты;

отключено – пакеты LLDP не отправляются и не принимаются.

Port Description

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение передачи описания порта в LLDP-пакетах.

Device Name

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение передачи системного имени устройства в LLDP-пакетах.

System Description

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение передачи описания системы в LLDP-пакетах.

Sys Capability

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение передачи информации о возможностях устройства в LLDP-пакетах.

Management Address

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение передачи адреса управления устройства в LLDP-пакетах.

2. Просмотрите информацию LLDP, как показано ниже.

Рисунок 310 – Отображение информации LLDP

Для отображения информации LLDP необходимо включить LLDP на двух подключенных устройствах.

8.4 Traceroute

Трассировка маршрута позволяет при помощи команды traceroute определить путь прохождения IP-пакетов от одного устройства до другого, показывая последовательность промежуточных шагов (маршрутизаторов).

1. Настройте traceroute, как показано ниже.

Рисунок 311 – Настройка traceroute

Destination address

Формат конфигурации: A.B.C.D

Функция: указывает IP-адрес конечного устройства, до которого необходимо выполнить трассировку.

Timeout Period

Диапазон: 1–10 с

По умолчанию: 2 с

Функция: время ожидания ответа от каждого промежуточного устройства. Если в течение этого времени ответ не получен, считается, что связь с данным узлом отсутствует.

Max Hop

Диапазон: 1–255

По умолчанию: 30

Функция: максимальное количество промежуточных узлов (маршрутизаторов), через которые может пройти пакет при трассировке. По достижении этого значения трассировка прекращается.

2. Просмотрите выходные данные команды traceroute, как показано ниже.

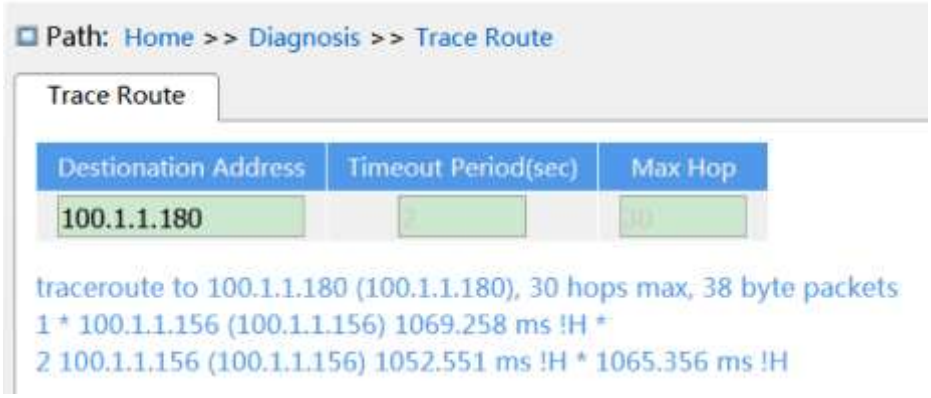


Рисунок 312 – Вывод информации о маршруте

8.5 Ping

Команда ping позволяет проверить доступность устройства по заданному IP-адресу и выявить возможные проблемы с сетевым соединением в процессе обслуживания системы.

1. Ниже показана настройка команды ping

Рисунок 313 – Настройка команды ping

Server Address

Формат: A.B.C.D

Описание: укажите IP-адрес устройства, доступность которого необходимо проверить.

Ping Length

Диапазон: 2–1452 байта

По умолчанию: 56 байт

Функция: задает длину ICMP-запроса (без учета заголовков IP и ICMP) для передачи.

Ping Count

Диапазон: 1–60

По умолчанию: 5

Функция: определяет количество ICMP-запросов, которые будут отправлены.

Ping Interval

Диапазон: 0–30 с

По умолчанию: 0 с

Функция: задает интервал времени между отправкой последовательных ICMP-запросов.

2. Просмотрите информацию, выводимую командой ping.

Рисунок 314 – Вывод команды ping

8.6 IP Source Guard

8.6.1 Введение

Функция IP Source Guard (защита источника IP) позволяет связывать IP-адреса с определенными портами коммутатора и фильтровать передаваемые через эти порты сообщения. Это предотвращает прохождение нелегитимных пакетов и ограничивает несанкционированное использование сетевых ресурсов, например, когда злоумышленник пытается выдать себя за законного пользователя, используя чужой IP-адрес. В результате повышается безопасность порта и всей сети.

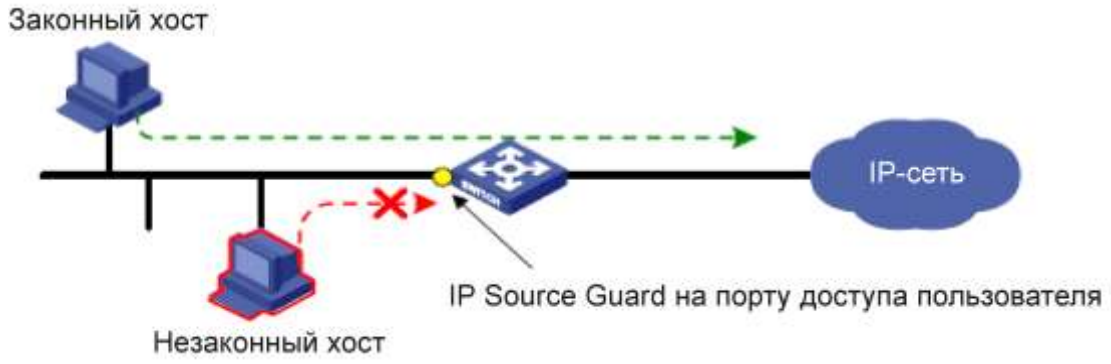


Рисунок 315 – Функциональная схема IP Source Guard

8.6.2 Принцип работы

Порт, на котором включена функция IP Source Guard, при получении пакета проверяет информацию в привязочной таблице (binding table). Если параметры пакета совпадают с записью в таблице, пакет пропускается через порт. В противном случае пакет отбрасывается. Привязка выполняется по отдельному порту – ограничения действуют только на этот порт, остальные порты не затрагиваются.

Параметры привязки (binding items):

Функция IP Source Guard использует для проверки пакетов такие параметры как исходный IP-адрес, исходный MAC-адрес, VLAN ID (тег VLAN).

Поддерживаются различные комбинации этих параметров:

- IP, MAC, IP+MAC
- IP + VLAN, MAC+VLAN, IP+MAC+VLAN

Типы параметров, поддерживаемые конкретным портом, зависят от модели и конфигурации устройства.

IP Source Guard поддерживает два способа формирования привязочной таблицы:

➢ Статическая привязка

Записи в таблице создаются вручную администратором. Подходит для небольших сетей или случаев, когда требуется индивидуальная настройка для каждого хоста.

➢ Динамическая привязка

Записи формируются автоматически на основе данных DHCP Snooping или DHCP Relay. Подходит для больших локальных сетей с динамическим распределением IP-адресов через DHCP. Принцип работы заключается в том, что при выдаче DHCP-адреса пользователю автоматически добавляется соответствующая запись в привязочную таблицу, разрешающая доступ к сети. Если пользователь пытается использовать IP-адрес без получения его через DHCP (например, вручную настроенный адрес), доступ к сети будет запрещен, так как соответствующая запись в таблице отсутствует.

8.6.3 Настройка с помощью WEB-интерфейса

1. Включите IP Source Guard глобально, как показано ниже.

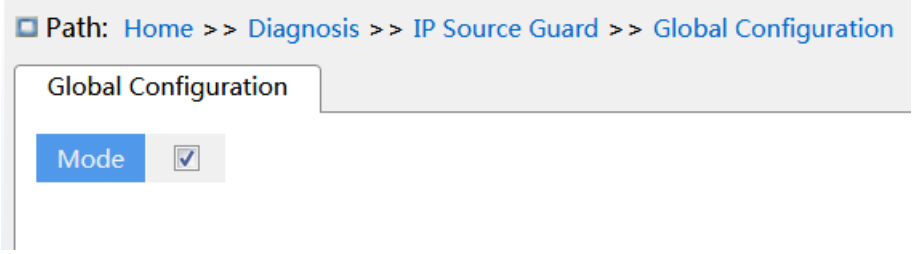


Рисунок 316 – Включение IP Source Guard

Mode

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение IP Source Guard в режиме глобальной конфигурации

2. Включите IP Source Guard на портах, как показано ниже.

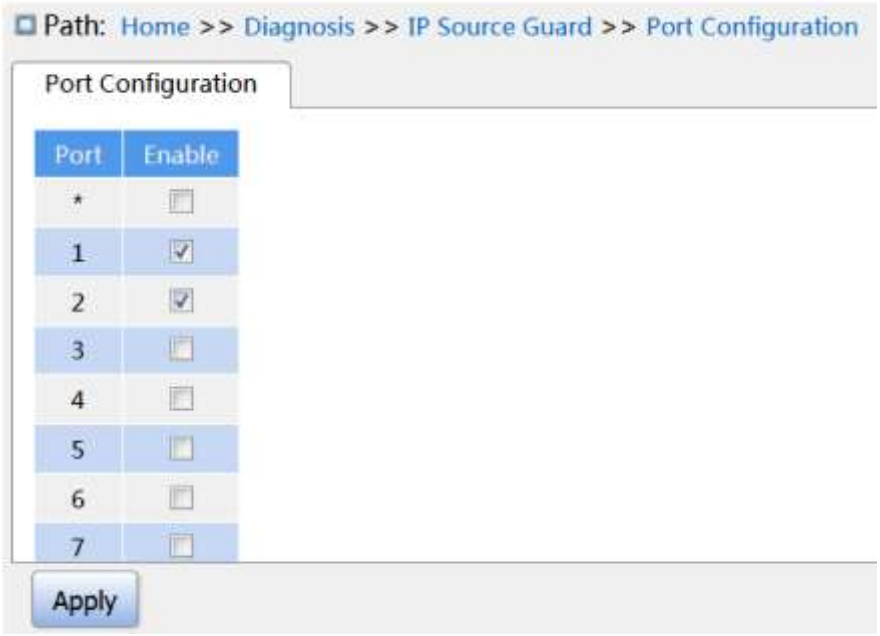


Рисунок 317 – Включение IP Source Guard на портах

Enable

Варианты настройки: включено/выключено

По умолчанию: включено

Функция: включение IP Source Guard в режиме настройки интерфейса

3. Ниже показана настройка статической привязки IP Source Guard

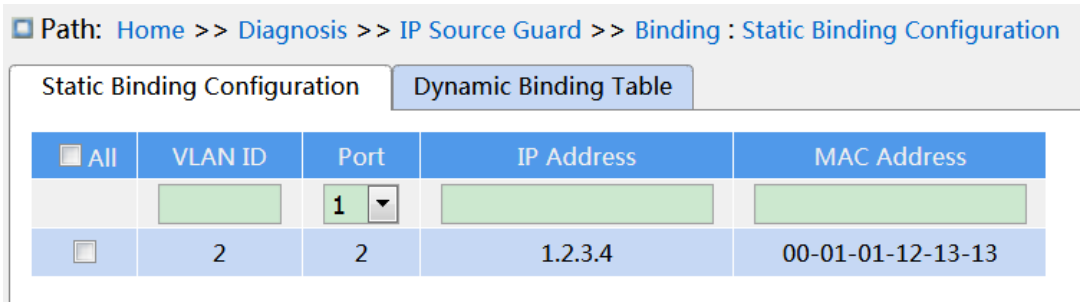


Рисунок 318 – Статическая привязка IP Source Guard

VLAN ID

Варианты настройки: все VLAN ID

Функция: задает идентификатор VLAN для записи в статической таблице привязки. Позволяет указать, к какой VLAN относится данная запись.

Port

Функция: выбор порта коммутатора, которому будет принадлежать запись в статической таблице привязки. Записи привязки применяются только к выбранному порту.

IP address

Формат конфигурации: A.B.C.D

Функция: задает IP-адрес, который будет привязан к указанному порту и MAC-адресу в статической таблице.

MAC address

Формат конфигурации: HH-HH-HH-HH-HH-HH или HH:HH:HH:HH:HH:HH (H – шестнадцатеричный символ от 0 до F)

Функция: задает MAC-адрес, который будет привязан к указанному порту и IP-адресу в статической таблице. Допускается только указание MAC-адреса unicast.

4. Просмотрите таблицу динамической привязки, как показано ниже.

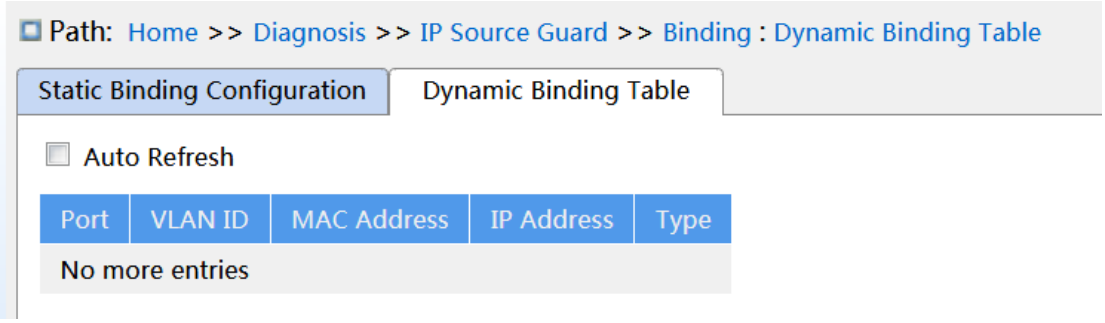


Рисунок 319 – Таблица динамической привязки

Type

Варианты отображения: Relay/Snooping

Описание: динамическая таблица привязки формируется на основе данных, полученных от DHCP Relay и DHCP Snooping.

Записи типа «Relay» создаются после включения глобальной функции IP Source Guard.

Записи типа «Snooping» формируются при включении функции IP Source Guard как глобально, так и на портах, подключенных к DHCP-клиентам.

8.6.4 Пример типовой настройки

1. Записи типа Relay в таблице IP Source Guard

На рисунке 320 показана следующая схема:

Коммутатор A – DHCP-сервер,

Коммутатор B – DHCP Relay,

Коммутатор C – DHCP-клиент.

Порт 1 коммутатора A подключен к порту 1 коммутатора B, порт 2 коммутатора B – к порту 2 коммутатора C. DHCP-сервер и DHCP-клиент находятся в разных LAN.

После включения функции IP Source Guard на ретрансляторе (коммутаторе B) клиент динамически получает IP-адрес и другие сетевые параметры через DHCP с использованием DHCP relay. В результате ретранслятор формирует записи таблицы IP Source Guard типа Relay.

Рисунок 320 – Конфигурация DHCP с ретранслятором

➢ Настройка коммутатора A (DHCP-сервер):

1. Создайте VLAN 1 и настройте IP-адрес: 100.1.1.156;
2. Включите DHCP-сервер в VLAN 1 (см. рисунок 200);
3. Создайте пул адресов pool-33 (см. рисунок 201);
4. Выберите тип пула – Network, IP-адрес: 33.1.1.6, маска: 255.0.0.0 (см. рисунок 202).

➢ Настройка коммутатора B (DHCP Relay):

1. Создайте VLAN 1 и настройте IP-адрес: 100.1.1.180;
2. Создайте VLAN 33 и настройте IP-адрес: 33.1.1.2;
3. Включите функцию задержки DHCP (DHCP delay) (см. рисунок 215);
4. Настройте IP-адрес DHCP-сервера: 100.1.1.156 (см. рисунок 215);

5. Включите глобальную функцию IP Source Guard (см. рисунок 316).

➢ Настройка коммутатора C (DHCP-клиент):

1. Создайте VLAN 33 и включите DHCP-клиент;
2. Коммутатор A назначит коммутатору C IP-адрес 33.0.0.1.

После получения IP-адреса коммутатором C записи таблицы IP Source Guard типа Relay можно просмотреть на коммутаторе B (см. рисунок 319).

2. Записи типа Snooping в таблице IP Source Guard

На схеме ниже показана следующая конфигурация:

Коммутатор A – DHCP-сервер,

Коммутатор B – устройство с включенным DHCP Snooping,

Коммутатор C – DHCP-клиент.

Порт 1 коммутатора A подключен к порту 1 коммутатора B, порт 2 коммутатора B – к порту 2 коммутатора C. DHCP-сервер и DHCP-клиент находятся в разных LAN.

После включения функции IP Source Guard на устройстве с DHCP Snooping клиент динамически получает IP-адрес и другие сетевые параметры через DHCP с использованием DHCP Snooping. В результате устройство формирует записи таблицы IP Source Guard типа Snooping.

Рисунок 321 – Конфигурация DHCP с функцией Snooping

➢ Настройка коммутатора A (DHCP-сервер):

1. Создайте VLAN 1 и настройте IP-адрес: 100.1.1.156;
2. Включите DHCP-сервер в VLAN 1 (см. рисунок 200);
3. Создайте пул адресов pool-1;
4. Выберите тип пула — Network, IP-адрес: 33.1.1.6, маска: 255.0.0.0.

➢ Настройка коммутатора B (устройство с DHCP Snooping):

1. Создайте VLAN 1 и настройте IP-адрес: 100.1.1.180;
2. Включите DHCP Snooping;
3. Настройте порт 1 как доверенный (trust port) (см. рисунок 211);
4. Включите глобальную функцию IP Source Guard (см. рисунок 316);
5. Включите IP Source Guard на порту 2 (см. рисунок 317).

➢ Настройка коммутатора C (DHCP-клиент):

1. Создайте VLAN 1 и включите DHCP-клиент;
2. Коммутатор A назначит коммутатору C IP-адрес 100.0.0.1.

После получения IP-адреса коммутатором C записи таблицы IP Source Guard типа Snooping можно просмотреть на коммутаторе B.

8.7 DDM

8.7.1 Введение

Цифровая диагностика – это эффективный метод мониторинга ключевых параметров работы оптических модулей. К контролируемым параметрам относятся:

- мощность передаваемого оптического сигнала,
- мощность принимаемого оптического сигнала,
- температура модуля,
- рабочее напряжение,
- ток смещения,
- информация о тревожных событиях.

С помощью функции цифровой диагностики оптический модуль предоставляет сетевому управляющему устройству возможность через двухпроводной последовательный интерфейс (I^2C-шину) в реальном времени получать данные о температуре, рабочем напряжении, токе смещения, мощности передаваемого и принимаемого оптического сигнала. Это позволяет своевременно контролировать состояние модуля и оперативно реагировать на возможные отклонения в работе.

8.7.2 Настройка с помощью WEB-интерфейса

1. Основная информация

Согласно указанному ниже пути, выберите [Basic Information], чтобы просмотреть основную информацию об оптическом модуле, вставленном в устройство, как показано на следующем рисунке.

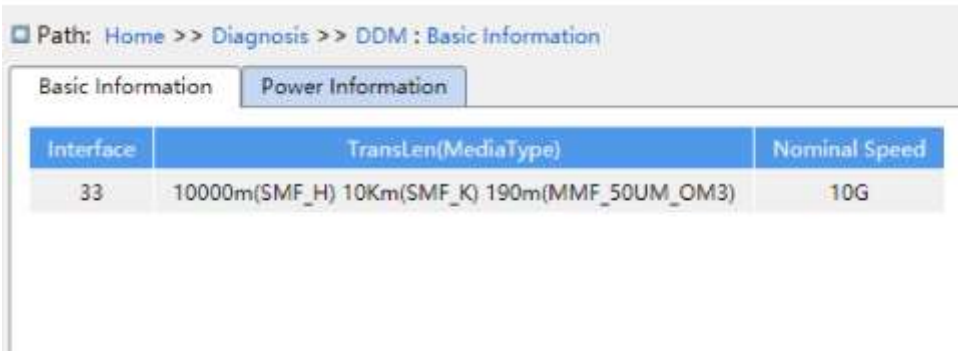


Рисунок 322 – Основная информация об оптическом модуле

2. Информация о мощности

Согласно указанному ниже пути, выберите [Power Information], чтобы просмотреть информацию об оптической мощности оптического модуля, как показано на рисунке ниже.

Рисунок 323 – Информация об оптической мощности оптического модуля

Расшифровка аббревиатур

AAA	Authentication Authorization and Accounting	Система аутентификации авторизации и учета событий
ABR	Area Border Router	Граничный маршрутизатор
ACL	Access Control List	Список управления доступом
AES	Advanced Encryption Standard	Симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит)
AS	Autonomous System	Автономная система
ASBR	Autonomous System Boundary Router	Граничный маршрутизатор автономной системы в OSPF
ARP	Address Resolution Protocol	Протокол определения MAC-адреса другого узла по известному IP-адресу
BDR	Backup Designated Router	Резервный выделенный маршрутизатор
BMC	Best Master Clock	Алгоритм выбора мастер-часов в сети
BootP	Bootstrap Protocol	Протокол, используемый для автоматического получения клиентом IP-адреса
BPDU	Bridge Protocol Data Unit	Блок данных протокола управления сетевыми мостами
BSR	BootStrap Router	Элемент в протоколе PIM, который служит в качестве централизованного узла, помогая автоматически обнаруживать и регистрировать многоадресные группы, а также управлять распределением многоадресных данных
CFI	Canonical Format Indicator	1-битное поле в заголовке IEEE 802.1Q, которое указывает формат кадра
CIST	Common and Internal Spanning Tree	Общее и внутреннее связующее дерево
CLI	Command Line Interface	Интерфейс командной строки
CoS	Class of Service	Класс сервиса

CRC	Cyclic Redundancy Check	Циклический избыточный код. Алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных
CST	Common Spanning Tree	Общее связующее дерево
DD	Database Description	Описание базы данных
DDM	Digital Diagnostics Monitoring	Функция цифрового контроля параметров производительности SFP-трансивера
DEI	Drop Eligible Indicator	Бит в теге VLAN, который указывает, может ли кадр быть отброшен в случае перегрузки сети
DES	Data Encryption Standard	Симметричный алгоритм блочного шифрования (размер блока 64 бита, ключ 56 бит)
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки узла
DHP	Dual Homing Protocol	Протокол, позволяющий подключить устройство к двум разным коммутаторам, обеспечивая резервирование подключения
DNS	Domain Name System	Система доменных имен
DP	Drop Precedence	Приоритет отбрасывания пакета (Class Selector поля DSCP)
DR	Designated Router	Назначенный маршрутизатор
DSAP	Destination Service Access Point	Точка доступа к сервису системы получателя (LLC)
DSCP	Differentiated Services Code Point	Точка кода дифференцированных услуг. Использует 6-битное поле 8-битного IP-заголовка DS
DST	Daylight Saving Time	Переход на летнее время
EAPOL	Extensible Authentication Protocol over LAN	Протокол определяющий способ инкапсуляции, который позволяет передавать пакеты EAP между запрашивающим устройством и

		аутентификатором в локальных проводных сетях
FCS	Frame Check Sequence	Часть кадра, содержащая контрольную сумму (CRC), используемую для проверки целостности данных внутри кадра
FTP	File Transfer Protocol	Протокол передачи файлов
GARP	Generic Attribute Registration Protocol	Протокол регистрации основных атрибутов
GMRP	GARP Multicast Registration Protocol	Протокол GARP для регистрации многоадресных групп
GVRP	GARP (Generic) VLAN Registration Protocol	Протокол GARP для регистрации VLAN
HTTP	Hyper Text Transfer Protocol	Протокол передачи гипертекста
HTTPS	Hypertext Transfer Protocol Secure	Безопасный протокол передачи гипертекста
ICMP	Internet Control Message Protocol	Протокол межсетевых управляющих сообщений
IGMP	Internet Group Management Protocol	Протокол управления многоадресной передачей данных в сетях, основанных на протоколе IP. Используется только в сетях IPv4. Аналогичную роль в стеке протоколов IPv6 выполняет протокол MLD
IGMP Snooping	Internet Group Management Protocol Snooping	Протокол отслеживания сетевого трафика IGMP
IP	Internet Protocol	Интернет-протокол
IST	Internal Spanning Tree	Внутреннее связующее дерево
LACP	Link Aggregation Control Protocol	Протокол агрегирования каналов
LAN	Local Area Network	Локальная сеть
LLC	Logical Link Control	Подуровень канального уровня, отвечающий за управление логическими соединениями, кадрами и контроль ошибок, обеспечивая интерфейс между сетью и MAC-подуровнем

LLDP	Link Layer Discovery Protocol	Протокол обнаружения канального уровня
LLDPDU	Link Layer Discovery Protocol Data Unit	Блок данных протокола обнаружения канального уровня
LSA	Link State Advertisement	Сообщение с описанием локального состояния маршрутизатора или сети
LSAck	Link State Acknowledgment	Пакет подтверждения состояния канала
LSDB	Link State Database	База данных о состоянии каналов
LSR	Link State Request	Пакет запроса о состоянии канала
LSU	Link State Update	Пакет подтверждения состояния канала
MDR	Message Delay Request	Параметр в настройках Precision Time Protocol (PTP), который используется для запроса информации о задержке сообщений.
MIB	Management Information Base	Виртуальная база данных, используемая для управления объектами в сети связи
MST	Multiple Spanning Tree	Множественное связующее дерево
MSTI	Multiple Spanning Tree Instance	Экземпляр множественного связующего дерева
MSTP	Multiple Spanning Tree Protocol	Протокол множественного связующего дерева
MTU	Maximum Transmission Unit	Максимальный размер передаваемого кадра
NAD	Network Access Device	Устройство сетевого доступа
NAS	Network Access Server	Сервер сетевого доступа
NAT	Network Address Translator	Транслятор сетевых адресов
NBMA	Non-Broadcast Multi-Access	Сеть множественного доступа без широковещательных доменов, в которой подключено несколько хостов, но данные передаются только напрямую от одного компьютера к другому по виртуальному каналу или через коммутаторы

NetBIOS	Network Basic Input/Output System	Базовая сетевая система ввода-вывода
NIS	Network Information Service	Протокол службы каталогов для распределения данных конфигурации системы (имен пользователей и хостов) между компьютерами в сети
NMS	Network Management System	Система сетевого управления
NSSA	Not-So-Stubby Area	Область OSPF, позволяющая ограниченно распространять внешние маршруты через Type 7 LSA.
NTP	Network Time Protocol	Протокол синхронизации сетевого времени
OID	Object Identifier	Идентификатор объекта
OLT	Optical Line Terminal	Центральный узел, который управляет и контролирует передачу данных по оптической сети и обеспечивает связь между оптической сетью и клиентскими устройствами
OSPF	Open Shortest Path First	Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и передающий информацию по наилучшему пути
PCP	Priority Code Point	Поле в теге VLAN, которое указывает приоритет кадра. Используется для определения уровня приоритета трафика и может принимать значения от 0 (низкий) до 7 (высокий)
PD	Powered Device	Устройство, получающее электропитание через витую пару по технологии PoE
PID	Protocol Identifier	Идентификатор протокола (в кадре Ethernet версии 802.3)
PIM	Protocol Independent Multicast	Протокол независимой многоадресной рассылки
PoE	Power over Ethernet	Технология подачи электропитания на клиентское устройство через витую пару стандарта Ethernet

PSE	Power Sourcing Equipment	Оборудование, передающее электропитание другим устройствам
PTP	Precision Time Protocol	Протокол точного времени
PVID	Port VLAN Identifier	Идентификатор VLAN по умолчанию для порта
PVLAN	Private VLAN	Частная виртуальная локальная сеть
QCE	QoS Control Entry	Запись списка управления QoS, содержащая правила классификации
QCL	QoS Control List	Список управления QoS
QoS	Quality of Service	Качество обслуживания (технология предоставления различным классам трафика различных приоритетов в обслуживании)
RADIUS	Remote Authentication Dial-In User Service	Служба удаленной аутентификации пользователей по коммутируемым линиям
RARP	Reverse Address Resolution Protocol	Протокол определения IP-адреса другого узла по известному MAC-адресу
RID	Router ID	Идентификатор маршрутизатора
RIP	Routing Information Protocol	Протокол дистанционно-векторной маршрутизации
RMON	Remote Network Monitoring	Дистанционный мониторинг сети (расширение SNMP, разработанное IETF)
RPF	Reverse Path Forwarding	Проверка обратного пути передачи
RSTP	Rapid Spanning Tree Protocol	Быстрый протокол связующего дерева (версия протокола STP с ускоренной реконфигурацией дерева)
Rx	Receive	Контакт коннектора для приема данных
SFP	Small Form-factor Pluggable	Промышленный стандарт модульных компактных приемопередатчиков (трансиверов), используемых для передачи и приема данных в телекоммуникациях

SNAP	Subnetwork Access Protocol	Поле заголовка LLC, указывающее протокол сетевого уровня, которому должен быть передан кадр
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 упроще нной реализацией протокола NTP)
SSAP	Destination Service Access Point	Точка доступа к сервису системы источника (LLC)
SSH	Secure Shell	«Безопасная оболочка», сетевой протокол прикладного уровня
SSL	Secure Sockets Layer	Уровень защище нных сокетов; криптографический протокол, который отвечает за безопасную передачу данных на сеансовом уровне
STP	Spanning Tree Protocol	Протокол связующего дерева
SYSLOG	System Log	Протокол передачи сообщений системного журнала от устройств к серверу
TACACS+	Terminal Access Controller Access Control System	Сеансовый протокол аутентификации, авторизации и учета доступа
TCN	Topology Change Notification	Сообщение об изменении топологии сети
TCP	Transmission Control Protocol	Протокол управления передачей
TFTP	Trivial File Transfer Protocol	Простой протокол передачи файлов
TTL	Time to Live	Предельный период времени или число итераций (переходов), которые пакет данных может осуществить (прожить) до своего исчезновения
Tx	Transmit	Контакт коннектора для передачи данных
UDP	User Datagram Protocol	Протокол пользовательских дейтаграмм
USM	User-Based Security Model	Модель безопасности на основе

		пользователей
UTC	Universal Coordinated Time	Глобальное время, которое используется для координации времени во всем мире
VLAN	Virtual Local Area Network	Виртуальная локальная сеть
VLSM	Variable Length Subnet Mask	Маска подсети с переменной длиной
VRRP	Virtual Router Redundancy Protocol	Протокол резервирования «Виртуальный маршрутизатор»
WRR	Weighted Round Robin	Взвешенная очередь