SYMANITRON

Инновационные
промышленные сети

SEWM54G
управляемый коммутатор L3

Руководство CLI

интерфейс
командной строки

Оглавление

Введение

В руководстве описаны режимы доступа и программные функции коммутаторов серии SEWM54G, а также приводится детальная информация по их настройке с помощью интерфейса командной строки.

Условные обозначения

1. Условные обозначения в тексте

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

2. Условные обозначения CLI

Формат	Описание
Bold	Означает команды и ключевые слова. Например, **show version** будет показываться с использованием шрифта **Bold**
Italic	Параметры, для которых вы указываете значения, выделены курсивом. Например, для команды **show vlan** *vlan id* необходимо указать фактическое значение идентификатора 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. Подготовка к настройке

В данной главе описываются следующие подготовительные работы перед первой настройкой коммутатора:

- номер порта коммутатора;
- подготовка коммутатора к запуску;
- получение помощи;
- командный режим;
- отмена команды;
- сохранение конфигурации.

1.1 Номер порта коммутатора

Физический порт коммутатора нумеруется в формате **<type><slot>/<port>**. Таблица преобразования типа в имя выглядит следующим образом:

Тип интерфейса	Имя	Упрощенное имя
10M Ethernet	Ethernet	e
100M fast Ethernet	FastEthernet	f
1000M Ethernet	GigaEthernet	g

Номер слота расширения для маркировки и настройки портов должен быть равен **0**. Другие слоты расширения нумеруются слева направо, начиная с **1**.

Порты в одном слоте расширения нумеруются в порядке снизу вверх и слева направо, начиная с **1**. Если существует только один порт, его номер равен **1**.

Порты в модулях каждого вида должны быть последовательно пронумерованы снизу вверх и слева направо.

1.2 Подготовка к запуску коммутатора

Перед настройкой коммутатора выполните следующие подготовительные работы:

1. Настройте оборудование коммутатора в соответствии с требованиями руководства.
2. Настройте программу моделирования терминала на ПК.
3. Определите структуру IP-адресов для сетевых протоколов IP.

1.3 Получение помощи

Используйте знак вопроса (?) и знак направления для облегчения ввода команд:

- Введите вопросительный знак. Отобразится текущий список доступных команд.
- Switch> ?
- Введите несколько знакомых символов и нажмите клавишу пробела. Отобразится список доступных команд, начиная с введенных знакомых символов.
- Switch> s?
- Введите команду, нажмите клавишу пробела и введите вопросительный знак. Отобразится список параметров команды.
- Switch> show ?
- Нажмите клавишу «вверх», чтобы отобразить ранее введенные команды. Продолжайте нажимать клавишу «вверх», и отобразятся дополнительные команды. После этого нажмите клавишу «вниз», и под текущей командой отобразится следующая вводимая команда.

1.4 Командные режимы

Интерфейсы командной строки для коммутатора можно разделить на несколько режимов. Каждый командный режим позволяет настраивать различные группы программ. Команда, которую можно использовать в настоящее время, зависит от командного режима, в котором вы находитесь. Вы можете ввести знак вопроса в различных командных режимах, чтобы получить доступный список команд. Наиболее распространенные режимы перечислены в следующей таблице:

Командный режим	Способ входа	Подсказка	Способ выхода
Режим системного мониторинга	Введите **Ctrl-p** после включения питания	monitor#	Выполните **quit**
Пользовательский режим	Аутентификация пользователя	Switch>	Выполните **exit** или **quit**
Режим управления (привилегированный режим EXEC)	Введите **enter** или **enable** в пользовательском режиме	Switch#	Выполните **exit** или **quit**

Режим глобальной конфигурации (общая настройка коммутатора)	Введите **config** в режиме управления	Switch_config#	Выполните **exit** или **quit** или введите **Ctrl-z**, чтобы вернуться в режим управления
Режим настройки интерфейса	Введите команду **interface** в режиме глобальной конфигурации, например, **interface f0/1**	Switch_config_f0/1#	Выполните **exit** или **quit** или введите **Ctrl-z**, чтобы вернуться в режим управления

Для каждого режима существует определенный набор команд, с которыми он может работать. Если при вводе команд возникает проблема, проверьте подсказку и введите вопросительный знак, чтобы получить список команд, доступных для текущего режима. Проблема может возникнуть при запуске в неправильном командном режиме или при неправильном написании команды.

В следующем примере показано изменение подсказки интерфейса относительно выбранного командного режима:

```
Switch> enter
Password: <enter password>
Switch# config
Switch_config# interface f0/1
Switch_config_f0/1# quit
Switch_config# quit
Switch#
```

1.5 Отмена команды

Чтобы отменить команду или восстановить ее функции по умолчанию, перед большинством команд можно добавить ключевое слово **no**. Например:

no ip routing

1.6 Сохранение конфигурации

На случай перезапуска системы или внезапного отключения питания рекомендуется периодически сохранять текущую конфигурацию. Это поможет быстро восстановить ее. Вы

можете выполнить **write** для сохранения настроек в режиме управления или в режиме глобальной конфигурации.

2. Настройка управления системой

2.1 Настройка управления файлами

2.1.1 Управление файловой системой

Имя файла во флеш-памяти состоит не более чем из 20 символов. Имена файлов нечувствительны к регистру.

2.1.2 Команды для файловой системы

Жирным шрифтом во всех командах выделены ключевые слова. Остальные слова и символы – это параметры. Содержимое квадратных скобок «[]» не является обязательным.

Команда	Описание
format	Форматирует файловую систему и удаляет все данные
dir [filename]	Отображает имена файлов и каталогов. Имя файла в скобках «[]» означает отображение файлов, начинающихся с нескольких букв. Файл отображается в следующем формате: Index number file name <FILE> lengthestablished time, где: 1. Index number – порядковый номер файла 2. File name – имя файла 3. <FILE> – это обозначение типа файла, которое может быть использовано для идентификации типа файла в системе 4. Length – длина файла в байтах 5. Established time – время создания файла
delete filename	Удаляет файл. Система подскажет, если файл не существует
md dirname	Создает каталог
rd dirname	Удаляет каталог. Система предложит, если каталог не существует
more filename	Отображает содержимое файла. Если содержимое файла не может быть отображено на одной странице, оно будет отображено на

	нескольких
cd	Изменяет текущую директорию. Позволяет перейти в другую директорию или подкаталог, где хранятся файлы
pwd	Отображает текущий путь

2.1.3 Запуск из файла вручную

monitor# boot flash <*local_filename*>

Данная команда предназначена для запуска программного обеспечения коммутатора во флеш-памяти, которая может содержать несколько различных программ для коммутатора.

- Параметры

Параметр	Описание
Flash	Файл, хранящийся во флеш-памяти
local_filename	Имя файла, сохраненное во флеш-памяти. Пользователи должны ввести имя файла

- Пример

monitor# boot flash switch.bin

2.1.4 Обновление программного обеспечения

Пользователь может использовать эту команду для загрузки системного программного обеспечения коммутатора локально или удаленно, чтобы получить обновление версии или пользовательскую версию, содержащую определенную функцию (например, шифрование данных и т. д.).

Обновления программного обеспечения осуществляется в режиме системного мониторинга.

- Загрузка файла при помощи TFTP: monitor# copy tftp flash: [ip_addr]

Данная команда предназначена для копирования файла с tftp-сервера на флеш-память в системе. После ввода команды система предложит ввести имя удаленного сервера и имя удаленного файла.

- Параметры

Параметр	Описание
flash	Устройство хранения – флеш-память

ip_addr	IP-адрес tftp-сервера Если IP-адрес не указан, система предложит ввести IP-адрес после запуска команды **copy**

➢ Пример

В следующем примере показано, как файл main.bin считывается с сервера, записывается на носитель коммутатора и переименовывается в switch.bin.

monitor# copy tftp flash

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

please wait ...

##
##
##
##
##
##

TFTP: successfully receive 3377 blocks, 1728902 bytes

monitor#

2.1.5 Обновление конфигурации

Конфигурация коммутатора сохраняется в виде файла с именем «startup-config». Для обновления конфигурации используются те же команды, что и для обновления программного обеспечения.

monitor# copy tftp flash startup-config

2.1.6 Обновление при помощи FTP

switch# copy ftp {flash|cf} [ip_addr|option]

Для обновления программного обеспечения и конфигурации в режиме управления можно использовать FTP. Введите команду **copy** для загрузки файла с FTP-сервера на коммутатор, а также для выгрузки файла из файловой системы коммутатора на FTP-сервер. После ввода команды система предложит ввести имя удаленного сервера и имя удаленного файла.

copy{**ftp**:[[[//login-name:[login-password]@]location]/directory]/filename}|{**flash**<:filename>}
{{**flash**<:filename>}|**ftp**:[[[//login-name: [login-password]@]location] /directory]/filename}
<blksize> <mode> <type>

➢ Параметры

Параметр	Описание
login-name	Имя пользователя FTP-сервера Если имя пользователя не указано, система предложит вам ввести его после запуска команды **copy**
login-password	Пароль пользователя FTP-сервера Если пароль пользователя не указан, система предложит вам ввести его после запуска команды **copy**
nchecksize	Размер файла не проверяется на сервере
blksize	Размер блока передаваемых данных Значение по умолчанию: 512
ip_addr	IP-адрес FTP-сервера Если IP-адрес не указан, система предложит ввести его после запуска команды **copy**
active	Означает подключение FTP-сервера в активном режиме
passive	Означает подключение FTP-сервера в пассивном режиме
type	Установить режим передачи данных (ascii или binary)

➢ Пример

В следующем примере показано, как файл main.bin считывается с сервера, записывается на носитель коммутатора и переименовывается в switch.bin.

config# copy ftp flash

Prompt: ftp user name[anonymous]? login-name

Prompt: ftp user password[anonymous]? login-password

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

или

config# copy ftp://login-name:login-password@192.168.20.1/main.bin flash:switch.bin

##

##

FTP:successfully receive 3377 blocks ,1728902 bytes

config#

1) Когда FTP-сервер не работает, время ожидания увеличивается. Если эта проблема вызвана временем ожидания TCP (значение по умолчанию – 75 с), вы можете глобально применить команду **ip tcp synwait-time** для изменения времени подключения TCP. Однако использовать эту функцию не рекомендуется.

2) При использовании FTP в некоторых сетевых условиях скорость передачи данных может быть относительно низкой. Вы можете должным образом настроить размер блока передачи для получения наилучшего эффекта. Размер по умолчанию – 512 символов, что гарантирует относительно высокую скорость работы в большинстве сетей.

2.2 Базовые настройки управления системой

2.2.1 Настройка IP-адреса Ethernet

monitor# ip address <*ip_addr*> <*net_mask*>

Эта команда предназначена для настройки IP-адреса Ethernet. IP-адрес по умолчанию – 192.168.0.1, маска подсети – 255.255.255.0.

- Параметры

Параметр	Описание
ip_addr	IP-адрес Ethernet
net_mask	Маска подсети Ethernet

- Пример

monitor# ip address 192.168.1.1 255.255.255.0

2.2.2 Настройка маршрута по умолчанию

monitor# ip route default <ip_addr>

Эта команда используется для настройки маршрута по умолчанию. Можно настроить только один маршрут по умолчанию.

- Параметры

Параметр	Описание
ip_addr	IP-адрес шлюза по умолчанию

➢ Пример

monitor# ip route default 192.168.1.1

2.2.3 Команда ping

monitor# ping <*ip_address*>

Эта команда предназначена для проверки состояния сетевого подключения.

➢ Параметры

Параметр	Описание
ip_address	IP-адрес получателя

➢ Пример

monitor# ping 192.168.20.100

PING 192.168.20.100: 56 data bytes

64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms

----192.168.20.100 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

3. Настройка терминала

3.1 Введение

Система использует команду **line** для настройки параметров терминала. С помощью нее можно настроить ширину и высоту, отображаемые терминалом.

В системе есть четыре типа линий: консоль, aid (асинхронный ввод-вывод), асинхронный и виртуальный терминал. Разные системы имеют разное количество линий этих типов.

Обратитесь к руководству по настройке программного и аппаратного обеспечения для правильной настройки.

Тип линии	Интерфейс	Описание	Нумерация
CON(CTY)	Консоль	Для входа в систему с целью настройки.	0
VTY	Виртуальный и асинхронный	Для подключения Telnet, X.25 PAD, HTTP и Rlogin синхронных портов (таких как Ethernet и последовательный порт) в системе	32 номера, начиная с 1

3.2 Связь между линией и интерфейсом

1. Связь между синхронным интерфейсом и линией VTY

Линия виртуального терминала обеспечивает синхронный интерфейс для доступа к системе. Когда вы подключаетесь к системе через линию VTY, вы фактически подключаетесь к виртуальному порту на интерфейсе. Для каждого синхронного интерфейса может быть много виртуальных портов.

Например, если к интерфейсу (Ethernet или последовательному порту) подключаются несколько Telnet, вам необходимо выполнить следующие шаги для настройки VTY:

- войти в режим настройки линии;
- настроить параметры терминала.

3.3 Мониторинг и обслуживание

Запустите **showline**, чтобы проверить конфигурацию VTY.

3.4 Пример настройки VTY.

Данный пример показывает, как отменить ограничение количества строк на экране для всех VTY без запросов **more**:

```
Switch_config# line vty 0 31
Switch_config_line# length 0
```

4. Команды настройки SSH

4.1 Введение

Безопасное и зашифрованное коммуникационное соединение может быть создано между клиентом SSH и устройством через сервер SSH. Соединение имеет telnet-подобные функции. Сервер SSH поддерживает алгоритмы шифрования, включая des, 3des и blowfish.

SSH-клиент – это приложение, работающее по протоколу SSH. Клиент SSH может обеспечивать аутентификацию и шифрование, поэтому он гарантирует безопасную связь между коммуникационными устройствами или устройствами, поддерживающими сервер SSH, даже если эти устройства работают в небезопасных сетевых условиях. Клиент SSH поддерживает алгоритмы шифрования, включая des, 3des и blowfish.

SSH-сервер и SSH-клиент поддерживают версию 1.5. Оба они поддерживают только приложение оболочки.

4.2 Задачи настройки

4.2.1 Настройка списка методов аутентификации

SSH-сервер использует режим аутентификации по логину и паролю. По умолчанию он использует список методов аутентификации **default**.

Выполните следующую команду в командном режиме глобальной конфигурации, чтобы настроить список методов аутентификации:

Команда	Описание
ip sshd auth_method STRING	Настраивает список методов аутентификации Длина имени метода аутентификации не более 20 символов

4.2.2 Настройка списка контроля доступа

Чтобы контролировать доступ к SSH-серверу устройства, необходимо настроить для него список контроля доступа.

Для настройки списка выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
ip sshd access-class STRING	Настраивает список контроля доступа Длина имени списка контроля доступа не более 19 символов

4.2.3 Настройка времени ожидания аутентификации

После установления соединения между клиентом и сервером сервер прерывает соединение, если аутентификация не может быть подтверждена в течение установленного времени.

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить значение времени ожидания аутентификации:

Команда	Описание
ip sshd timeout <60-65535>	Настраивает значение для времени ожидания аутентификации

4.2.4 Настройка количества повторных попыток аутентификации

Если количество неудачных попыток аутентификации превышает установленное максимальное количество, SSH-сервер не позволит вам повторить аутентификацию, пока не будет создано новое соединение. По умолчанию максимальное количество повторных попыток аутентификации равно 6.

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить максимальное количество повторных попыток аутентификации:

Команда	Описание
ip sshd auth-retries <0-65535>	Настраивает максимальное количество повторных попыток аутентификации

4.2.5 Настройка периода молчания при входе в систему

Когда количество неудачных попыток входа в систему превышает пороговое значение, устройство переходит в режим молчания. Продолжительность периода этого режима – 60 с.

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить период молчания при входе:

Команда	Описание
ip sshd silence-period <0-3600>	Настраивает период молчания при входе

4.2.6 Включение SFTP

SFTP – это защищенный протокол передачи файлов, основанный на протоколе SSH, аутентификация и передача данных которого зашифрованы. Хотя его скорость передачи низкая, он имеет надежную сетевую безопасность.

SFTP отключен по умолчанию. Выполните следующую команду в режиме глобальной конфигурации, чтобы включить SFTP:

Команда	Описание
ip sshd sftp	Включает SFTP

4.2.7 Включение SSHD

Расчет начального пароля при включении SSH-сервера занимает одну-две минуты. Начальный пароль будет сохранен во флеш-памяти при включении функции. Устройство будет считывать ключ шифрования из флеш-памяти при повторном включении SSH-сервера. Таким образом, время инициализации сокращается.

SSHD (сохранение ключа шифрования) по умолчанию отключен. Выполните следующую команду, чтобы включить SSHD в режиме глобальной конфигурации:

Команда	Описание
ip sshd save	Включает SSHD

4.2.8 Включение SSH-сервера

SSH-сервер по умолчанию отключен. Когда сервер SSH включен, устройство будет генерировать пару ключей RSA, а затем прослушивать запросы на подключение от клиента. Процесс занимает одну-две минуты.

Выполните следующую команду в режиме глобальной конфигурации, чтобы включить сервер SSH:

Команда	Описание
ip sshd enable	Включает SSH-сервер. Длина пароля – 1024 бита

4.3 Пример настройки SSH-сервера

Следующая конфигурация разрешает доступ к SSH-серверу только хосту с IP-адресом 192.168.20.40. Локальная база данных пользователей используется для распознавания идентификатора пользователя.

Настройка список контроля доступа:

```
ip access-list standard ssh-acl
permit 192.168.20.40
```

Общая настройка:

```
aaa authentication login ssh-auth local
ip sshd auth-method ssh-auth
ip sshd access-class ssh-acl
ip sshd enable
```

5. Настройка управления сетью

5.1 SNMP

5.1.1 Введение

Система SNMP включает следующие компоненты:

- система управления SNMP (NMS);
- агент SNMP (AGENT);
- информационная база управления (MIB).

SNMP – это протокол управления сетевыми устройствами через TCP/IP, работающий на прикладном уровне. С помощью него NMS и агенты обмениваются пакетами данных для управления сетью.

Система управления SNMP может быть частью системы управления сетью. Агент и MIB хранятся в системе. Перед настройкой SNMP в системе необходимо определить взаимосвязь между системой управления сетью и агентом.

Агент SNMP содержит переменные MIB. Система управления SNMP может проверять или изменять значения этих переменных. Система управления может получить значение переменной от агента или сохранить значение переменной для агента. Агент собирает данные из MIB. MIB – это база данных параметров устройства и сетевых настроек. Агент также может реагировать на загрузку системы управления или запрос на настройку данных. Агент SNMP может отправлять прерывания в систему управления. Агенты отправляют в

NMS trap-сообщения, содержащие информацию о тревоге при определенном состоянии сети. trap-сообщение может указывать на неправильную аутентификацию пользователя, перезагрузку, состояние канала связи (включено или выключено), закрытие TCP-соединения, потерю соединения с соседними системами или другие важные события.

1. SNMP-уведомление

Когда происходят какие-то особые события, система отправляет информационные сообщения в NMS. Например, когда агент обнаруживает ненормальное состояние сети, он отправляет информацию в систему управления.

SNMP-уведомления можно рассматривать как trap-сообщения или информационные запросы (inform request). Поскольку принимающая сторона не отправляет никакого ответа при получении trap-сообщения, это приводит к тому, что принимающая сторона не может быть уверена, что сообщение было получено. Поэтому система уведомлений посредством trap-сообщений ненадежна. Для сравнения, система управления SNMP, которая получает информационный запрос, использует PDU, который SNMP отображает в качестве ответа на эту информацию. Если в NMS не получен информационный запрос, эхо-ответ не будет отправлен. Если принимающая сторона не отправляет никакого ответа, агент может повторно отправить информационный запрос. Так уведомления в конечном итоге достигают своего назначения.

Поскольку информационные запросы более надежны, они потребляют больше ресурсов системы и сети. trap-сообщение удаляется после отправки. Информационный запрос должен храниться в памяти до тех пор, пока не будет получено эхо или не истечет время ожидания. Кроме того, «trap» отправляется только один раз, а «inform request» может быть повторно отправлен много раз. Повторная отправка запроса создает дополнительную коммуникационную активность и увеличивает нагрузку на сеть. Таким образом, чередование отправки сообщений типа «trap» и «inform request» обеспечивает баланс между надежностью и использованием ресурсов. Если системе управления SNMP очень важно получать каждое уведомление, имеет смысл использовать информационный запрос. Если приоритет отдается количеству коммуникационных сообщений в сети, и нет необходимости получать каждое уведомление, то можно использовать trap.

Данный коммутатор поддерживает только trap-сообщения, но для него может быть предоставлено расширение, позволяющее отправлять запросы типа «inform request».

2. Версия SNMP

Система поддерживает следующие версии SNMP:

- SNMPv1 – простой протокол управления сетью, полный интернет-стандарт, определенный в документе сетевых стандартов RFC1157.
- SNMPv2C – архитектура управления, основанная на группах. Интернет-стандарт протокола для тестирования, который определен в документе сетевых стандартов RFC1901.

Данный коммутатор 3-го уровня также поддерживает следующие NMP:

- SNMPv3 – простой протокол управления сетью версии 3, определенный в RFC3410.

SNMPv1 использует групповой формат безопасности. Используйте список управления доступом к IP-адресу и пароль, чтобы определить группу NMS, которая может получить доступ к MIB агента.

SNMPv3 обеспечивает безопасный доступ к устройствам за счет комбинации проверки подлинности и шифрования пакетов по сети.

В SNMPv3 реализованы следующие функции безопасности:

- целостность сообщения – гарантия того, что пакет не был изменен при передаче;
- аутентификация – определение того, что сообщение получено из достоверного источника;
- шифрование – шифрование содержимого пакета предотвращает его просмотр неавторизованным источником.

SNMPv3 обеспечивает как модели безопасности, так и уровни безопасности. Модель безопасности – это стратегия проверки подлинности, настроенная для пользователя и группы, в которой находится пользователь. Уровень безопасности – это допустимый уровень безопасности в рамках текущей модели. Сочетание модели безопасности и уровня безопасности определяет, какой механизм безопасности используется при обработке SNMP-пакета. Доступны три модели безопасности, то есть аутентификация и шифрование, аутентификация и отсутствие шифрования, отсутствие аутентификации.

Вам необходимо настроить агент SNMP на версию SNMP, которую поддерживает рабочая станция управления. Агент может общаться со многими NMS.

3. Поддерживаемая MIB

SNMP данной системы поддерживает все переменные MIBII (RFC 1213) и trap-сообщения SNMP (RFC 1215).

Для каждой системы предоставляется собственное расширение MIB.

5.1.2 Настройка SNMP

Задачи настройки

- Настройка представления SNMP
- Создание или изменение контроля доступа для SNMP-комьюнити
- Настройка способа связи системного администратора и системы
- Определение максимальной длины пакета данных агента SNMP
- Мониторинг состояния SNMP
- Настройка локального ядра SNMP
- Настройка trap-сообщений SNMP
- Настройка группы SNMPv3
- Настройка пользователя SNMPv3

- Настройка шифрования SNMP-сервера
- Настройка источника trap-сообщений SNMP-сервера
- Настройка времени ожидания trap-сообщений SNMP-сервера
- Настройка SNMP-сервера для отправки trap-сообщений на указанный хост с использованием имен хостов
- Настройка trap-логов SNMP-сервера
- Настройка количества повторных сообщений
- Настройка времени поддержания активности
- Настройка кодирования SNMP-сервера
- Настройка идентификатора события SNMP-сервера
- Настройка тайм-аута для SNMP-запросов getBulk
- Настройка задержки для SNMP-запросов getBulk
- Отображение информации о работе SNMP
- Отображение отладочной информации SNMP

5.1.2.1 Настройка представления SNMP

Представление SNMP предназначено для регулирования прав доступа (включение или исключение) для MIB. Используйте следующую команду для настройки представления SNMP:

Команда	Описание
snmp-server view *name oid* [**excluded** | **included**]	Добавляет поддерево или таблицу определяемой идентификатором OID базы MIB в SNMP-представление. **included**: включить указанные объекты; **excluded**: исключить указанные объекты

Подмножества, к которым можно получить доступ в представлении SNMP, включают переменные, называемые управляемыми объектами или MIB-объектами. Они представляют характеристики сетевых устройств, такие как имя системы, время перезагрузки, количество интерфейсов и IP-адреса. Доступ к этим объектам осуществляется через идентификаторы объектов (OID), которые представляют собой иерархическую структуру с уникальными идентификаторами для каждого объекта. Объекты, которые не настроены, по умолчанию недоступны.

После создания и настройки представления SNMP вы можете добавить его к конфигурации определенной группы, чтобы ограничить доступ этой группы только к тем объектам, которые разрешены в соответствующем SNMP-представлении.

5.1.2.2 Создание или изменение контроля доступа для SNMP-комьюнити

Строку символов комьюнити SNMP можно использовать для определения связи между управляющей системой SNMP и агентом. Строка символов комьюнити аналогична паролю, который позволяет системе доступа войти в агент. Вы можете указать одно или несколько свойств, относящихся к строке комьюнити. Эти свойства являются необязательными:

- разрешение использовать строку символов комьюнити для получения списка доступа по IP-адресу в системе управления SNMP;
- определение представлений MIB всех подмножеств объектов MIB, которые могут получить доступ к указанному комьюнити;
- указание комьюнити с правами на чтение и запись доступных объектов MIB.

Настройте строку символов комьюнити в режиме глобальной конфигурации с помощью следующей команды:

Команда	Описание
snmp-server community [**0**|**7**] *string* [**view** *view-name*] [**ro** | **rw**] [*word*]	Определяет строку символов группового доступа

Вы можете настроить одну или несколько строк символов группы. Запустите команду **no snmp-server community**, чтобы удалить указанную строку комьюнити.

5.1.2.3 Настройка способа связи системного администратора и местоположения системы

SysContact и sysLocation – это переменные управления в системной группе MIB, соответственно определяющие идентификатор оператора связи и фактическое местоположение контролируемого узла. Доступ к этой информации можно получить через config-файлы. Вы можете использовать следующие команды в режиме глобальной конфигурации:

Команда	Описание
snmp-server contact *text*	Задает строку символов для описания контактного лица узла
snmp-server location *text*	Задает строку символов для описания местонахождения узла

5.1.2.4 Определение максимальной длины пакета данных агента SNMP

Когда агент SNMP получает запросы или отправляет ответы, вы можете настроить максимальную длину пакета данных. Используйте следующую команду в режиме глобальной конфигурации:

Команда	Описание
snmp-server packetsize *byte-count*	Задает максимальный размер пакета

5.1.2.5 Мониторинг состояния SNMP

Вы можете запустить следующую команду в режиме глобальной конфигурации, чтобы отслеживать статистику вывода/ввода SNMP, включая недопустимые элементы строки символов сообщества, количество ошибок и переменные запроса.

Команда	Описание
show snmp	Отслеживание состояния SNMP

5.1.2.6 Настройка локального ядра SNMP

Используйте следующую команду, чтобы настроить систему для отправки локального ядра SNMP:

Команда	Описание
snmp-server engineID local *engineID*	Настройка локального ядра SNMP

5.1.2.7 Настройка SNMP Trap

Используйте следующую команду, чтобы настроить систему для отправки trap-сообщений (вторая задача не является обязательной):

- Настройка системы для отправки

Запустите следующие команды в режиме глобальной конфигурации, чтобы настроить систему для отправки сообщений на хост:

Команда	Описание
snmp-server host | **hostv6** host community-string [trap-type]	Указывает получателя trap-сообщения

snmp-server host | **hostv6** *host* [**vrf** *word*] [**udp-port** *port-num*] [**permit** | **deny** *event- id*] {{**version** [**v1** | **v2c** | **v3**]} | {[**informs** | **traps**] | [auth | noauth]}} *community-string/user* [**authentication** | **configure** | **snmp**]	Указывает получателя, номер версии и имя пользователя для trap-сообщения

При запуске системы автоматически запускается агент SNMP. Активируются все типы trap-сообщений. Вы можете использовать команду **snmp-server host**, чтобы указать, какой хост будет получать какие сообщения.

Некоторыми сообщениями нужно управлять с помощью других команд. Например, если вы хотите, чтобы сообщения о состоянии связи SNMP отправлялись при открытии или закрытии интерфейса, вам нужно запустить **snmp trap link-status** в режиме настройки интерфейса. Чтобы закрыть эти trap-сообщения, запустите команду **snmp trap link-stat**.

Вы должны настроить команду **snmp-server host**, чтобы хост получал trap-сообщения.

- Изменение текущего параметра trap-сообщения

В качестве необязательного элемента можно указать исходный интерфейс, на котором возникают сообщения, длину очереди сообщений или значение интервала повторной отправки для каждого хоста.

Чтобы изменить параметры trap-сообщений, вы можете запустить следующие необязательные команды в режиме глобальной конфигурации:

Команда	Описание
snmp-server trap-source *interface*	Определяет исходный интерфейс, на котором создаются trap-сообщения, и задает для них исходный IP-адрес
snmp-server queue-length *length*	Создает длину очереди сообщений для каждого хоста, имеющего Trap. Значение по умолчанию: 10
snmp-server trap-timeout *seconds*	Определяет частоту отправки trap-сообщений в очереди повторной отправки. Значение по умолчанию: 30 секунд

5.1.2.8 Настройка адреса источника привязки SNMP

Выполните следующую команду в режиме глобальной конфигурации, чтобы задать исходный адрес для сообщения SNMP:

Команда	Описание
snmp source-addr *ipaddress*	Устанавливает исходный адрес для сообщений SNMP

5.1.2.9 Настройка UDP-порта SNMP-сервера

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить UDP-порт SNMP-сервера:

Команда	Описание
snmp-server udp-port *portnum*	Указывает номер UDP-порта SNMP-сервера

5.1.2.10 Настройка группы SNMPv3

Выполните следующую команду, чтобы настроить группу:

Команда	Описание
snmp-server group [*groupname* {**v3** [**auth** | **noauth** | **priv**]}] [**read** readview] [**write** writeview] [**notify** notifyview] [**access** access-list]	Настройка группы SNMPv3. По умолчанию доступно только чтение элементов поддерева

5.1.2.11 Настройка пользователя SNMPv3

Вы можете запустить следующую команду для настройки локального пользователя. Когда администратор входит в систему на устройстве, он должен использовать настроенные на нем логин и пароль. Уровень безопасности пользователя должен быть выше или равен уровню безопасности группы, к которой он принадлежит. В противном случае пользователь не сможет пройти аутентификацию.

Команда	Описание
snmp-server user *username groupname* {**v3** [**encrypted** | **auth**] [**md5** | **sha**] *auth-password*}	Настраивает локального пользователя SNMPv3

5.1.2.12 Настройка шифрования SNMP-сервера

Вы можете запустить следующую команду в режиме глобальной конфигурации, чтобы настроить шифрование SNMP-сервера. Используйте зашифрованный текст, чтобы показать пароль SHA и пароль MD5. Команда является одноразовой и не может быть отменена командой **no**.

Команда	Описание
snmp-server encryption	Используйте зашифрованный текст, чтобы показать пароль SHA и пароль MD5

5.1.2.13 Настройка trap-интерфейса SNMP-сервера

Вы можете запустить следующую команду в режиме глобальной конфигурации, чтобы настроить источник trap-сообщений. Используйте команду **no**, чтобы удалить такой интерфейс.

Команда	Описание
snmp-server trap-source *interface*	Любой SNMP-сервер имеет trap-адрес независимо от того, с какого интерфейса он отправляет trap-сообщение

5.1.2.14 Настройка trap-timeout SNMP-сервера

Вы можете запустить следующую команду в режиме глобальной конфигурации, чтобы настроить время ожидания отправки trap-сообщений SNMP-сервера.

Команда	Описание
snmp-server trap-timeout *seconds*	Перед отправкой trap-сообщения программное обеспечение коммутатора найдет маршрут к адресу назначения. Если маршрута нет, сообщение будет сохранено в очереди для повторной передачи. Команда **server trap-timeout** определяет интервал повторной передачи

5.1.2.15 Настройка определения источника trap-уведомлений

Выполните следующую команду, чтобы настроить определение источника trap-уведомлений в управляемой сети:

Команда	Описание
snmp-server trap-add-hostname	Когда на управляемой сети происходит какое-либо событие и генерируется SNMP-уведомление (trap), с помощью данной команды можно определить, с какого хоста или устройства пришло это уведомление

5.1.2.16 Настройка trap-логов SNMP-сервера

Используйте следующую команду для настройки trap-логов SNMP-сервера:

Команда	Описание
snmp-server trap-logs	Включает журнал SNMP-сервера для записи пересылаемых trap-сообщений

5.1.2.17 Настройка snmp-dos-max

Установите количество попыток для повторного ввода пароля SNMP в течение пяти минут:

Команда	Описание
snmp-server set-snmp-dos-max *retry times*	Устанавливает количество попыток для повторного ввода пароля SNMP в течение пяти минут

Эту функцию следует использовать совместно с **snmp-server host**.

5.1.2.18 Настройка времени поддержания активности

Вы можете выполнить следующую команду в режиме глобальной конфигурации, чтобы настроить время поддержания активности SNMP-сервера:

Команда	Описание
snmp-server keep-alive *times*	Интервал отправки пакетов keep-alive. Единица измерения: секунды

5.1.2.19 Настройка necode SNMP-сервера

Вы можете запустить следующую команду в режиме глобальной конфигурации, чтобы настроить информацию о кодировке SNMP-сервера (это единственный тег устройства). Используйте команду **no**, чтобы удалить информацию тега.

Команда	Описание
snmp-server necode *text*	Соответствует переменным приватной MIB SNMP

5.1.2.20 Настройка идентификатора события SNMP-сервера

Вы можете запустить следующую команду в режиме глобальной конфигурации, чтобы настроить идентификаторы событий. Используйте команду **no** для удаления этой настройки.

Команда	Описание
snmp-server event-id *number* **trap-oid** *oid*	Используется в конфигурации хоста и для фильтрации пересылаемых trap-сообщений

5.1.2.21 Настройки времени ожидания для операции GetBulk

Вы можете запустить следующую команду в режиме глобальной конфигурации, чтобы настроить время ожидания для операции GetBulk. Во время тайм-аута все запросы множества значений переменных из MIB в одном блоке не будут обработаны. Используйте команду **no** для удаления настройки.

Команда	Описание
snmp-server getbulk-timeout *seconds*	Устанавливает тайм-аут GetBulk в секундах. Во время тайм-аута запросы от GetBulk не обрабатываются

5.1.2.22 Настройка задержки ответа на запросы GetBulk

Вы можете запустить следующую команду в режиме глобальной конфигурации, чтобы настроить время задержки ответа на запросы GetBulk. Единица измерения – сантисекунда. Используйте команду **no** для удаления настройки.

Команда	Описание
snmp-server getbulk-delay *ticks*	Чтобы SNMP не занимал слишком много ресурсов ЦП, установите метки задержки ответа на запросы GetBulk. Единица измерения: одна сотая секунды

5.1.2.23 Отображение информации о работе SNMP

Используйте команду **show snmp** для мониторинга входной и выходной статистики SNMP, включая недопустимые записи строк сообщества, ошибки и количество переменных запроса. Используйте команду **show snmp engineID** для отображения информации об узле SNMP. Используйте команду **show snmp host**, чтобы отобразить информацию о trap-хосте SNMP. Используйте команду **show snmp view**, чтобы отобразить информацию о представлении SNMP. Используйте команду **show snmp mibs** для отображения информации о регистрации MIB. Используйте команду **show snmp group** для отображения информации о группе SNMP. Используйте команду **show snmp user** для отображения информации о пользователе SNMP.

Команда	Описание
show snmp *engineID*	Показать информацию о локальном ядре SNMP
show snmp *host*	Показать информацию о хосте SNMP
show snmp *view*	Показать информацию о представлении SNMP
show snmp *mibs*	Показать информацию о регистрации MIB
show snmp *group*	Показать информацию о группе SNMP
show snmp *user*	Показать информацию о пользователе SNMP

5.1.2.24 Отображение отладочной информации SNMP

Отображение информации об ошибках, событиях и пакетах SNMP.

Команда	Описание
debug snmp *error*	Включение режима отладки ошибок SNMP
debug snmp *event*	Включение режима отладки событий SNMP
debug snmp *packet*	Включение режима отладки пакетов SNMP

5.1.3 Примеры настройки

Пример 1

snmp-server community public RO

snmp-server community private RW

snmp-server host 192.168.10.2 public

В приведенном выше примере показано, как создать строку публичного комьюнити «public», которое может только читать все переменные MIB. Как сделать строку частного сообщества «private» с доступом к переменным MIB на чтение и запись. Последняя команда предписывает публичному комьюнити «public» отправку trap-сообщений на 192.168.10.2, когда этого требует система. Например, когда порт находится в нерабочем состоянии, система отправит по адресу 192.168.10.2 информацию о прерывании соединения.

Пример 2

snmp-server group getter v3 auth

snmp-server group setter v3 priv write v-write

snmp-server user get-user getter v3 auth sha 12345678

snmp-server user set-user setter v3 encrypted auth md5 12345678

snmp-server view v-write internet included

В приведенном выше примере демонстрируется использование SNMPv3 для управления сетевыми устройствами. Группа «getter» может просматривать информацию об устройствах, в то время как группа «setter» может устанавливать параметры устройств. Пользователь «get-user» принадлежит группе «getter», а пользователь «set-user» – группе «setter».

Для пользователя «get-user» уровень безопасности состоит в аутентификации, но без шифрования. Пароль пользователя – «12345678», и для хеширования пароля используется алгоритм SHA. Для пользователя «set-user» уровень безопасности включает аутентификацию и шифрование. Пароль также «12345678», однако для его хеширования используется алгоритм MD5.

5.2 RMON

RMON (Remote Monitoring) – это стандарт протокола, который используется для удаленного мониторинга сетевых устройств. Он определяет методы и переменные для сбора информации о сетевом трафике, производительности и ошибках. RMON позволяет администраторам сети контролировать и анализировать сетевую активность, идентифицировать проблемы и оптимизировать работу сети. RMON может использоваться для отладки сетевых проблем, мониторинга загрузки сети, определения узких мест и прогнозирования емкости сети.

5.2.1 Настройка RMON

Задачи настройки RMON включают в себя:

- настройку функции аварийной сигнализации;
- настройку функции обработки события;
- настройку статистики;
- настройку истории;
- отображение конфигурации RMON.

5.2.1.1 Настройка сигнализации RMON

Функцию тревоги RMON можно настроить при помощи командной строки или через SNMP NMS. Если вы настраиваете через SNMP NMS, предварительно необходимо настроить SNMP коммутатора. После настройки функции тревоги устройство может отслеживать определенные статистические значения в системе. В следующей таблице показано, как настроить функцию аварийного сигнала RMON:

Команда	Описание
config	Вход в режим глобальной конфигурации
rmon alarm index variable *interval* {**absolute** | **delta**} **rising-threshold** *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [**owner** *string*] [**repeat**]	Добавление элемента тревоги RMON **index** – это номер элемента тревоги. Его диапазон составляет от 1 до 65535 **variable** – переменная, объект в отслеживаемой MIB. Объект должен быть активным и корректно функционировать в системе MIB. Могут быть обнаружены только объекты определенных типов, таких как Integer (целочисленные значения), Counter

	(счетчики), Gauge (измерительные приборы) или Time Ticks (единицы времени) **interval** – временной интервал для выборки. Его единица – секунда. Диапазон значений – от 1 до 2 147 483 647 **absolute** – используется для прямого контроля значения объекта MIB **delta** используется для отслеживания изменения значений объектов MIB между двумя выборками **value** – это пороговое значение, при котором генерируется аварийный сигнал **event number** – это индекс события, которое генерируется при достижении порога. Не является обязательным **owner string** – строка владельца, предназначена для описания информации о тревоге **repeat** – повторить триггерное событие
exit	Вернуться в режим управления
write	Сохранить настройки

После настройки элемента аварийного сигнала RMON устройство через определенный интервал времени получит значение OID, указанное в переменной. Полученное значение будет сравниваться с предыдущим значением в зависимости от типа тревоги (**absolute** или **delta**). Если значение, полученное из определенного OID, превышает предыдущее значение и пороговое значение, будет сгенерировано событие с указанным индексом eventnumber. Если значение eventnumber равно 0 или событие с указанным индексом отсутствует в таблице событий, ничего не произойдет. Если невозможно получить указанный в переменной OID, состояние элемента тревоги в этой строке будет отмечено как недопустимое. Если вы запускаете **rmon alarm** много раз для настройки элементов сигналов тревоги с одним и тем же индексом, актуальной будет только последняя конфигурация. Для удаления конфигурации с определенным индексом можно использовать команду **no rmon alarm** *index*.

5.2.1.2 Настройка события RMON

Этапы настройки события RMON показаны в следующей таблице:

Команда	Описание
config	Вход в режим глобальной конфигурации

rmon event index [**description** *string*] [**log**] [**owner** *string*] [**trap** *community*] [**ifctrl** *interface*]	Добавляет событие RMON **index** – означает номер элемента события. Диапазон составляет от 1 до 65535 **description** – описание, означает информацию о событии **log** – означает добавление информации в таблицу журнала при возникновении события **trap** – означает, что при возникновении события генерируется trap-сообщение **community** – имя комьюнити **ifctrl interface** – интерфейс, управляющий завершением события **owner string** – строка владельца, предназначена для описания информации о событии
exit	Выход в режим управления
write	Сохранение настроек

После того, как событие RMON сконфигурировано, вы должны установить для параметра eventLastTimeSent элемента события RMON значение sysUpTime при срабатывании тревоги RMON. Если для атрибута журнала задано событие RMON, в таблицу журнала добавляется сообщение. Если для атрибута trap установлено событие RMON, от имени комьюнити отправляется trap-сообщение. Если вы запускаете **rmon event** много раз для настройки элементов событий с одним и тем же индексом, будет актуальна только последняя конфигурация. Для удаления элементов событий с определенным индексом можно использовать команду **no rmon event** *index*.

5.2.1.3 Настройка статистики RMON

Группа статистики RMON используется для мониторинга статистической информации по каждому порту устройства.

Этапы настройки статистики RMON следующие:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface *iftype ifid*	Вход в режим настройки интерфейса **iftype** – означает тип интерфейса **ifid** – означает идентификатор интерфейса
rmon collection stats index [**owner** *string*]	Разрешить сбор статистики на порту **index** – означает индекс статистики

	owner string – строка владельца, предназначена для описания информации о статистике
exit	Войти в режим глобальной конфигурации
exit	Вернуться в режим управления
write	Сохранить настройки

Если вы запускаете **rmon collection stats** много раз для настройки элементов статистики с одним и тем же индексом, будет актуальна только последняя конфигурация. Вы можете запустить **no rmon collection stats** *index*, чтобы отменить обработку элементов статистики с указанным индексом.

5.2.1.4 Настройка истории RMON

Группа истории RMON используется для сбора статистической информации в различных временных интервалах на порту устройства. Функция истории RMON настраивается следующим образом:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface *iftype ifid*	Вход в режим настройки интерфейса **iftype** – означает тип порта **ifid** – означает идентификатор интерфейса
rmon collection history index [**buckets** *bucket-number*] [**interval** *second*] [**owner** *owner-name*]	Включает функцию истории на порту **index** – порядковый номер элемента истории Настройки этой функции определяют, сколько последних пакетов данных будет сохраняться в истории. Вы можете просмотреть элементы истории для Ethernet-порта, чтобы получить статистические значения. Значение по умолчанию обычно составляет 50 элементов. **second** – означает временной интервал получения статистических данных. Значение по умолчанию – 1800 секунд. **owner string** – строка владельца, используется для описания элемента истории
exit	Выход в режим глобальной конфигурации

exit	Выход в режим управления
write	Сохранение настроек

После добавления элемента истории RMON устройство будет получать значения статистики с указанного порта каждую секунду. Значение статистики будет добавлено к элементу истории как часть информации. Если вы запускаете **rmon collection history** *index* много раз для настройки элементов истории с одним и тем же индексом, актуальной будет только последняя конфигурация. Вы можете запустить **no rmon collection history** *index*, чтобы отменить обработку элементов истории с указанным индексом.

В случае, если значение «bucket-number» слишком велико или значение интервала «second» слишком мало, будет задействовано много системных ресурсов.

5.2.1.5 Отображение RMON-конфигурации коммутатора

Запустите **show**, чтобы отобразить конфигурацию RMON коммутатора.

Команда	Описание
show rmon [**alarm**] [**event**] [**statistics**] [**history**]	Отображает информацию о настройках **alarm** – означает отображение конфигурации элемента аварийного сигнала **event** – означает отображение конфигурации элемента события и элементов, которые генерируются при возникновении событий и содержатся в таблице журнала **statistics** – означает отображение конфигурации элемента статистики и значений статистики, которые устройство собирает с порта **history** – означает отображение настроек элемента истории и значений статистики, которые устройство собирает с порта в последние заданные промежутки времени

6. Аутентификация, авторизация и учет

6.1 Введение

Управление доступом необходимо для контроля доступа пользователей к OLT или NAS и для разграничения их прав на использование тех или иных видов услуг. Службы сетевой безопасности аутентификации, авторизации и учета (AAA) обеспечивают основную структуру, с помощью которой настраивается контроль доступа.

6.1.1 Служба безопасности AAA

AAA – это архитектурная структура для согласованной настройки набора из трех независимых функций безопасности. AAA предлагает модульный способ предоставления следующих услуг:

- Аутентификация – это метод идентификации пользователей, включая запрос имени пользователя/пароля и шифрование в соответствии с выбранным протоколом безопасности.

  Аутентификация – это метод идентификации личности пользователя до того, как пользователи получат доступ к сети и воспользуются сетевыми услугами. Аутентификацию AAA можно настроить с помощью определения списка методов аутентификации и последующего его применения на всех интерфейсах. Этот список методов определяет тип аутентификации и порядок выполнения; любой определенный список методов аутентификации должен быть применен к определенному интерфейсу перед его выполнением. Единственным исключением является список методов аутентификации по умолчанию (который называется default). Если других списков методов аутентификации нет, на всех интерфейсах автоматически будет применен метод default. Если метод для отдельного интерфейса определен, он заменит значение по умолчанию. Чтобы узнать, как настроить все проверки подлинности, см. раздел «Настройка аутентификации».

- Авторизация – это метод управления удаленным доступом для ограничения разрешений пользователя.

  Авторизация AAA осуществляется через группу функций, в которых пользователь авторизуется с некоторыми разрешениями. Во-первых, функции в этой группе будут сравниваться с информацией о конкретном пользователе в базе данных, затем результат сравнения будет возвращен в AAA для подтверждения фактических разрешений этого пользователя. Эта база данных может находиться на локальном сервере, к которому осуществляется доступ, или на OLT, или на удаленном сервере RADIUS/TACACS+. Сервер RADIUS или TACACS+ проводит авторизацию пользователя через связанный с пользователем одноранговый атрибут-значение. Значение атрибута (AV) определяет доступные разрешения. Все методы авторизации определяются через AAA. Как и при аутентификации, сначала будет определен список методов авторизации, а затем этот

список будет применяться ко всем типам интерфейсов. О том, как выполнить настройку авторизации, см. в разделе «Настройка авторизации».

- Учет – это метод сбора информации о пользователе и отправки информации на сервер безопасности. Собранную информацию можно использовать для открытия учетной записи, проведения аудита и формирования списков отчетов на базе таких сведений, как идентификатор пользователя, время начала/окончания сеанса, выполненные команды и количество пакетов или байтов.

  Функция учета может отслеживать сервисы, к которым обращаются пользователи, и в то же время отслеживать количество потребляемых сервисом сетевых ресурсов. Когда учет AAA активирован, сервер доступа может сообщать о действиях пользователя серверу TACACS+ или RADIUS в порядке учета. Каждая учетная запись содержит узел AV, который хранится на сервере безопасности. Данные могут быть использованы для управления сетью, анализа клиента или аудита. Подобно аутентификации и авторизации, список методов учета должен быть сначала определен, а затем применен к различным интерфейсам. О том, как выполнить настройку учета, см. в разделе «Настройка учета».

6.1.2 Преимущества использования AAA

AAA дает следующие преимущества:

- повышенную гибкость и контроль конфигурации доступа;
- масштабируемость;
- стандартные методы аутентификации, такие как RADIUS, TACACS+;
- несколько систем резервного копирования.

6.1.3 Принципы AAA

AAA предназначен для того, чтобы вы могли динамически настраивать нужный тип аутентификации и авторизации для каждой линии (для каждого пользователя) или для каждой услуги (например, IP, IPX или VPDN). Вы определяете нужный тип аутентификации и авторизации, создавая списки методов, а затем применяя эти списки методов к определенным службам или интерфейсам.

6.1.4 Список методов AAA

Чтобы настроить AAA, сначала определите именованный список методов, а затем примените его к конкретной службе или интерфейсу. Этот список методов определяет текущий тип AAA и последовательность выполнения методов. Любой определенный список методов должен быть применен к конкретному интерфейсу или службе перед запуском. Единственным исключением является список методов по умолчанию default. Он автоматически применяется ко всем интерфейсам или службам, если интерфейс явно не применяет другой список, который заменяет список по умолчанию.

Список методов – это последовательный список, определяющий методы аутентификации, используемые для проверки подлинности пользователя. В списке методов AAA вы можете указать один или несколько протоколов безопасности. Таким образом, он обеспечивает резервную систему аутентификации на случай, если первоначальный метод не сработает. Наше программное обеспечение коммутатора использует первый метод для аутентификации пользователей; если этот метод не отвечает, программное обеспечение выбирает следующий метод аутентификации в списке методов. Этот процесс продолжается до тех пор, пока не будет установлена успешная связь или список методов не будет исчерпан. В таком случае аутентификация завершается ошибкой.

Важно отметить, что программное обеспечение коммутатора пытается выполнить аутентификацию с помощью следующего из перечисленных методов аутентификации только в том случае, если предыдущий метод не дает ответа. Если аутентификация завершается ошибкой в какой-либо момент цикла, это означает, что сервер безопасности или локальная база данных имен отвечает пользователю отказом в доступе. Процесс аутентификации останавливается, и никакие другие методы аутентификации далее не предпринимаются.

На следующем рисунке показана типичная конфигурация сети AAA, включающая четыре сервера безопасности: R1 и R2 – серверы RADIUS, а T1 и T2 – серверы TACACS+. Аутентификация взята в качестве примера, чтобы продемонстрировать связь между сервисом AAA и списком методов AAA.

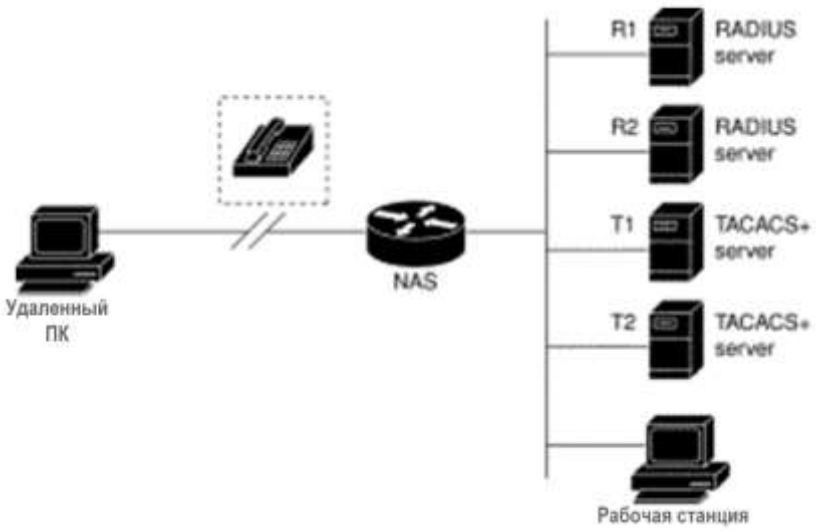

Рисунок 6-1 – Типовая конфигурация AAA

В этом примере «default» – это имя списка методов, включая протокол в списке методов, а последовательность запросов списка методов следует за именем. Список методов default автоматически применяется ко всем интерфейсам.

Когда удаленный пользователь пытается подключиться к сети, сервер доступа NAS сначала запрашивает у R1 информацию об аутентификации. Если R1 аутентифицирует пользователя, он выдает серверу NAS ответ PASS, и пользователю разрешается доступ в

сеть. Если R1 возвращает ответ FAIL, пользователю отказывают в доступе, и сеанс завершается. Если R1 не отвечает, то сервер доступа обрабатывает это как ошибку (ERROR) и запрашивает у R2 информацию об аутентификации. Этот механизм продолжает применять оставшиеся назначенные методы до тех пор, пока пользователь не будет аутентифицирован или отклонен, или пока не завершится сеанс.

Ответ FAIL значительно отличается от ответа ERROR. FAIL означает, что пользователь не соответствует критериям, содержащимся в применяемой базе данных аутентификации, чтобы быть успешно аутентифицированным. ERROR означает, что сервер безопасности не ответил на запрос аутентификации. Только при обнаружении такой ошибки AAA выберет следующий метод аутентификации, определенный в списке методов.

Предположим, системный администратор хочет применить список методов к определенному порту. В таком случае он должен создать список методов, отличный от списка по умолчанию default, а затем применить список с этим именем к соответствующему порту.

6.1.5 Процесс настройки AAA

Сначала необходимо определить, какое решение безопасности вы хотите внедрить. Вам нужно оценить риски безопасности в конкретной сети и выбрать подходящие средства для предотвращения несанкционированного проникновения и атак. Прежде чем настраивать AAA, необходимо знать базовую процедуру настройки. Чтобы провести настройку безопасности AAA на OLT или серверах доступа, выполните следующие действия:

- если вы решили использовать сервер безопасности, сначала настройте параметры протокола безопасности, такие как RADIUS, TACACS+;
- определите списки методов для аутентификации с помощью команды настройки аутентификации AAA;
- при необходимости примените списки методов к конкретному интерфейсу или линии;
- (необязательно) настройте авторизацию с помощью команды настройки авторизации AAA;
- (необязательно) настройте учет с помощью команды настройки учета AAA.

6.2 Настройка аутентификации

Задачи настройки аутентификации AAA

- Настройка аутентификации при входе с помощью AAA
- Включение защиты паролем на привилегированном уровне
- Настройка баннеров сообщений для аутентификации AAA
- Изменение строки уведомления для ввода имени пользователя

- Изменение подсказки пароля аутентификации AAA
- Создание локальной базы данных аутентификации имени пользователя

Чтобы настроить аутентификацию AAA, выполните следующие процедуры:

1. Если вы решили использовать отдельный сервер безопасности, настройте параметры протокола безопасности, например, RADIUS или TACACS+. Обратитесь к соответствующему разделу для ознакомления с конкретными методами настройки.

2. Настройте список методов аутентификации AAA.

3. При необходимости примените список методов аутентификации к конкретному интерфейсу или линии.

6.2.1 Настройка аутентификации при входе с помощью AAA

Службы безопасности AAA упрощают различные методы аутентификации при входе в систему. Используйте команду **aaa authentication login**, чтобы включить аутентификацию AAA независимо от того, какой из поддерживаемых методов аутентификации при входе вы решите использовать. С помощью команды **aaa authentication login** вы создаете один или несколько списков методов аутентификации, которые пробуются при входе в систему. После настройки списков методов вы можете применить их, запустив **login authentication**. Запустите следующую команду в режиме глобальной конфигурации:

Команда	Описание
aaa authentication login {**default** | *list-name*} *method1* [*method2...*]	Включает AAA глобально
line {**console** | **vty**} *line-number* [*ending-line-number*]	Вход в режим настройки линии
login authentication {**default** | *list-name*}	Применяет список проверки подлинности к линии или набору линий

list-name – это строка символов, используемая для наименования списка, который вы создаете. Ключевое слово метода определяет фактический метод аутентификации. Дополнительные методы аутентификации используются только в том случае, если предыдущий метод возвращает ошибку, а не в случае неудачи. Если необходимо, чтобы аутентификация проходила успешно, даже если все методы возвращают ошибку, нужно указать **none** в качестве последнего метода в командной строке. Это предоставляет возможность разрешить аутентификацию в случае проблем и неисправностей, возникших при попытке применения других методов.

Параметр **default** может создать список аутентификации по умолчанию, который будет автоматически применяться ко всем интерфейсам. Например, чтобы указать, что аутентификация должна пройти успешно, даже если сервер TACACS+ возвращает ошибку, введите следующую команду:

aaa authentication login default group radius

- Поскольку ключевое слово **none** позволяет успешно пройти аутентификацию любому пользователю, вошедшему в систему, его следует использовать только в качестве резервного метода аутентификации.
- Если вы не можете найти список методов аутентификации, вход возможен только через консольный порт. Любой другой способ входа в систему недоступен.

В следующей таблице перечислены поддерживаемые методы аутентификации при входе:

Ключевое слово	Описание
enable	Использует пароль enable для аутентификации
group *name*	Использует определенную группу серверов для аутентификации
group radius	Использует RADIUS для аутентификации
group tacacs+	Использует TACACS+ для аутентификации
line	Использует пароль линии для аутентификации
local	Использует локальную базу данных имен пользователей для аутентификации
localgroup	Использует базу данных имен пользователей локальной группы в рамках стратегии безопасности группы
local-case	Использует аутентификацию локального имени пользователя с учетом регистра
none	Проходит аутентификацию без каких-либо условий

1. Аутентификация при входе с использованием пароля уровня enable

Используйте команду аутентификации AAA с ключевым словом **enable**, чтобы указать пароль enable в качестве метода аутентификации при входе в систему. Например, чтобы указать пароль enable в качестве метода аутентификации, когда не задан другой список методов, введите следующую команду:

aaa authentication login default enable

2. Аутентификация при входе с использованием пароля линии

Используйте команду аутентификации AAA с ключевым словом **line**, чтобы указать пароль конкретной линии/порта в качестве метода аутентификации входа. Например, чтобы

указать пароль линии в качестве метода аутентификации пользователя при входе в систему, когда не задан другой список методов, введите следующую команду:

aaa authentication login default line

Прежде чем вы сможете использовать линейный пароль в качестве метода аутентификации при входе в систему, вам необходимо определить этот пароль.

3. Аутентификация при входе с использованием локального пароля

Используйте команду аутентификации AAA с ключевым словом **local**, чтобы указать, что маршрутизатор или сервер доступа будут использовать локальную базу данных имен пользователей для аутентификации. Например, чтобы указать локальную базу данных имен пользователей в качестве метода аутентификации пользователя при входе в систему, если не задан другой список методов, введите следующую команду:

aaa authentication login default local

4. Аутентификация при входе с помощью группы RADIUS

Используйте команду аутентификации AAA с ключевыми словами **group radius**, чтобы указать RADIUS в качестве метода аутентификации при входе. Например, чтобы указать RADIUS в качестве метода аутентификации пользователя при входе в систему, когда не задан другой список методов, введите следующую команду:

aaa authentication login default group radius

Прежде чем вы сможете использовать RADIUS в качестве метода аутентификации при входе в систему, вам необходимо включить связь с сервером безопасности RADIUS. Дополнительные сведения об установлении связи с сервером RADIUS см. в разделе «Настройка RADIUS».

6.2.2 Включение защиты паролем на привилегированном уровне

Используйте команду **aaa authentication enable default**, чтобы создать серию методов аутентификации, которые используются для определения того, может ли пользователь получить доступ к привилегированному командному режиму уровня EXEC. Вы можете указать до четырех методов аутентификации. Дополнительные методы аутентификации используются только в том случае, если предыдущий метод возвращает ERROR, а не FAIL. Чтобы указать, что аутентификация должна пройти успешно, даже если все методы возвращают ошибку, укажите **none** в качестве последнего метода в командной строке. Используйте следующую команду в режиме глобальной конфигурации:

Команда	Описание
aaa authentication enable default *method1* [*method2*...]	Включает проверку идентификатора пользователя и пароля для пользователей, запрашивающих привилегированный уровень EXEC

Аргумент метода относится к фактическому списку методов, которые пробует алгоритм аутентификации в введенной последовательности.

В следующей таблице содержатся ключевые слова, связанные с поддерживаемыми методами аутентификации при входе в привилегированный режим:

Ключевое слово	Описание
enable	Использует пароль enable для аутентификации
group *name*	Использует определенную группу серверов для аутентификации
group radius	Использует RADIUS для аутентификации
group tacacs+	Использует TACACS+ для аутентификации
line	Использует пароль линии для аутентификации
none	Проходит аутентификацию без каких-либо условий

При настройке метода «enable» в качестве удаленной аутентификации используйте RADIUS, как описано ниже.

1. Использование RADIUS для аутентификации «enable»

Имя пользователя для аутентификации – $ENABLElevel$; **level** – это привилегированный уровень, на который переходит пользователь, то есть номер привилегированного уровня после команды **enable**. Например, если пользователь хочет перейти на привилегированный уровень 7, введите команду **enable 7**. При настройке RADIUS для аутентификации, имя пользователя, представляемое хосту RADIUS-сервера, равно $ENABLE7$; привилегированный уровень «enable» по умолчанию равен 15, то есть имя пользователя, представляемое хосту RADIUS-сервера, равно $ENABLE15$. Имя пользователя и пароль нужно настроить на хосте RADIUS-сервера заранее. Дело в том, что в базе данных пользователей хоста RADIUS-сервера Service-Type пользователя, задающий привилегированную аутентификацию, равен 6, то есть Admin-User.

6.2.3 Настройка баннеров сообщений для аутентификации AAA

Программой поддерживается баннер для различных типов входа в систему. В случае неудачной аутентификации AAA во время входа, будет отображаться настроенный баннер с сообщением независимо от причины сбоя.

1. Настройка баннера регистрации

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
aaa authentication banner *delimiter text-string delimiter*	Используется для настройки персонального баннера, который будет

	отображаться при входе пользователей на устройство

2. Настройка баннера неудачного входа в систему

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
aaa authentication fail-message *delimiter text-string delimiter*	Используется для настройки персонального баннера, который будет отображаться при неудачной попытке входа пользователей на устройство

3. Методические рекомендации

При создании баннера необходимо настроить разделитель (*delimiter*), а затем настроить саму текстовую строку. Разделитель уведомляет о том, что следующая текстовая строка будет отображаться в качестве баннера. Разделитель повторно появляется в конце строки текстовых символов, указывая на то, что сообщение баннера завершено.

6.2.4 Изменение строки уведомления для ввода имени пользователя

Чтобы изменить текст приглашения ввода имени пользователя по умолчанию, запустите **aaa authentication username-prompt**. Вы можете запустить **no aaa authentication username-prompt**, чтобы возобновить стандартный запрос:

username:

Команда **aaa authentication username-prompt** не изменяет никакой информации о приглашении, предоставляемой удаленным сервером TACACS+ или сервером RADIUS. Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
aaa authentication username-prompt *text-string*	Изменяет текст приглашения ввода имени пользователя по умолчанию

6.2.5 Изменение запроса пароля для аутентификации AAA

Чтобы изменить текст, отображаемый при запросе пароля, используйте команду **aaa authentication password-prompt**. Чтобы вернуться к тексту запроса пароля по умолчанию, используйте форму **no** этой команды. Вы можете запустить **no aaa authentication username-prompt**, чтобы возобновить стандартный запрос на ввод пароля:

password:

Команда **aaa authentication password-prompt** не изменяет никакой информации, предоставленной удаленным сервером TACACS+ или сервером RADIUS. Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
aaa authentication password-prompt *text-string*	Строка текста, которая будет отображаться, когда пользователю предлагается ввести пароль

6.2.6 Создание базы данных аутентификации с локальными привилегиями

Чтобы создать базу данных для пользователей с локальным уровнем привилегий enable, запустите **enable password** в режиме глобальной конфигурации. Вы можете указать тип шифрования, зашифрованный пароль и уровень привилегий. Для удаления или отмены настройки пароля enable, используйте команду **no enable password** с указанием уровня привилегий, если необходимо.

enable password {[*encryption-type*] *encrypted-password*} [**level** *level*]
no enable password [**level** *level*]

6.2.7 Пример настройки аутентификации AAA

В следующем примере показано, как настроить OLT для аутентификации и авторизации с использованием RADIUS:

```
aaa authentication login radius-login group radius local
aaa authorization network radius-network group radius
line vty 3
login authentication radius-login
```

Значение каждой командной строки показано ниже:

- Команда **aaa authentication login radius-login group radius local** настраивает OLT на использование RADIUS для аутентификации при запросе входа в систему. Если RADIUS возвращает ошибку, пользователь аутентифицируется с использованием локальной базы данных.
- Команда **aaa authorization network radius-network group radius** запрашивает у RADIUS сетевую авторизацию, назначение адресов и другие списки доступа.
- Команда **login authentication radius-login** включает список методов входа в систему для линии 3.

6.3 Настройка авторизации

Чтобы настроить авторизацию AAA, выполните следующие процедуры:

1. Если вы решили использовать отдельный сервер безопасности, настройте параметры протокола безопасности, например, RADIUS или TACACS+. Обратитесь к соответствующему разделу для ознакомления с конкретными методами настройки.

2. Запустите **aaa authorization**, чтобы определить список методов авторизации. Служба авторизации не предоставляется по умолчанию.

3. При необходимости примените список методов авторизации к конкретному интерфейсу или линии.

6.3.1 Настройка авторизации EXEC через AAA

Чтобы включить авторизацию AAA, запустите **aaa authorization**. Команда **aaa authorization exec** может создать один или несколько списков методов авторизации и включить авторизацию EXEC, чтобы решить, запускается ли программа оболочки EXEC пользователями или нет, а также авторизованы ли пользователи с привилегией при входе в программу оболочки EXEC. После настройки списков методов авторизации вы можете применить эти списки, запустив **login authorization**. Чтобы начать настройку, вы можете запустить следующую команду:

Команда	Описание
aaa authorization exec {**default** | *list-name*} *method1* [*method2...*]	Создает общий список авторизации
line [**console** | **vty**] *line-number* [*ending-line-number*]	Вход в режим настройки линии
login authorization {**default** | *list-name*}	Применяет список авторизации к линии или набору линий (в режиме настройки линии)

list-name – это строка символов, используемая для имени создаваемого вами списка. Ключевое слово метода используется для обозначения реального метода авторизации. Только когда ранее использованный метод возвращает ошибку авторизации, можно использовать другие методы. Если авторизация не удалась и предыдущий метод возвратил FAIL, другие методы использоваться не будут. Если требуется, чтобы вход в оболочку EXEC был произведен даже тогда, когда все методы возвращают ошибки, назначьте **none** как последний метод авторизации в командной строке.

Параметр **default** может создать список авторизации по умолчанию, который будет автоматически применяться ко всем интерфейсам. Например, вы можете запустить следующую команду, чтобы указать RADIUS в качестве метода авторизации по умолчанию для EXEC:

```
aaa authorization exec default group radius
```

Если список методов не может быть найден во время процесса авторизации, авторизация будет пройдена напрямую, без проведения авторизационных процедур.

В следующей таблице перечислены поддерживаемые в настоящее время методы авторизации EXEC:

Ключевое слово	Описание
group *WORD*	Использует определенную группу серверов для выполнения авторизации
group radius	Использует авторизацию RADIUS
group tacacs+	Использует авторизацию TACACS+
local	Использует локальную базу данных для выполнения авторизации
if-authenticated	Автоматически авторизует аутентифицированного пользователя со всеми необходимыми функциями
none	Проходит авторизацию без каких-либо условий

6.3.2 Пример авторизации AAA

В следующем примере показано, как выполнить локальную авторизацию и локальную авторизацию путем настройки OLT:

```
aaa authentication login default local
aaa authorization exec default local
!
localauthor a1
 exec privilege default 15
!
local author-group a1
username exec1 password 0 abc
username exec2 password 0 abc author-group a1
username exec3 password 0 abc maxlinks 10
```

```
username exec4 password 0 abc autocommand telnet 172.16.20.1
!
```

Ниже показано значение каждой командной строки:

- Команда **aaa authentication login default local** используется для определения списка методов аутентификации по умолчанию, который будет автоматически применяться ко всем службам аутентификации при входе.
- Команда **aaa authorization exec default local** используется для определения списка методов авторизации EXEC по умолчанию, который будет автоматически применяться ко всем пользователям, которым требуется войти в оболочку EXEC.
- Команда **localauthor a1** определяет политику локальной авторизации с именем a1.
- Команда **exec privilege default 15** определяет уровень привилегий по умолчанию для пользователей, входящих в режим EXEC. Значение 15 указывает на высший уровень привилегий, позволяющий доступ ко всем командам настройки и управления устройством.
- Команда **local author-group a1** означает применение локальной политики авторизации a1 к глобальной конфигурации (локальная группа политик по умолчанию).
- Команда **username exec1 password 0 abc** определяет учетную запись exec1 с паролем abc в режиме глобальной конфигурации.
- Команда **username exec2 password 0 abc author-group a1** определяет учетную запись exec2 с паролем abc в режиме глобальной конфигурации. Учетная запись применяется к локальной политике авторизации a1.
- Команда **username exec3 password 0 abc maxlinks 10** определяет учетную запись exec3 с паролем abc в режиме глобальной конфигурации. Учетная запись делает доступными одновременно 10 пользовательских соединений.
- Команда **username exec4 password 0 abc autocommand telnet 172.16.20.1** определяет учетную запись exec4 с паролем abc. Telnet 172.16.20.1 запускается автоматически, когда пользователь входит в учетную запись.

6.4 Настройка учета

Задачи настройки

- Настройка учета подключений с помощью AAA
- Настройка сетевого учета с помощью AAA
- Настройка обновления учета с помощью AAA
- Ограничение учета пользователей с нулевым именем

Чтобы настроить учет AAA, выполните следующие процедуры:

1. Если вы решили использовать отдельный сервер безопасности, настройте параметры протокола безопасности, например, RADIUS или TACACS+. Обратитесь к соответствующему разделу для выбора конкретных методов настройки.

2. Настройте списки методов учета. Служба учета не предоставляется по умолчанию.

3. При необходимости примените список методов учета к конкретному интерфейсу или линии.

6.4.1 Настройка учета подключений с помощью AAA

Чтобы включить учет AAA, запустите команду **aaa accounting**. Чтобы создать один или несколько списков методов для предоставления учетных данных обо всех исходящих соединениях, выполненных из OLT, используйте команду **aaa accounting connection**. Исходящие соединения включают Telnet, PAD, H323 и Rlogin. В настоящее время поддерживается только H323. Вы можете запустить следующую команду в режиме глобальной конфигурации:

Команда	Описание
aaa accounting connection {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname}* | **none**}	Устанавливает глобальный список учета

list-name – это строка символов, используемая для имени создаваемого вами списка. Ключевое слово метода определяет реальный метод учетного процесса.

В следующей таблице перечислены поддерживаемые в настоящее время методы учета подключений:

Ключевое слово	Описание
group *WORD*	Использует определенную группу серверов для проведения учета
group radius	Использует RADIUS для учета
group tacacs+	Использует TACACS+ для учета
none	Отключает службы учета для указанной линии или интерфейса
stop-only	Отправляет в журнал учетное старт-уведомление в конце запрошенного пользовательского процесса
start-stop	RADIUS или TACACS+ отправляет учетное старт-уведомление в начале запрошенного процесса и стоп-уведомление в конце процесса

6.4.2 Настройка сетевого учета с помощью AAA

Чтобы включить учет AAA, запустите команду **aaa accounting**. Команда **aaa accounting network** может использоваться для создания одного или нескольких списков методов учета. Сетевой учет включен для предоставления информации обо всех сеансах PPP/SLIP, эта информация включает учет пакетов, байтов и времени. Вы можете запустить следующую команду в режиме глобальной конфигурации:

Команда	Описание
aaa accounting network {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname*} | **none**}	Устанавливает глобальный список учета

list-name – это строка символов, используемая для имени создаваемого вами списка. Ключевое слово метода используется для обозначения реального метода процесса учета.

В следующей таблице перечислены поддерживаемые в настоящее время методы сетевого учета:

Ключевое слово	Описание
group *WORD*	Использует определенную группу серверов для проведения учета
group radius	Использует RADIUS для учета
group tacacs+	Использует TACACS+ для учета
none	Отключает службы учета для указанной линии или интерфейса
stop-only	Отправляет в журнал учетное старт-уведомление в конце запрошенного пользовательского процесса
start-stop	RADIUS или TACACS+ отправляет учетное старт-уведомление в начале запрошенного процесса и стоп-уведомление в конце процесса

6.4.3 Настройка обновления учета через AAA

Чтобы активировать функцию обновления учета AAA с целью отправки временных учетных записей всем пользователям системы, выполните следующую команду:

Команда	Описание
aaa accounting update [**newinfo**] [**periodic** *number*]	Включает обновление учета AAA

Если используется ключевое слово **newinfo**, временная учетная запись будет отправлена на сервер учета, когда появится новая учетная информация, которую необходимо сообщить. Например, после согласования IPCP с IP-адресом удаленного терминала временная учетная запись, включая IP-адрес удаленного терминала, будет отправлена на сервер учета.

При использовании ключевого слова **periodic** временная учетная запись будет отправляться периодически. Период определяется параметром *number*. Временная учетная запись включает всю учетную информацию, имевшуюся до ее отправки.

Два ключевых слова **newinfo** и **periodic** не работают одновременно, то есть параметр, настроенный ранее, заменится параметром, настроенным позднее. Например, если настроено **aaa accounting update periodic**, а затем – **aaa accounting update newinfo**, все уже зарегистрированные к настоящему моменту пользователи продолжат генерировать временные записи учета периодически. У всех новых пользователей учетные записи будут формироваться по алгоритму **newinfo**.

6.4.4 Ограничение учета пользователей без имени

Чтобы предотвратить отправку AAA записей об учетных событиях, если имя пользователя отсутствует или равно пустому (null) значению, выполните следующую команду в режиме глобальной конфигурации:

```
aaa accounting suppress null-username
```

6.5 Настройка политики локальной учетной записи

Задачи настройки

- Настройка локальной политики аутентификации
- Настройка локальной политики авторизации
- Настройка локальной политики паролей
- Настройка локальной группы политик

6.5.1 Настройка локальной политики аутентификации

Чтобы начать настройку локальной аутентификации, запустите команду **localauthen** *WORD* в режиме глобальной конфигурации.

1. Максимальное количество попыток входа в систему в течение определенного времени:

login max-tries *<1-9>* **try-duration** *1d2h3m4s*

Настроенную локальную политику аутентификации можно применить к локальной группе политик или напрямую к определенной локальной учетной записи. Это сразу даст ей приоритет.

6.5.2 Настройка локальной политики авторизации

Чтобы начать настройку локальной авторизации, выполните команду **localauthor** *WORD* в режиме глобальной конфигурации.

1. Присвоение приоритета пользователям, вошедшим в систему:

exec privilege {**default** | **console** | **ssh** | **telnet**} *<1-15>*

Настроенную локальную политику авторизации можно применить к локальной группе политик или напрямую к определенной локальной учетной записи. Это сразу даст ей приоритет.

6.5.3 Настройка локальной политики паролей

Чтобы настроить локальную политику паролей, запустите команду **localpass** *WORD* в режиме глобальной конфигурации.

1. Пароль не может совпадать с именем пользователя:

non-user

2. Проверка истории паролей. История состоит из 20 записей, то есть при изменении пароля, новый пароль не должен совпадать с 20 предыдущими использованными паролями:

non-history

3. Указать компоненты пароля (усложнить пароль):

element [**number**] [**lower-letter**] [**upper-letter**] [**special-character**]

4. Указать длину пароля (усложнить пароль):

min-length *<1-127>*

5. срок действия пароля:

validity *1d2h3m4s*

Настроенную локальную политику паролей можно применить к локальной группе политик или напрямую к локальной учетной записи.

6.5.4 Настройка локальной группы политик

Чтобы настроить локальную группу политик, используйте команду **localgroup** *WORD* в режиме глобальной конфигурации. Режим глобальной конфигурации считается режимом настройки локальной политики по умолчанию.

1. Настройка локальной аутентификации: примените настроенную локальную политику аутентификации к группе политик.

local authen-group *WORD*

2. Настройка локальной авторизации: применить настроенную локальную политику авторизации к группе политик.

local author-group *WORD*

3. настройка локального пароля: примените настроенную локальную политику паролей к группе политик.

local pass-group *WORD*

4. настройка локального учета: установите максимальное количество одновременных соединений/сессий для учетной записи и блокируйте учетную запись пользователя на определенный период времени или до выполнения определенного действия, указанного вместо *WORD*:

local user {{**maxlinks** <*1-255*>} | {**freeze** *WORD*}}

5. Настройка учетной записи: создайте учетную запись для группы политик в локальной базе данных.

username *username* [**password** *password* | {**encryption-type** *encrypted-password*}] [**maxlinks** *number*] [**authen-group** *WORD*] [**author-group** *WORD*] [**pass-group** *WORD*] [**autocommand** *command*]

Настроенную группу политик можно использовать для локальной аутентификации и авторизации. Локальный метод применим к группе политик по умолчанию. С помощью ключевого слова **localgroup** можно настраивать пользовательско-определенные группы политик для контроля доступа к сетевым устройствам, применять разные наборы правил аутентификации и авторизации для различных пользователей и сценариев использования сети.

6.5.5 Пример локальной политики учета

В этом разделе представлен один пример конфигурации с использованием политики локальной учетной записи. В примере показано, как настроить локальную аутентификацию и локальную авторизацию.

```
aaa authentication login default local
aaa authorization exec default local
!
localpass a3
 non-user
 non-history
 element number lower-letter upper-letter special-character
 min-length 10
 validity 2d
```

```
!
localauthen a1
 login max-tries 4 try-duration 2m
!
localauthor a2
 exec privilege default 15
!
local pass-group a3
local authen-group a1
local author-group a2
!
```

Значение каждой командной строки показано ниже:

- Команда **aaa authentication login default local** используется для определения списка методов аутентификации по умолчанию, который будет автоматически применяться ко всем службам аутентификации при входе.
- Команда **aaa authorization exec default local** используется для определения списка методов авторизации EXEC по умолчанию, который будет автоматически применяться ко всем пользователям, которым требуется войти в оболочку EXEC.
- Команда **localpass a3** определяет политику паролей с именем a3.
- Команда **localauthen a1** определяет политику аутентификации с именем a1.
- Команда **localauthor a2** определяет политику авторизации с именем a2.
- Команда **local pass-group a3** применяет политику паролей с именем a3 к группе политик по умолчанию.
- Команда **localauthen-group a1** применяет политику аутентификации с именем a1 к группе политик по умолчанию.
- Команда **localauthor-group a2** применяет политику авторизации с именем a2 к группе политик по умолчанию.

7. RADIUS

В этой главе описывается безопасная система удаленной аутентификации пользователей RADIUS, определяется ее работа, а также подходящие и неподходящие сетевые среды для использования данной технологии. В разделе 7.3 «Список задач настройки RADIUS» описывается, как настроить RADIUS с помощью набора команд аутентификации,

авторизации и учета (AAA). В последнем разделе этой главы приведены два примера настройки.

7.1 Описание

7.1.1 Обзор RADIUS

RADIUS – это распределенная клиент-серверная система, защищающая сети от несанкционированного доступа. Клиенты RADIUS работают на удаленных устройствах и отправляют запросы аутентификации на центральный сервер RADIUS, который содержит всю информацию об аутентификации пользователей и доступе к сетевым службам. RADIUS был реализован в различных сетевых средах, требующих высокого уровня безопасности при сохранении сетевого доступа для удаленных пользователей.

Используйте RADIUS в следующих сетевых средах, требующих безопасности доступа:

- Сети с серверами доступа от разных поставщиков, каждый из которых поддерживает RADIUS. Например, серверы доступа от нескольких поставщиков используют единую базу данных безопасности на основе сервера RADIUS. В сети на основе IP с различными серверами доступа удаленные пользователи аутентифицируются через сервер RADIUS.
- Сети, в которых пользователь должен иметь доступ только к одной услуге. Используя RADIUS, вы можете контролировать доступ пользователей к одному хосту, к одной утилите, такой как Telnet, или к одному протоколу, такому как протокол двухточечной связи (PPP). Например, когда пользователь входит в систему, RADIUS определяет, что этот пользователь имеет право запускать PPP с использованием IP-адреса 10.2.3.4, и выполняются правила определенного списка доступа.
- Сети, требующие учета ресурсов. Вы можете использовать учет RADIUS независимо от аутентификации или авторизации RADIUS. Функции учета RADIUS позволяют отправлять данные в начале и в конце сеанса, указывая количество ресурсов (таких как время, пакеты, байты и т. д.), использованных во время сеанса.

RADIUS не совместим с определенными сетевыми условиями:

- RADIUS не поддерживает следующие протоколы:
- удаленный доступ AppleTalk (ARA);
- протокол управления кадрами NetBIOS (NBFCP)
- интерфейс асинхронных служб NetWare (NASI)
- соединения X.25 PAD
- в условиях работы с OLT RADIUS не обеспечивает двустороннюю аутентификацию. На OLT при работе RADIUS доступна только аутентификация входящего вызова.
- сети, использующие различные услуги. RADIUS обычно привязывает пользователя к одной модели обслуживания.

7.1.2 Принцип работы

Когда пользователь пытается войти и аутентифицироваться на сервере доступа с помощью RADIUS, выполняются следующие шаги:

1. Пользователю предлагается ввести имя пользователя и пароль.
2. Имя пользователя и зашифрованный пароль отправляются по сети на сервер RADIUS.
3. Пользователь получает один из следующих ответов от сервера RADIUS:

ACCEPT: пользователь аутентифицирован.

REJECT: пользователь не аутентифицирован и ему предлагается повторно ввести имя пользователя и пароль, или доступ запрещен.

CHALLENGE: сервером RADIUS выдается запрос для сбора дополнительных данных от пользователя.

Ответ ACCEPT или REJECT связан с дополнительными данными, которые используются для EXEC или сетевой авторизации. Вы должны сначала пройти аутентификацию RADIUS, прежде чем использовать авторизацию RADIUS. Дополнительные данные, включенные в пакеты ACCEPT или REJECT, содержат следующее:

а) службы, к которым пользователь может получить доступ, включая Telnet или Rlogin;

б) параметры подключения, включая IP-адрес хоста или клиента, список доступа и тайм-ауты пользователя.

7.2 Настройка RADIUS

Чтобы настроить RADIUS на удаленном устройстве или сервере доступа, вы должны выполнить следующие действия:

- Используйте команду **aaa authentication** в режиме глобальной конфигурации для определения списков методов аутентификации RADIUS. Дополнительные сведения об использовании команды аутентификации см. в разделе «Настройка аутентификации».
- Используйте линейные и интерфейсные команды, чтобы разрешить использование определенных списков методов. Дополнительные сведения см. в разделе «Настройка аутентификации».

Следующие действия при настройке являются необязательными:

- При необходимости запустите **aaa authorization** в режиме глобальной конфигурации, чтобы авторизовать запрос пользователя на обслуживание. Дополнительные сведения об использовании команды **aaa authorization** см. в разделе «Настройка авторизации».
- При необходимости запустите **aaa accounting record** в режиме глобальной конфигурации для отслеживания и документирования действий пользователей на устройстве.

Задачи настройки

- Настройка связи с сервером RADIUS
- Настройка для использования специфичных атрибутов поставщика
- Назначение RADIUS для аутентификации

- Назначение RADIUS для авторизации
- Назначение RADIUS для учета

7.2.1 Настройка связи коммутатора с сервером RADIUS

Хост RADIUS обычно представляет собой многопользовательскую систему с программным обеспечением сервера RADIUS от Livingston, Merit, Microsoft или другого поставщика программного обеспечения. Сервер RADIUS и коммутатор используют общую секретную текстовую строку для шифрования паролей и обмена ответами. Используйте команду **radius-server host**, чтобы указать сервер RADIUS. Используйте команду **radius-server key**, чтобы указать строку общего секретного текста (ключа).

Чтобы настроить взаимодействие с RADIUS-сервером для каждого сервера, используйте следующую команду в режиме глобальной конфигурации:

Команда	Описание
radius-server host *ip-address* [**auth-port** *port-number*] [**acct-port** *portnumber*]	Задает IP-адрес или имя хоста удаленного узла RADIUS-сервера и указывает номера портов назначения для аутентификации и учета
radius-server key *string*	Задает общую секретную текстовую строку, используемую маршрутизатором и RADIUS-сервером

Чтобы настроить глобальные коммуникационные параметры между маршрутизатором и RADIUS-сервером, используйте следующие команды в режиме глобальной конфигурации:

Команда	Описание
radius-server retransmit *retries*	Указывает, сколько раз коммутатор передает серверу каждый запрос RADIUS, прежде чем прекратить запросы (по умолчанию – 2)
radius-server timeout *seconds*	Указывает, в течение скольких секунд коммутатор ожидает ответа на запрос RADIUS, прежде чем повторно передать запрос
radius-server deadtime *minutes*	Устанавливает время (в минутах), в течение которого устройство не будет пытаться повторно связаться с удаленным RADIUS-сервером после его сбоя или отказа

7.2.2 Настройка коммутатора для использования специфичных атрибутов поставщика

Проект стандарта Internet Engineering Task Force (IETF) определяет метод передачи информации о поставщике между сервером доступа к сети и сервером RADIUS с использованием атрибута поставщика (атрибут 26). Атрибуты, специфичные для поставщика (VSA), позволяют поставщикам поддерживать свои собственные расширенные функции, не подходящие для общего использования. Дополнительные сведения об идентификаторах поставщиков и VSA см. в RFC 2138, RFC 2138, Remote Authentication Dial-In User Service (RADIUS). Чтобы настроить сервер доступа к сети для распознавания и использования VSA, выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
radius-server vsa send [authentication]	Позволяет серверу доступа к сети распознавать и использовать VSA в соответствии с атрибутом 26 RADIUS IETF

7.2.3 Назначение RADIUS для аутентификации

После определения сервера RADIUS и определения ключа аутентификации RADIUS необходимо определить списки методов для аутентификации RADIUS. Поскольку аутентификация RADIUS упрощается с помощью AAA, вы должны ввести команду **aaa authentication**, указав RADIUS в качестве метода аутентификации. Дополнительные сведения см. в разделе «Настройка аутентификации».

7.2.4 Назначение RADIUS для авторизации

Авторизация AAA позволяет установить параметры, ограничивающие доступ пользователя к сети. Авторизация с использованием RADIUS обеспечивает один метод управления удаленным доступом, включая однократную авторизацию или авторизацию для каждой службы, список и профиль учетных записей для каждого пользователя, поддержку групп пользователей и поддержку IP, IPX, ARA и Telnet. Поскольку авторизация RADIUS упрощается с помощью AAA, вы должны выполнить команду **aaa authentication**, указав RADIUS в качестве метода авторизации. Подробнее см. в разделе «Настройка авторизации».

7.2.5 Назначение RADIUS для учета

Функция учета AAA позволяет отслеживать, к каким услугам пользователи обращаются, а также объем потребляемых ими сетевых ресурсов. Поскольку учет RADIUS упрощается с помощью AAA, вы должны выполнить команду **aaa authentication**, указав RADIUS в качестве метода учета. Дополнительные сведения см. в разделе «Настройка учета».

7.3 Примеры настройки RADIUS

7.3.1 Пример аутентификации RADIUS

В следующем примере показано, как настроить коммутатор для аутентификации и авторизации с использованием RADIUS:

```
aaa authentication login use-radius group radius local
```

Эта команда настраивает удаленное устройство на использование RADIUS для аутентификации при подсказке входа в систему. Если RADIUS возвращает ошибку, пользователь аутентифицируется с использованием локальной базы данных. В этом примере use-radius – это имя списка методов, в котором указывается RADIUS, а затем – локальная аутентификация.

7.3.2 Применение RADIUS в AAA

В следующем примере показана общая конфигурация с использованием RADIUS с набором команд AAA:

```
radius-server host 1.2.3.4
radius-server key myRaDiUSpassWoRd
username root password AlongPassword
aaa authentication login admins group radius local
line vty 1 16
login authentication admins
```

Значение команд показано ниже:

Команда **radius-server host** используется для определения IP-адреса сервера RADIUS.

Команда **radius-server key** используется для определения общего ключа между сервером доступа к сети и сервером RADIUS.

Команда **aaa authentication login admins group radius local** определяет список методов аутентификации «admins», который указывает на аутентификацию RADIUS, а затем (если сервер RADIUS не отвечает) будет использоваться локальная аутентификация на последовательных линиях с использованием PPP.

Команда **login authentication admins** используются для обозначения применения списка методов «admins» во время входа в систему.

8. TACACS+

8.1 Описание

В качестве протокола управления безопасностью доступа TACACS+ обеспечивает пользователям централизованную проверку получения прав доступа к серверу сетевого доступа. Безопасность связи гарантирована, так как обмен информацией между сервером сетевого доступа и сервисной программой TACACS+ зашифрован.

Перед использованием TACACS+, настроенного на сервере сетевого доступа, необходимо получить доступ к серверу TACACS+ и настроить его. TACACS+ обеспечивает независимую модульную аутентификацию, авторизацию и учет.

Аутентификация: поддерживает несколько способов аутентификации (ASCII, PAP, CHAP и т. д.), обеспечивает возможность обработки любого диалога с пользователями (например, задавая уточняющие вопросы, такие как тип сетевого адреса, тип услуги, идентификационный номер и т. д. после предоставления логина и пароля). Кроме того, служба аутентификации TACACS+ поддерживает отправку информации на экран пользователя, например, уведомления пользователя о том, что его пароль необходимо изменить из-за настроек политики устаревания паролей.

Авторизация: детальное управление ограничением доступных для пользователя служб во время сеанса, включая настройку автоматических команд, контроль доступа, время продолжения диалога и т. д. Также возможно ограничивать функционал команд, которые может выполнять пользователь.

Учет: сбор и отправка информации для создания счетов, аудита или контроля использования сетевых ресурсов. Сетевой менеджер может использовать возможности учета, чтобы отслеживать действия пользователя для аудита безопасности или предоставлять информацию необходимую для выставления счетов пользователям, например, когда какой-то сервис оплачивается на основе использованных ресурсов, таких как пропускная способность или время доступа. Функция учета отслеживает аутентификацию пользователя, время начала и окончания сессии, выполненные команды, количество пакетов, количество байтов и т. д.

8.1.1 Работа протокола TACACS+

8.1.1.1 Аутентификация в форме ASCII

Когда пользователь входит на сервер сетевого доступа, использующий TACACS+, и запрашивает простую аутентификацию в форме ASCII, в типичных обстоятельствах может произойти следующий процесс:

Когда соединение установлено, сервер доступа связывается с сервисной программой TACACS+, чтобы получить приглашение ввода имени пользователя, а затем передает его пользователю. Пользователь вводит имя, и сервер доступа к сети снова связывается с сервисной программой TACACS+ для запроса пароля. Он показывает запрос пароля

пользователю. Пользователь вводит пароль, после чего пароль отправляется сервисной программе TACACS+.

TACACS+ допускает любые диалоги между серверной программой и пользователем, пока не соберет достаточно информации для идентификации пользователя. Обычно это достигается комбинацией запроса имени пользователя и пароля, но может также включать другие элементы, такие как идентификационный номер. Все это находится под управлением программы сервера TACACS+.

В итоге сервер доступа к сети получает один из следующих ответов от сервера TACACS+:

ACCEPT	Когда пользователь успешно проходит аутентификацию, ему предоставляются соответствующие услуги. Если сервер сетевого доступа настроен как требующий авторизацию, она начинается в этот момент
REJECT	Пользователь не проходит аутентификацию. Пользователю может быть отказано в дальнейшем доступе или ему будет предложено снова получить доступ. Это зависит от работы сервера TACACS+
ERROR	Ошибка возникает во время аутентификации, и причина может быть на сервере. Это также может произойти при сетевом соединении между сервером TACACS+ и сервером доступа к сети. Если получен ответ ERROR, обычно сервер доступа пытается идентифицировать пользователя другим способом
CONTINUE	Сервер предлагает пользователю ввести дополнительную информацию для аутентификации

8.1.1.2 Аутентификация в режимах PAP и CHAP

Вход в систему PAP (Password Authentication Protocol) похож на вход ASCII, но разница в том, что имя пользователя и пароль сервера доступа к сети находятся в сообщении PAP, а не вводятся пользователем, поэтому пользователю не будет предложено ввести соответствующую информацию. Вход в режиме CHAP (Challenge Handshake Authentication Protocol) аналогичен в основных частях, но использует определенный ключ для проверки пользователя. При этом пароль передается в хэшированном виде. После аутентификации наступает этап авторизации, если сервер доступа к сети запрашивает авторизацию для пользователя. Но перед проведением авторизации TACACS+ аутентификация должна быть уже завершена.

Если необходимо выполнить авторизацию TACACS+, нужно снова связаться с серверной программой TACACS+ и вернуться к ответу авторизации ACCEPT или REJECT. Если ответом является принятие (ACCEPT), включаются данные AV (атрибут-значение), используемые для

указания пользовательского исполнительного (EXEC) или сетевого (NETWORK) диалога и подтверждения доступных пользователю услуг.

8.2 Настройка TACACS+

Чтобы настроить поддержку TACACS+, необходимо выполнить следующие процедуры:

Используйте команду **tacacs-server** для назначения одного или нескольких IP-адресов сервера TACACS+. Используйте команду **tacacs key**, чтобы назначить зашифрованный секретный ключ для всей информации, которой обмениваются сервер сетевого доступа и сервер TACACS+. Такой же секретный ключ необходимо настроить в серверной программе TACACS+.

Используйте команду глобальной конфигурации **aaa authentication**, чтобы определить список методов, который использует TACACS+ для аутентификации. Дополнительную информацию о команде **aaa authentication** см. в разделе «Настройка аутентификации».

Используйте команды **line** и **interface**, чтобы применить определенную таблицу методов к интерфейсам или линиям. Дополнительную информацию см. в разделе «Настройка аутентификации».

Задачи настройки

- Назначение сервера TACACS+
- Настройка секретного ключа шифрования TACACS+
- Назначение TACACS+ для аутентификации
- Назначение TACACS+ для авторизации
- Назначение TACACS+ для учета

8.2.1 Назначение сервера TACACS+

Команда **tacacs-server** может помочь назначить IP-адрес сервера TACACS+. Поскольку TACACS+ ищет хосты в определенной последовательности, этот механизм полезен для серверов, которые настроены с разными приоритетами. Чтобы назначить хост TACACS+, используйте следующие команды в режиме глобальной конфигурации:

Команда	Описание
tacacs-server host *ip-address* [**single-connection**| **multi-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]	Команда предназначена для назначения IP-адреса сервера TACACS+ и связанных с ним параметров

При помощи команды **tacacs-server** настраиваются следующие параметры:

- Ключевое слово **single-connection** указывает на использование одиночного соединения. Это позволит серверной программе выполнять больше операций TACACS+ и работать более эффективно. Множественное соединение (**multi-connection**) означает использование нескольких TCP-соединений.
- Параметр **port** определяет номер интерфейса TCP, который используется серверной программой TACACS+. Номер интерфейса по умолчанию – 49.
- Параметр **timeout** обозначает верхний предел времени в секундах для ожидания ответа от сервера.
- Параметр **key** применяется для назначения секретных ключей шифрования сообщений.

После использования сервера TACACS+ для авторизации, соединитесь с хостом и установите значение таймаута, определенное командой **timeout**. Это значение будет заменять глобальное значение таймаута, настроенное командой **tacacs-server timeout**. Вместо ключа шифрования по умолчанию, настроенного с помощью **tacacs-server key**, используйте ключ, присвоенный сервером TACACS+. Это позволит настроить уникальное подключение TACACS+ с целью улучшения защиты сети.

8.2.2 Настройка секретного ключа шифрования TACACS+

Чтобы настроить секретный ключ шифрования сообщений TACACS+, используйте следующую команду в режиме глобальной конфигурации:

Команда	Описание
tacacs-server key *keystring*	Задает ключ шифрования, соответствующий ключу, используемому сервером TACACS+

Для успешного шифрования тот же секретный ключ должен быть настроен для программы сервера TACACS+.

8.2.3 Назначение TACACS+ для аутентификации

После определения сервера TACACS+ и связанного с ним ключа шифрования необходимо определить список методов для аутентификации TACACS+. Поскольку аутентификация TACACS+ осуществляется с помощью AAA, нужно назначить TACACS+ в качестве способа аутентификации при помощи команды **aaa authentication**. Дополнительную информацию см. в разделе «Настройка аутентификации».

8.2.4 Назначение TACACS+ для авторизации

Авторизация AAA может помочь настроить параметр для ограничения доступа пользователя к сети. Авторизация TACACS+ может быть применена к различным службам и функциям, таким как выполнение команд, сетевые подключения, диалоги EXEC и т. д. Поскольку авторизация TACACS+ осуществляется с помощью AAA, нужно назначить TACACS+ в качестве способа авторизации при помощи команды **aaa authorization**. Дополнительную информацию см. в разделе «Настройка авторизации».

8.2.5 Назначение TACACS+ для учета

Учет AAA позволяет отслеживать текущие программы пользователя и количество потребляемых им сетевых ресурсов. Поскольку учет TACACS+ осуществляется с помощью AAA, нужно назначить TACACS+ в качестве способа учета при помощи команды **aaa accounting**. Дополнительную информацию см. в разделе «Настройка учета».

8.3 Примеры настройки TACACS+

8.3.1 Настройка аутентификации TACACS+

Следующая настройка аутентификации при входе выполняется с помощью TACACS+:

```
aaa authentication login test group tacacs+ local
tacacs-server host 1.2.3.4
tacacs-server key testkey
line vty 0
login authentication test
```

В этом примере команда **aaa authentication** определяет список методов аутентификации **test**, используемый на vty0. Ключевое слово **tacacs+** означает, что аутентификация обрабатывается TACACS+ и, если TACACS+ не отвечает во время аутентификации, ключевое слово **local** указывает на использование для аутентификации локальной базы данных на сервере сетевого доступа.

Команда **tacacs-server host** указывает IP-адрес сервера TACACS+ как 1.2.3.4. Команда **tacacs-server key** определяет общий секретный ключ шифрования как **testkey**.

В следующем примере показан протокол безопасности, используемый во время настройки TACACS+ в качестве средства аутентификации. В данном случае применяется список методов **default**, а не **test**:

```
aaa authentication login default group tacacs+ local
tacacs-server host 1.2.3.4
```

tacacs-server key goaway

В этом примере команда **aaa authentication** определяет стандартный список методов аутентификации default во время аутентификации при входе в систему. Если требуется аутентификация, ключевое слово **tacacs+** означает аутентификацию с помощью TACACS+. Если TACACS+ не отвечает, ключевое слово **local** указывает на использование для аутентификации локальной базы данных на сервере доступа к сети.

Команда **tacacs-server host** указывает IP-адрес сервера TACACS+ как 1.2.3.4. Команда **tacacs-server key** определяет общий секретный ключ как **goaway**.

8.3.2 Настройка авторизации TACACS+

aaa authentication login default group tacacs+ local

aaa authorization exec default group tacacs+

tacacs-server host 10.1.2.3

tacacs-server key goaway

В этом примере команда **aaa authentication** определяет стандартный список методов аутентификации **default**. Если требуется аутентификация, ключевое слово **tacacs+** означает аутентификацию с помощью TACACS+. Если TACACS+ не отвечает, ключевое слово **local** указывает на использование для аутентификации локальной базы данных на сервере доступа к сети.

Команда **aaa authorization** выполняет авторизацию сетевых служб с помощью TACACS+.

Команда **tacacs-server host** указывает IP-адрес сервера TACACS+ как 10.1.2.3. Команда **tacacs-server key** определяет общий секретный ключ шифрования как **goaway**.

8.3.3 Настройка учета TACACS+

Следующая конфигурация использует TACACS+ в качестве одного из методов настройки учета:

aaa authentication login default group tacacs+ local

aaa accounting exec default start-stop group tacacs+

tacacs-server host 10.1.2.3

tacacs-server key goaway

В этом примере команда **aaa authentication** определяет стандартный список методов аутентификации **default**. Если требуется аутентификация, ключевое слово **tacacs+** означает аутентификацию с помощью TACACS+. Если TACACS+ не отвечает, ключевое слово **local** указывает на использование для аутентификации локальной базы данных на сервере доступа к сети.

Команда **aaa account** выполняет учет сетевых услуг с помощью TACACS+. В этом примере соответствующая информация о времени начала и окончания сеанса учитывается и отправляется на сервер TACACS+.

Команда **tacacs-server host** указывает IP-адрес сервера TACACS+ как 10.1.2.3. Команда **tacacs-server key** определяет общий ключ шифрования как **goaway**.

9. Настройка HTTP

Настройку коммутатора можно проводить не только через командную строку и SNMP, но и через веб-браузер. Коммутаторы поддерживают настройку HTTP, времени ожидания для нормальных и ненормальных пакетов и т. д.

9.1 Выбор языка подсказок

Язык подсказок можно переключать с помощью следующей команды.

Команда	Описание
[**no**] **ip http language** {**english**}	Выбрать в качестве языка подсказок английский

9.2 Настройка HTTP-порта

Как правило, HTTP-портом по умолчанию является порт 80, и пользователи могут получить доступ к коммутатору, введя IP-адрес напрямую; однако коммутатор также поддерживает возможность изменения служебного порта, после чего для доступа к нему потребуется использовать IP-адрес и измененный порт. Например, если вы установите IP-адрес и служебный порт на 192.168.1.3 и 1234 соответственно, адрес доступа HTTP следует изменить на http:// 192.168.1.3:1234. Порты других распространенных протоколов лучше не использовать, чтобы не произошло коллизии доступа. Поскольку порты, используемые многими протоколами, трудно запомнить, лучше использовать идентификаторы портов (ID), превышающие 1024.

Команда	Описание
ip http port {*portNumber*}	Устанавливает HTTP-порт

9.3 Включение службы HTTP

Коммутатор поддерживает управление HTTP-доступом. Только когда служба HTTP включена, может происходить обмен HTTP между коммутатором и ПК, а когда служба закрыта, обмен HTTP-данными прекращается.

Команда	Описание
ip http server	Запускает службу HTTP

9.4 Настройка режима доступа HTTP

Вы можете получить доступ к коммутатору в двух режимах: доступ по HTTP и доступ по HTTPS. Для выбора режима HTTP введите следующую команду:

Команда	Описание
ip http http-access enable	Устанавливает режим доступа HTTP

9.5 Установка максимального количества записей VLAN на веб-странице

Коммутатор поддерживает не более 4094 VLAN, и в большинстве случаев Web отображает ограниченное число VLAN, то есть те VLAN, которые пользователи хотят видеть. Вы можете использовать следующую команду, чтобы установить максимальное количество VLAN. Максимальное количество VLAN по умолчанию равно 100.

Команда	Описание
ip http web max-vlan {*max-vlan*}	Устанавливает максимальное количество записей VLAN, отображаемых на веб-странице

9.6 Установка максимального количества многоадресных записей на веб-странице

Коммутатор поддерживает не более 100 многоадресных записей. Вы можете запустить следующую команду, чтобы установить максимальное количество записей многоадресной рассылки, а затем Web отобразит эти записи. Максимальное количество записей многоадресной рассылки по умолчанию равно 15.

Команда	Описание
ip http web igmp-groups {*igmp-groups*}	Устанавливает максимальное количество многоадресных записей, отображаемых на веб-странице

9.7 Настройка HTTPS

В целях повышения безопасности связи коммутаторы поддерживают не только протокол HTTP, но и протокол HTTPS. HTTPS – это HTTP-канал, предназначенный для обеспечения безопасности, и он использует протокол SSL/TLS для создания защищенной связи между клиентом и сервером.

9.7.1 Настройка режима доступа HTTPS

Вы можете запустить следующую команду, чтобы установить режим доступа HTTPS.

Команда	Описание
ip http ssl-access enable	Устанавливает режим доступа HTTPS

9.7.2 Настройка HTTPS-порта

Аналогично HTTP, HTTPS имеет свой служебный порт по умолчанию – порт 443. Вы также можете запустить следующую команду, чтобы изменить служебный порт HTTPS. Рекомендуется использовать значение ID выше 1024, чтобы избежать конфликтов с портами других протоколов.

Команда	Описание
ip http secure-port {*portNumber*}	Устанавливает HTTPS-порт

10. Доступ к коммутатору

10.1 Доступ к коммутатору через HTTP

При доступе к коммутатору с помощью Web убедитесь, что используемый браузер соответствует следующим требованиям:

- HTML не ниже версии 4.0
- HTTP не ниже версии 1.1
- JavaScriptTM не ниже версии 1.5

Кроме того, убедитесь, что основной программный файл, работающий на коммутаторе, поддерживает доступ в Интернет, а ваш компьютер уже подключен к сети, в которой находится коммутатор.

10.1.1 Первоначальный доступ к коммутатору

При первоначальном доступе к коммутатору вы можете использовать веб-интерфейс без каких-либо дополнительных настроек:

1. Измените IP-адрес сетевого адаптера и маску подсети вашего компьютера на 192.168.0.2 и 255.255.255.0 соответственно.

2. Откройте веб-браузер и введите 192.168.0.1 в адресную строку. Следует отметить, что 192.168.0.1 является адресом управления коммутатором по умолчанию.

3. Если используется браузер Internet Explorer, вы можете увидеть диалоговое окно, изображенное на рисунке 10-1. И исходное имя пользователя, и пароль – «admin», то есть с учетом заглавных букв.

Рисунок 10-1 – Диалоговое окно входа

4. После успешной аутентификации систематизированная информация о коммутаторе появится в браузере.

10.1.2 Обновление до веб-версии

После обновления прошивки до версии, поддерживающей веб-интерфейс, если у коммутатора уже были сохранены файлы конфигурации до обновления, прямой доступ к нему через веб-интерфейс становится недоступным. Для исправления этой ситуации выполните следующие шаги один за другим:

1. Подключитесь с помощью вспомогательного кабеля к консольному порту коммутатора или по telnet к адресу управления коммутатором через компьютер.

2. Войдите в режим глобальной конфигурации коммутатора через командную строку (приглашение DOS – «Switch_config#»).

3. Если адрес управления коммутатором не настроен, создайте интерфейс VLAN и настройте IP-адрес.

4. Введите команду **ip http server** в режиме глобальной конфигурации и запустите веб-службу.

5. Запустите **username**, чтобы установить имя пользователя и пароль коммутатора. Чтобы узнать, как использовать эту команду, обратитесь к разделу «Аутентификация, авторизация и учет» настоящего руководства.

После выполнения вышеупомянутых шагов вы можете ввести адрес коммутатора в веб-браузере, чтобы получить доступ к коммутатору.

6. Выполните **write**, чтобы сохранить текущие настройки в файле конфигурации.

10.2 Доступ к коммутатору через безопасное соединение

Данные между веб-браузером и коммутатором не будут зашифрованы, если вы получаете доступ к коммутатору через обычный HTTP. Чтобы зашифровать эти данные, вы можете использовать безопасное соединение, основанное на протоколе SSL.

Для этого следует выполнить следующие шаги:

1. Подключитесь с помощью вспомогательного кабеля к консольному порту коммутатора или по telnet к адресу управления коммутатором через компьютер.

2. Войдите в режим глобальной конфигурации коммутатора через командную строку (приглашение DOS – «Switch_config#»).

3. Если адрес управления коммутатором не настроен, создайте интерфейс VLAN и настройте IP-адрес.

4. Введите команду **ip http server** в режиме глобальной конфигурации и запустите веб-службу.

5. Запустите **username**, чтобы установить имя пользователя и пароль коммутатора. Чтобы узнать, как использовать эту команду, обратитесь к разделу 6 «Настройка AAA» настоящего руководства.

6. Запустите **ip http ssl-access enable**, чтобы включить безопасный доступ к коммутатору.

7. Запустите **no ip http http-access enable**, чтобы запретить доступ к коммутатору через небезопасное соединение HTTP.

8. Выполните **write**, чтобы сохранить текущие настройки в файле конфигурации.

9. Откройте веб-браузер на ПК, к которому подключается коммутатор, введите https://192.168.0.1 в адресной строке (192.168.0.1 – это IP-адрес управления коммутатором) и нажмите клавишу Enter. Затем к коммутатору можно получить доступ через безопасное соединение.

11. Настройка интерфейсов

11.1 Введение

Этот раздел содержит общую информацию, которая может применяться ко всем типам интерфейсов.

11.1.1 Поддерживаемые типы интерфейсов

Информацию о типах интерфейсов см. в следующей таблице:

Тип интерфейса	Описание
Интерфейс Ethernet	Fast Ethernet Gigabit Ethernet
Логический интерфейс	Интерфейс группы агрегации Интерфейс VLAN

Поддерживаются два типа интерфейса: интерфейс Ethernet и логический интерфейс. Тип Ethernet-интерфейса зависит от конфигурации конкретного устройства, а также наличия сетевой карты или модуля, установленного на коммутаторе. Логический интерфейс – это виртуальный порт, изначально не имеющий соответствующего физического устройства, который настраивается пользователем вручную.

Поддерживаемые интерфейсы Ethernet нашего коммутатора включают:

- интерфейс Fast Ethernet;
- интерфейс Gigabit Ethernet.

Поддерживаемые логические интерфейсы включает в себя:

- интерфейс группы агрегации;
- интерфейс VLAN.

11.1.2 Общие настройки интерфейсов

Данное описание относится к процессу настройки всех интерфейсов. Выполните следующие шаги в режиме глобальной конфигурации.

1. Запустите команду **interface**, чтобы войти в режим настройки интерфейса. В это время подсказка в командной строке показывает сокращенную форму названия интерфейса, который необходимо настроить. Используйте эти интерфейсы в порядке возрастания их номеров. Номера назначаются во время установки или при добавлении сетевой карты в систему. Запустите команду **show interface**, чтобы отобразить эти интерфейсы. Каждый интерфейс, поддерживаемый устройством, отображает собственное состояние следующим образом:

```
Switch_config# show interface g0/2
GigaEthernet0/2 is administratively down, line protocol is down
  Hardware is Giga-Combo-FX, address is 00e0.0f8d.e0e1 (bia 00e0.0f8d.e0e1)
  MTU 1500 bytes, BW 10000 kbit, DLY 10 usec
  Encapsulation ARPA
```

port info 1 0 2 1

Auto-duplex, Auto-speed

flow-control off

Received 0 packets, 0 bytes

0 broadcasts, 0 multicasts

0 discard, 0 error, 0 PAUSE

0 align, 0 FCS, 0 symbol

0 jabber, 0 oversize, 0 undersize

0 carriersense, 0 collision, 0 fragment

0 L3 packets, 0 discards, 0 Header errors

Transmitted 0 packets, 0 bytes

0 broadcasts, 0 multicasts

0 discard, 0 error, 0 PAUSE

0 sqettest, 0 deferred

0 single, 0 multiple, 0 excessive, 0 late

0 L3 forwards

Нет необходимости добавлять пробел между типом интерфейса и его номером. Например, в приведенном примере возможны оба варианта написания: g0/2 или g 0/2.

---

2. Вы можете проверить действие различных команд в режиме настройки интерфейса. Команды определяют протоколы и прикладные программы, которые должны выполняться на интерфейсе. Эти команды будут действовать до тех пор, пока пользователь не выйдет из режима настройки интерфейса или не переключится на другой интерфейс.

3. После завершения настройки интерфейса для проверки его состояния используйте команду **show** (см. раздел «Мониторинг и поддержка интерфейса»).

11.2 Конфигурация интерфейсов

11.2.1 Настройка общих атрибутов интерфейса

Далее описывается команда, которую можно выполнить на интерфейсе любого типа, и настроить общие атрибуты интерфейса. Настраиваемые общие атрибуты включают описание интерфейса, пропускную способность, задержку и т.д.

11.2.1.1 Добавление описания

Добавление описания связанного интерфейса помогает запомнить прикрепленное к нему содержимое. Это описание служит только примечанием к интерфейсу, чтобы помочь определить его использование и не влияет на какие-либо функции. Описание возвращается командами **show running-config** и **show interface**. Для добавления описания используйте следующую команду в режиме настройки интерфейса:

Команда	Описание
description *string*	Добавляет описание для настраиваемого интерфейса

Примеры, относящиеся к добавлению описания интерфейса, см. в разделе «Пример описания интерфейса».

11.2.1.2 Настройка полосы пропускания

Протокол передачи данных использует информацию о пропускной способности интерфейса для принятия решения об операции. Используйте следующую команду, чтобы настроить пропускную способность для интерфейса:

Команда	Описание
bandwidth *kilobps*	Указывает ширину полосы пропускания настраиваемого интерфейса

Полоса пропускания – это всего лишь параметр маршрутизации, который не влияет на фактическую скорость передачи данных по физическому интерфейсу.

11.2.1.3 Настройка временной задержки

Протокол передачи данных использует информацию о временной задержке интерфейса для принятия решения об операции. Используйте следующую команду, чтобы настроить временную задержку в режиме настройки интерфейса:

Команда	Описание

delay *tensofmicroseconds*	Указывает временную задержку для настраиваемого интерфейса

Конфигурация временной задержки является просто информационным параметром. Эта команда не может настроить фактическую задержку интерфейса.

11.2.2 Мониторинг и поддержка интерфейса

При помощи следующих операций можно контролировать и поддерживать интерфейс:

- проверка состояния интерфейса;
- инициализация и удаление интерфейса;
- выключение и включение интерфейса.

11.2.2.1 Проверка состояния интерфейса

Коммутатор поддерживает несколько команд, связанных с отображением информации об интерфейсе, включая номер версии программного и аппаратного обеспечения, состояние интерфейса. В следующей таблице перечислены некоторые команды для мониторинга интерфейса:

Команда	Описание
show interface [**type** [slot | port]]	Отображает состояние интерфейса
show running-config	Отображает текущую конфигурацию
show version	Отображает конфигурацию памяти, версию программного обеспечения, заставку и т.д.

11.2.2.2 Инициализация и удаление интерфейса

Вы можете динамически устанавливать и удалять логические интерфейсы. Это также относится к субинтерфейсу и многоканальному интерфейсу. Используйте следующую команду для инициализации и удаления интерфейса в режиме глобальной конфигурации:

Команда	Описание
no interface [**type** [*slot* | *port*]]	Инициализирует физический интерфейс или удаляет виртуальный

11.2.2.3 Выключение и включение интерфейса

Когда интерфейс закрыт, все функции этого интерфейса отключаются, а сам он помечается как недоступный во всех командах мониторинга. Эта информация может передаваться другим коммутаторам по протоколу динамической маршрутизации.

Используйте следующую команду, чтобы отключить или включить интерфейс в режиме настройки интерфейса:

Команда	Описание
shutdown	Выключает интерфейс
no shutdown	Включает интерфейс

Вы можете использовать команду **show interface** и команду **show running-config**, чтобы проверить, был ли закрыт интерфейс. Отключенный интерфейс, отображается как «administratively down» в ответе команды **show interface**. Для получения более подробной информации см. раздел «Пример отключения интерфейса».

11.2.3 Настройка интерфейса Ethernet

В этом разделе будет описана процедура настройки интерфейса Ethernet. Подробная процедура включает несколько шагов, среди которых обязательным является только первый.

11.2.3.1 Выбор интерфейса Ethernet

Выполните следующую команду в режиме глобальной конфигурации, чтобы войти в режим настройки интерфейса Ethernet:

Команда	Описание
interface gigaethernet [*slot* | *port*]	Вход в режим настройки интерфейса Gigabit-Ethernet

Команда **show interface gigaethernet** [*slot* | *port*] может использоваться для отображения состояния интерфейса Gigabit-Ethernet.

11.2.3.2 Настройка скорости

Скорость Ethernet может быть реализована не только с помощью автосогласования, но и с помощью настройки интерфейса.

Команда	Описание
speed {**10**|**100**|**auto**} (T port) **speed** {**100**|**1000**|**auto**} (SFP port)	Устанавливает скорость Ethernet на 10M, 100M, 1000M или автосогласование
no speed	Восстанавливает настройки по умолчанию. Скорость устанавливается в режим автосогласования

Скорость оптического интерфейса зависит от его модели. Например, скорость GE-FX составляет 1000 Мбит/с, но при настройке ее также можно указать равной 100 Мбит/с. Скорость FE-FX составляет 100M. Если после команды **speed** есть параметр **auto**, интерфейс может включить функцию автоматического согласования. В противном случае скорость оптического интерфейса является фиксированной и не может быть согласована. Гигабитный порт может поддерживать режим 10 100 1000 в автоматическом режиме. Конкретная настройка зависит от запроса от каждого порта.

11.2.3.3 Настройка дуплексного режима интерфейса

По умолчанию интерфейсы Ethernet могут автоматически согласовывать, будут ли они дуплексными или полудуплексными. Дуплексный режим для гигабитного интерфейса всегда автоматический.

Команда	Описание
duplex {**full** |**half** | **auto**}	Устанавливает дуплексный режим интерфейса Ethernet
no duplex	Восстанавливает настройки по умолчанию. Дуплексный режим согласуется автоматически

11.2.3.4 Настройка управления потоком на интерфейсе

Когда интерфейс находится в полнодуплексном режиме, управление потоком осуществляется с помощью кадра PAUSE, определенного в стандарте 802.3X. В полудуплексном режиме данная функция реализуется обратным давлением (back pressure).

Команда	Описание
flow-control *on* |*off* | *auto*	Включает или отключает управление потоком на интерфейсе
no flow-control	Восстанавливает настройки по умолчанию, то есть управление потоком на интерфейсе отсутствует

Разница между «flow-control auto» и «flow-control on» заключается в том, что во втором случае кадр управления потоком принимается принудительно. В то время как при использовании параметра «flow-control auto» кадр управления потоком пересылается только при успешном согласовании устройств в сети.

11.2.4 Настройка логистического интерфейса

В этом разделе описывается, как настроить логический интерфейс. Содержание следующее:

- настройка интерфейса агрегации;
- настройка интерфейса VLAN.

11.2.4.1 Настройка интерфейса агрегации

Проблема недостаточной пропускной способности одного интерфейса Ethernet решается путем создания виртуального интерфейса агрегации. Он может связать вместе несколько полнодуплексных физических интерфейсов с одинаковой скоростью, что значительно повышает пропускную способность.

Выполните следующую команду, чтобы определить интерфейс агрегации:

Команда	Описание
interface port-aggregator *number*	Настраивает интерфейс агрегации

11.2.4.2 Настройка интерфейса VLAN

Интерфейс VLAN – это интерфейс маршрутизации в коммутаторе. Команда **vlan** в режиме глобальной конфигурации только добавляет в систему VLAN второго уровня, не определяя, как поступать с IP-пакетом, адрес назначения которого находится в VLAN. Если интерфейса VLAN нет, такие пакеты будут отброшены.

Выполните следующую команду, чтобы определить интерфейс VLAN:

Команда	Описание
Interface vlan *number*	Настраивает интерфейс VLAN

12. Примеры настройки интерфейса

12.1 Настройка общедоступных атрибутов интерфейса

12.1.1 Пример описания интерфейса

В следующем примере показано, как добавить описание, относящееся к интерфейсу. Это описание отображается в файле конфигурации и на дисплее команд интерфейса.

```
interface vlan 1
ip address 192.168.1.23 255.255.255.0
```

12.1.2 Пример отключения интерфейса

В следующем примере показано, как отключить интерфейс Ethernet 0/1:

```
interface GigaEthernet0/1
shutdown
```

В следующем примере показано, как включить интерфейс Ethernet 0/1:

```
interface GigaEthernet0/1
no shutdown
```

13. Настройка диапазона интерфейсов

13.1 Введение

В процессе настройки бывают случаи, когда приходится настраивать один и тот же атрибут на портах одного типа. Во избежание повторной настройки на каждом порту мы предоставляем режим настройки диапазона интерфейсов. Вы можете настроить порты одного типа и номера слота с одинаковыми параметрами конфигурации.

Перед входом в режим настройки диапазона интерфейсов следует убедиться, что все интерфейсы диапазона установлены и инициализированы.

13.2 Вход в режим диапазона интерфейсов

Выполните следующую команду, чтобы войти в режим диапазона интерфейсов.

Команда	Описание
interface range *type slot/port1-port2*[,*port3-port4*]	Вход в режим настройки диапазона интерфейсов. *type*: относится к типу настраиваемых интерфейсов. *slot*: определяет номер конкретного модуля или шасси, на котором расположены порты. *port1-port2*: обозначает диапазон портов, которые будут настроены. Диапазон отделяется дефисом, вокруг дефиса не должно быть пробелов.

	[,*port3-port4*]: можно указать необязательный дополнительный диапазон портов, разделенных запятой; также не должно быть пробелов вокруг запятой

13.3 Пример настройки

Войдите в режим настройки интерфейса с помощью команды **interface range** со следующими параметрами:

switch_config# interface range gigaEthernet 0/1-4

switch_config_if_range#

14. Настройка дополнительных возможностей порта

14.1 Изоляция портов

В нормальных условиях пакет данных может быть перенаправлен между различными портами коммутаторов. Иногда требуется ограничить передачу данных между портами, и для этого используется функция изоляции портов. Существуют два типа изоляции: не основанная на группе и основанная на группе. В первом случае, изолированные порты не могут передавать данные друг другу, но могут обмениваться данными с неизолированными портами. Во втором случае, изолированные порты в группе не могут осуществлять передачу данных между собой, однако могут обмениваться данными с портами вне группы. Важно отметить, что функция изоляции портов применяется только к сообщениям уровня 2 модели OSI и не поддерживает изоляцию на основе групп.

Изоляция по негрупповому признаку:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в интерфейс, который нужно настроить
[no] **switchport protected**	Включить/отключить функцию изоляции портов
exit	Вернуться в режим глобальной конфигурации
exit	Вернуться в режим управления

Изоляция по групповому признаку:

Команда	Описание
config	Вход в режим глобальной конфигурации

[no] **port-protected** *group-id*	Создать и включить режим изолированной группы. *group-id* означает настройку идентификатора группы изоляции
[no] **description** *word*	Описание группы. *word* означает текстовую строку группы
exit	Вернуться в режим глобальной конфигурации
interface g0/1	Вход в интерфейс, который нужно настроить
[no] **switchport protected** *group-id*	Добавить/удалить изолированную группу. *group-id* означает ранее настроенный идентификатор группы
exit	Вернуться в режим глобальной конфигурации
exit	Вернуться в режим управления

14.2 Управление штормами

Порты коммутатора могут быть атакованы постоянными аномальными одноадресными (сбой определения MAC-адреса), многоадресными или широковещательными сообщениями. Это может привести к выходу из строя портов коммутатора и даже всего коммутатора. Поэтому был предусмотрен механизм для сдерживания этого явления. Функция управления штормом может устанавливать разные скорости на входе для разных типов сообщений, которым разрешено поступать на коммутатор.

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в интерфейс, который нужно настроить
[no] **storm-control** {**broadcast** | **multicast** | **unicast**} **threshold** *count*	Настройка функции управления штормом на порту. **Unicast** означает, что контролируются неизвестные одноадресные пакеты. **Multicast** означает, что контролируется многоадресная рассылка. **Broadcast** означает, что контролируется широковещательная рассылка.

	Count означает пороговое значение, которое необходимо настроить
exit	Вернуться в режим глобальной конфигурации
exit	Вернуться в режим управления

14.3 Ограничение скорости порта

Данная функция используется для ограничения скорости входящего и исходящего потока порта. Используйте следующие команды для ограничения скорости потока после входа в режим управления:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в интерфейс, который нужно настроить
[no] **switchport rate-limit** {*band* | **bandwidth** *percent}* {**ingress** | **egress**}	Настройка ограничения скорости потока для порта. *Band* – это предельная скорость потока. *Percent* – это ограничение потока в процентах. **Ingress** – настройка для входящего потока. **Egress** – настройка для исходящего потока
exit	Вернуться в режим глобальной конфигурации
exit	Вернуться в режим управления

14.4 Обнаружение петель на порту

Функция обнаружения петель используется для определения наличия петли на порту. Временной интервал сообщений об обнаружении петель, отправляемых портом, можно настроить. Для этого используйте следующую команду после входа в режим управления:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в интерфейс, который нужно настроить
[no] **keepalive** [*second*]	Настройка временного интервала сообщений об обнаружении петель, отправляемых портом.

	Second – это временной интервал отправки сообщений в секундах
exit	Вернуться в режим глобальной конфигурации
exit	Вернуться в режим управления

14.5 Изучение MAC-адреса порта

Функция используется для включения/выключения изучения MAC-адреса порта. Метод настройки следующий:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в интерфейс, который нужно настроить
[no] **switchport disable-learning**	Настройка изучения MAC-адреса порта. Включить/выключить функцию изучения MAC-адреса порта
exit	Вернуться в режим глобальной конфигурации
exit	Вернуться в режим управления

14.6 Безопасность порта

Безопасность порта контролируется путем доступа к порту в соответствии с MAC-адресом. Функция имеет три вида режимов: динамический режим безопасности, статический режим приема и статический режим отклонения. В динамическом режиме безопасности можно настроить максимальное количество MAC-адресов, которые могут быть изучены портами. Когда максимальное количество MAC-адресов было получено с какого-либо порта коммутатором, новый MAC-адрес не будет изучен; тем временем коммутатор отбрасывает все сообщения DLF. В режиме статической безопасности для порта можно настроить статический безопасный MAC-адрес. Таким образом, разрешается принимать только те сообщения, исходный MAC-адрес которых является для порта безопасным, другие же сообщения будут отбрасываться. В режиме статического отклонения сообщения, в которых исходный MAC-адрес является безопасным MAC-адресом, будут отброшены, а другим сообщениям будет разрешен вход.

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в интерфейс, который нужно настроить

[no] **switchport port-security mode** {**dynamic** | **static** [**accept** | **reject**] | **sticky**}	Настройка режима безопасности порта. **dynamic** означает динамический режим. **static accept** означает статический режим приема. **static reject** означает статический режим отклонения
[no] **switchport port-security dynamic maximum** *num*	Настройка максимального количества изучаемых MAC-адресов
[**no**] **switchport port-security static mac-address** *H.H.H*	Настройка статического безопасного MAC-адреса
[**no**] **switchport port-security sticky** {**maximum** *sticky_number* | **mac-address** *H.H.H* | **aging-time** *aging_time*}	Настройка привязки MAC-адреса к порту. **maximum** *sticky_number* означает максимальное количество привязанных MAC-адресов. **mac-address** *H.H.H* позволяет настроить привязанный MAC-адрес вручную. **aging-time** *aging_time* – ручная настройка времени устаревания привязанных MAC-адресов
exit	Вернуться в режим глобальной конфигурации
exit	Вернуться в режим управления

14.7 Привязка интерфейса

Привязку можно проводить одновременно с IP-адресом и MAC-адресом на интерфейсе или только с IP-адресом или MAC-адресом. Функция работает для сообщений IP и ARP.

Используйте следующие команды для настройки после входа в режим управления:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в интерфейс, который нужно настроить
[no] **switchport port-security bind** | **block** {**ip** | **arp**| **both-arp-ip** *A.B.C.D* | **mac** *H.H.H*}	Настройка функции привязки интерфейса. **Bind** позволяет передавать только те сообщения, которые соответствуют требованиям привязки, а другие сообщения пропущены не будут;

	Block отклоняет только те сообщения, которые соответствуют требованиям привязки, а остальные могут быть пропущены; **Ip** означает, что функция будет работать только для IP-сообщений, которые соответствуют требованиям привязки; **Arp** означает, что функция будет работать только для сообщений arp, которые соответствуют требованиям привязки; **Both-arp-ip** означает, что функция будет работать для сообщений IP и ARP, соответствующих требованиям привязки
exit	Вернуться в режим глобальной конфигурации
exit	Вернуться в режим управления

14.8 SVL/IVL

Этот коммутатор можно настроить на общий (SVL) или независимый (IVL) режим обучения VLAN. По умолчанию все порты находятся в режиме IVL.

Коммутатор может быть связан одновременно с IP-адресом и MAC-адресом на интерфейсе или только с IP-адресом или MAC-адресом. Функция работает для сообщений IP и ARP.

Используйте следующие команды для настройки после входа в режим управления:

Команда	Описание
config	Вход в режим глобальной конфигурации
[no] **vlan shared-learning**	Настройка SVL/IVL
exit	Вернуться в режим управления

14.9 Настройка проверки связи

Проверка состояния связи на портах осуществляется путем их периодического сканирования системой.

14.9.1 Настройка временного интервала сканирования портов

При настройке временного интервала сканирования портов используйте следующую команду в режиме глобальной конфигурации:

Команда	Описание
[**no**] **link scan** {**normal** *interval* | **fast** *interval*}	**Normal** означает стандартный режим сканирования. **Fast** означает режим быстрого сканирования связи. Быстрый режим в основном применяется к служебному протоколу, такому как RSTP. *Interval* – значение временного интервала сканирования в миллисекундах

14.9.2 Пример настройки

Настройка стандартного интервала сканирования в 20 миллисекунд:

```
link scan normal 20
```

14.10 Настройка системного MTU

MTU (Maximum Transmission Unit) – максимальный размер передаваемого кадра. Настройка системного MTU позволяет задать максимальный размер передаваемого кадра в байтах, который может обрабатываться на коммутаторе. Если размер кадра данных превышает установленный MTU, то он будет разбит на более мелкие кадры, что может приводить к ухудшению производительности и задержкам передачи.

14.10.1 Установка значения MTU

Используйте следующую команду в режиме глобальной конфигурации:

Команда	Описание
[no] system mtu *mtu*	Настройка значения системного MTU

14.10.2 Пример настройки

Настройка максимального размера передаваемого кадра в 2000 байт:

```
Switch_config# system mtu 2000
```

15. Зеркалирование портов

15.1 Настройка зеркалирования

Чтобы упростить управление коммутатором, вы можете настроить зеркалирование портов и использовать определенный порт коммутатора для наблюдения за потоком, проходящим через группу портов.

Зеркалирование портов можно разделить на локальное и удаленное. Локальное зеркалирование означает копирование сообщения на другой порт того же устройства, а функция удаленного зеркалирования означает передачу сообщения на удаленное устройство через несколько сетевых узлов. Данная функция настраивается по типу группы зеркалирования, а соответствующие понятия включают порт, порт назначения, VLAN удаленного зеркалирования, TPID удаленного зеркалирования, отключение обучения порта VLAN и т. д.

При удаленном зеркалировании локальное устройство добавляет тег VLAN в зеркальное сообщение. Сообщения от различных удаленных групп зеркалирования обнаруживаются с помощью полей тега VID и TPID. Для реализации функции удаленного зеркалирования необходимо, чтобы промежуточное устройство могло передавать сообщения внутри виртуальной локальной сети удаленного зеркалирования на удаленное устройство.

Схема удаленного зеркалирования выглядит следующим образом:

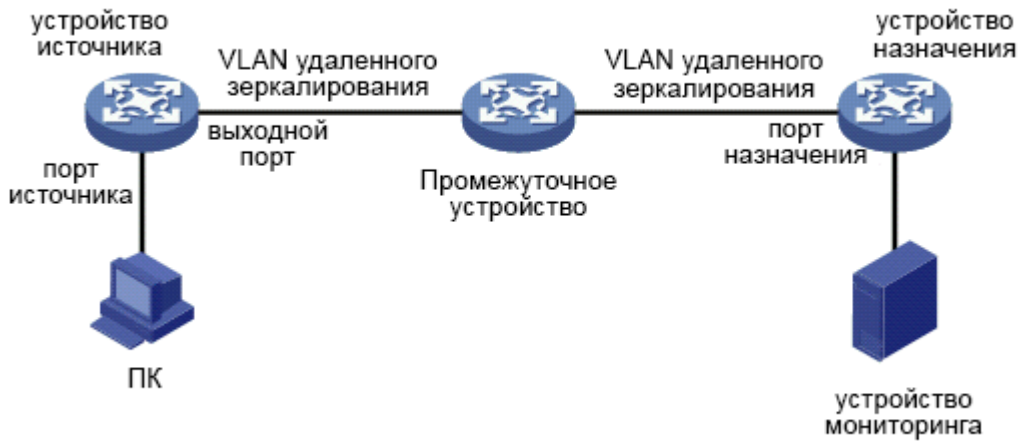

Рисунок 15-1 – Схема удаленного зеркалирования

Настройка функции удаленного зеркалирования на исходном устройстве и зеркалирование сообщения исходного порта на выходной порт с добавлением настройки RSPAN TAG в сообщении. Идентификатор VLAN в этом теге – это VLAN удаленного зеркалирования. Промежуточное устройство передает зеркальное сообщение в порт назначения посредством широковещательной рассылки. Устройство назначения передает сообщение из порта назначения на устройство мониторинга данных в соответствии с конфигурацией.

Если устройство назначения поддерживает функцию зеркалирования портов, сообщение может быть передано с порта назначения на устройство мониторинга данных путем настройки локального зеркалирования. Если устройство назначения поддерживает функцию изучения MAC-адресов на основе VLAN, сообщение может быть передано на устройство мониторинга путем отключения этой функции для VLAN удаленного зеркалирования. Если сопоставление политики QoS устройства назначения поддерживает сопоставление с виртуальной локальной сетью, сообщение может быть передано на устройство мониторинга с помощью сопоставления политики QoS.

Войдите в режим EXEC и выполните следующие шаги для настройки зеркалирования портов:

Команда	Описание
config	Вход в режим глобальной конфигурации
mirror session *session_number* {**destination** {**interface** *interface-id*} {**rspan** *vid tpid*} | **source** {**interface** *interface-id* [, | -] rx | tx | both]}	Настройка зеркалирования портов **session-number** – номер сессии зеркалирования **destination** – порт назначения **vid** тега удаленного зеркалирования **tpid** тега удаленного зеркалирования **source** – порт источника зеркалирования **rx** – входящие данные **tx** – исходящие данные **both** – входящие и исходящие данные
exit	Возвращает в режим управления
write	Сохраняет настройки

15.2 Отображение информации о зеркалировании

Запустите **show**, чтобы отобразить информацию о конфигурации зеркалирования портов.

Команда	Описание
show mirror [**session** *session_number*]	Отображает информацию о настройке зеркалирования портов **session-number** – номер зеркалирования

15.3 Пример конфигурации удаленного зеркалирования

Сетевое окружение показано на следующем рисунке:

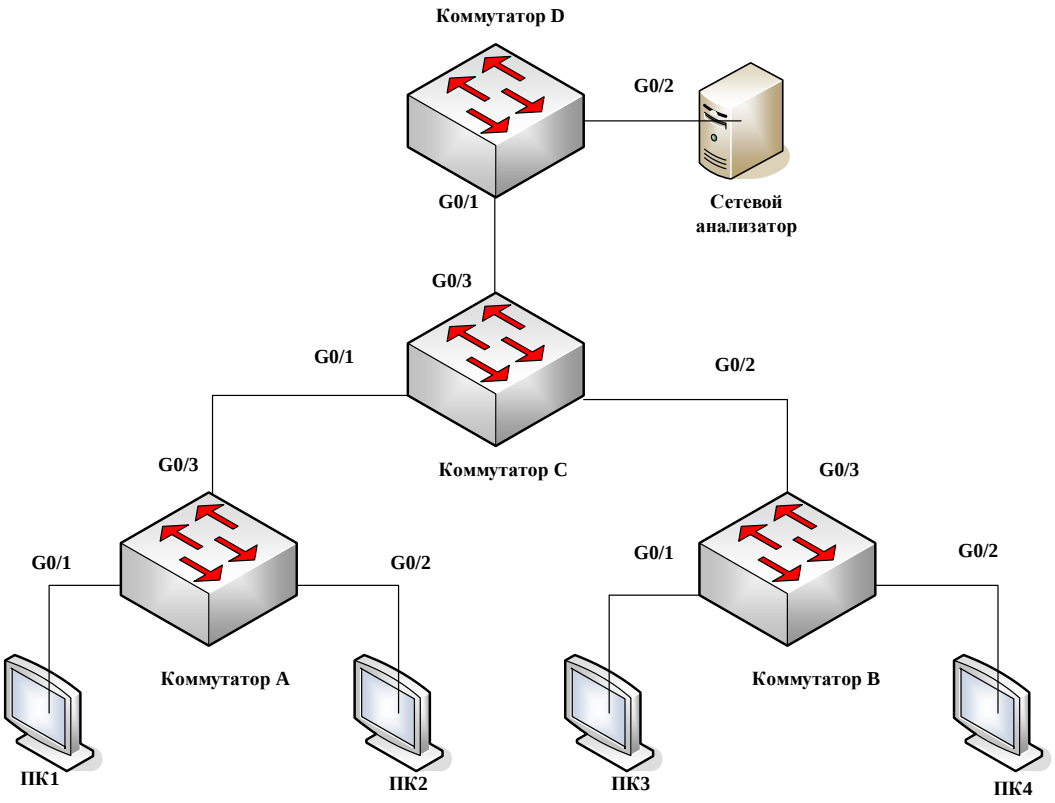

Рисунок 15-2 – Пример конфигурации зеркалирования

Пользователям необходимо контролировать поток порта g0/1 коммутатора A и порта g0/1 коммутатора B на сетевом анализаторе, что можно реализовать посредством удаленного зеркалирования. Настройка следующая:

Коммутатор A:

mirror session 1 destination interface g0/3 rspan 100 0x8100

mirror session 1 source interface g0/1 both

Коммутатор B:

mirror session 1 destination interface g0/3 rspan 1000 0x8100

mirror session 1 source interface g0/1 both

Коммутатор C:

interface GigaEthernet0/1

```
switchport mode trunk
!
interface GigaEthernet0/2
switchport mode trunk
!
interface GigaEthernet0/3
 switchport mode trunk
!
!
vlan 1,100,1000
!
```

Коммутатор D:

```
mirror session 1 destination interface g0/2
mirror session 1 source interface g0/1 both
```

16. Настройка таблицы MAC-адресов

Задачи настройки

- Настройка статического MAC-адреса
- Настройка времени устаревания MAC-адреса
- Настройка MAC-адреса blackhole
- Отображение таблицы MAC-адресов
- Удаление динамических MAC-адресов

16.1 Настройка статического MAC-адреса

Статические записи MAC-адресов – это записи MAC-адресов, которые не устаревают и могут быть удалены только вручную. В соответствии с фактическими требованиями в процессе работы вы можете добавлять и удалять статический MAC-адрес. Используйте следующую команду на привилегированном уровне, чтобы добавить и удалить статический MAC-адрес:

Команда	Описание
config	Вход в режим глобальной конфигурации

[**no**] **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	Добавить/удалить статическую запись MAC-адреса. **mac-addr** – указывает MAC-адрес. **vlan-id** – указывает номер VLAN. Диапазон допустимых значений 1~4094. **interface-id** – указывает имя интерфейса
exit	Возвращает в режим управления
write	Сохраняет настройки

16.2 Настройка времени устаревания MAC-адреса

Если динамический MAC-адрес не используется в течение указанного времени устаревания, коммутатор его из таблицы MAC-адресов. Время устаревания MAC-адреса можно настроить в соответствии с потребностями. По умолчанию значение составляет 300 секунд.

Настройте время устаревания MAC-адреса в привилегированном режиме следующим образом:

Команда	Описание
config	Вход в режим глобальной конфигурации
mac address-table aging-time [**0** | **10-1000000**]	Настройка времени устаревания MAC-адреса. **0** указывает на отсутствие времени устаревания. MAC-адрес не удаляется. Допустимое значение: от 10 до 1000000 секунд
exit	Возвращает в режим управления
write	Сохраняет настройки

16.3 Настройка MAC-адреса blackhole

Записи таблицы MAC-адресов blackhole относятся к тем записям, которым не разрешен обмен данными и которые можно удалить только вручную. MAC-адреса blackhole можно добавлять и удалять в соответствии с фактическими потребностями использования коммутатора. Для добавления и удаления MAC-адреса blackhole используются следующие команды:

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] **mac address-table blackhole** *mac-addr* **vlan** *vlan-id*	Добавление/удаление записи MAC-адреса blackhole.

	mac-addr – указывает MAC-адрес. **vlan-id** – указывает номер VLAN. Диапазон допустимых значений 1~4094
exit	Возвращает в режим управления
write	Сохраняет настройки

16.4 Отображение таблицы MAC-адресов

Поскольку в процессе работы требуются отладка и управление, пользователю необходимо знать содержимое таблицы MAC-адресов коммутатора. Используйте команду **show** для отображения содержимого таблицы.

Команда	Описание
show mac address-table [**dynamic** [**interface** *interface-id* | **vlan** *vlan-id*] | **static** | **brief** | **multicast** | **interface** *interface-id* | **vlan** *vlan-id* | **H.H.H** | **blackhole**]	**dynamic** отображает только динамические записи MAC-адресов. **interface** отображает динамические записи MAC-адресов на указанном интерфейсе. **interface-id** указывает имя интерфейса. **vlan** отображает динамические записи MAC-адресов в указанной VLAN **vlan-id** указывает номер VLAN. Диапазон допустимых значений 1~4094. **static** отображает только статические записи MAC-адресов, добавленные администратором. **brief** указывает краткую информацию о MAC-адресе. **multicast** отображает таблицу MAC-адресов многоадресной рассылки. **interface** отображает все записи MAC-адресов, связанные с указанным интерфейсом, независимо от их типа. **vlan** отображает все записи MAC-адресов в указанной VLAN, независимо от их типа. **H.H.H** отображает записи в таблице MAC-адресов, соответствующие указанному полному или частичному MAC-адресу. **blackhole** отображает записи MAC-адресов, помеченные как blackhole,

	обычно используется для блокировки определенных MAC-адресов

16.5 Удаление динамических MAC-адресов

Изученные коммутатором MAC-адреса в некоторых случаях необходимо очистить. Это может быть полезно при разрешении проблем со связностью или при изменении топологии сети.

Используйте следующую команду для удаления динамических MAC-адресов в привилегированном режиме:

Команда	Описание
clear mac address-table dynamic [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*]	Удаление динамических записей MAC-адресов. **dynamic** – означает динамические MAC-адреса. **Mac-addr** указывает конкретный MAC-адрес для удаления из таблицы. Если он указан, коммутатор удалит только запись с указанным MAC-адресом. **Interface-id** указывает интерфейс, с которого следует удалить все записи динамических MAC-адресов. **Vlan-id** указывает номер VLAN, все записи динамических MAC-адресов которой следует удалить

17. Настройка списка доступа на основе MAC-адресов

Задачи настройки

- Создание списка доступа MAC
- Настройка элементов списка доступа MAC
- Применение списка доступа MAC

17.1 Создание списка доступа

Список доступа основе MAC-адресов (MAC ACL) необходимо создать прежде чем применять его к порту. После создания этого списка, вы входите в специальный режим конфигурации, в котором можно настроить каждый элемент списка.

Войдите в привилегированный режим и выполните следующие действия, чтобы добавить или удалить список доступа основе MAC-адресов.

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] **mac access-list** *name*	Добавление или удаление MAC ACL. **name** означает имя списка

17.2 Настройка элементов списка доступа

В режиме настройки списка доступа укажите, следует ли разрешить или запретить любой MAC-адрес источника или определенный MAC-адрес источника и любой MAC-адрес назначения. Одни и те же элементы можно настроить в списке доступа только один раз.

Войдите в режим настройки MAC ACL и выполните следующие шаги, чтобы настроить запись:

Команда	Описание
[**no**] {**permit** | **deny**} {**any** | **host** *src-mac-addr* | *src-mac-addr src-mac-mask*} {**any** | **host** *dst-mac-addr* | *dst-mac-addr dst-mac-mask*} [**arp** [{**any** | *src-ip-addr*} {**any** | *dst-ip-addr*}] | *ethertype* |*cos value*]	Добавить/удалить запись MAC ACL. [**no**] – если это присутствует перед командой, оно будет использоваться для удаления соответствующего правила. {**permit** | **deny**} – выберите, разрешить (permit) или запретить (deny) трафик, удовлетворяющий критериям. {**any** | **host src-mac-addr** | **src-mac-addr src-mac-mask**} – задайте условие для MAC-адреса источника: любой (any), отдельный адрес (host src-mac-addr) или диапазон адресов (src-mac-addr src-mac-mask). {**any** | **host dst-mac-addr** | **dst-mac-addr dst-mac-mask**} – задайте условие для MAC-адреса получателя: любой (any), отдельный адрес (host dst-mac-addr) или диапазон адресов (dst-mac-addr dst-mac-mask). [**arp** [{**any** | **src-ip-addr**} {**any** | **dst-ip-addr**}] | **ethertype** |**cos value**] – определите дополнительные критерии для правила: **arp**: фильтрация трафика на основе ARP-запросов и адресов IP источника (src-ip-addr) и получателя (dst-ip-addr). **ethertype**: фильтрация трафика на основе типа Ethernet-протокола.

	cos value: фильтрация трафика согласно приоритету на основе значения CoS (Class of Service)
exit	Выйти из режима настройки списка и вернуться в режим глобальной конфигурации
exit	Возвращает в режим управления
write	Сохраняет настройки

Пример настройки MAC ACL

Switch_config# mac access-list 1

Switch_config_macl# permit host 1.1.1 any

Switch_config_macl# permit host 2.2.2 any

Switch_config# mac access-list 1: создает MAC ACL с идентификатором 1 и переводит в режим конфигурации MAC ACL (Switch-config-macl).

Switch_config_macl# permit host 1.1.1 any: добавляет правило в MAC ACL 1, которое разрешает трафик от хоста с MAC-адресом 1.1.1 к любому MAC-адресу (any).

Switch_config_macl# permit host 2.2.2 any: добавляет еще одно правило в MAC ACL 1, которое разрешает трафик от хоста с MAC-адресом 2.2.2 к любому MAC-адресу (any).

17.3 Применение списка доступа

Созданный MAC ACL можно применить к любому физическому порту. К порту можно применить только один список. Один и тот же список можно применить к нескольким портам. Войдите в привилегированный режим и выполните следующую операцию для настройки MAC ACL:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в режим настройки выбранного интерфейса
[**no**] **mac access-group** *name*	Применить/отменить MAC ACL для текущего порта. *name* – имя MAC ACL
exit	Вернуться в режим глобальной конфигурации
exit	Вернуться в режим управления
write	Сохранить настройки

18. Настройка 802.1x.

Задачи настройки

- Настройка аутентификации 802.1x на основе портов
- Настройка многопортовой аутентификации 802.1x
- Настройка повторной аутентификации 802.1x
- Настройка количества повторных аутентификаций 802.1x
- Настройка частоты передачи сообщений 802.1x
- Настройка привязки пользователя 802.1x
- Настройка метода аутентификации 802.1x для порта.
- Выбор типа аутентификации 802.1x для порта
- Настройка аутентификации MAB
- Настройка учета 802.1x
- Настройка гостевой виртуальной сети 802.1x
- Запрет использования нескольких сетевых карт
- Возобновление настроек 802.1x по умолчанию
- Мониторинг конфигурации и состояния аутентификации 802.1x

18.1 Настройка аутентификации 802.1x на основе портов

802.1x определяет три метода управления портом: обязательное подтверждение аутентификации, обязательное отклонение аутентификации и запуск аутентификации 802.1x.

Обязательное подтверждение аутентификации означает, что порт уже прошел аутентификацию. Порту больше не требуется аутентификация, и все пользователи могут осуществлять управление доступом через порт. Метод аутентификации определяется портом по умолчанию. Обязательное отклонение аутентификации означает, что аутентификация порта не проходит независимо от того, какой метод применяется. Ни один пользователь не может осуществлять доступ к данным через порт.

Запуск аутентификации 802.1x означает, что порт должен использовать протокол аутентификации 802.1x. Аутентификация 802.1x будет применяться к пользователям, имеющим доступ к порту. Только пользователи, прошедшие аутентификацию, могут осуществлять доступ к данным через порт. После запуска аутентификации 802.1x необходимо настроить метод аутентификации AAA.

Перед настройкой 802.1x выполните следующую команду, чтобы включить протокол:

Команда	Описание

dot1x enable	Включает функции 802.1x

Выполните следующую команду, чтобы запустить аутентификацию 802.1x:

Команда	Описание
dot1x port-control auto	Настраивает метод управления протоколом 802.1x на порту
aaa authentication dot1x {**default** |*list name*} *method1* [*method2*...]	Настраивает аутентификацию AAA 802.1x

Запустите одну из следующих команд в режиме настройки порта, чтобы выбрать метод управления 802.1x:

Команда	Описание
dot1x port-control auto	Включает метод аутентификации 802.1x на порту
dot1x port-control force-authorized	Утверждает обязательную аутентификацию на порту
dot1x port-control force-unauthorized	Отклоняет обязательную аутентификацию на порту
dot1x port-control misc-mab	Включает гибридную аутентификацию 802.1x

18.2 Настройка мульти-аутентификации 802.1x на основе портов

Аутентификация 802.1x предназначена для аутентификации пользователя с одного хоста. В этом случае коммутатор позволяет только одному пользователю выполнять аутентификацию и управление доступом. Другие пользователи не могут пройти аутентификацию и получить доступ, пока предыдущий не завершит сеанс. Если порт соединяет несколько хостов через коммутационные устройства, которые не поддерживают 802.1x, вы можете запустить функцию доступа множества портов, чтобы обеспечить доступ пользователям с разных хостов.

Множественная аутентификация (multi-auth) имеет два режима: режим «множество хостов» и режим «множество аутентификаций». В режиме «множество-хостов» порт переходит в активное состояние, если хотя бы один пользователь успешно прошел аутентификацию, и другие пользователи могут подключаться к устройству без прохождения аутентификации. В режиме «множество аутентификаций» коммутатор аутентифицирует каждого пользователя отдельно. Порт активируется, если хотя бы один пользователь успешно прошел аутентификацию, и деактивируется, если все пользователи не смогли пройти аутентификацию. В результате сбой одного пользователя не повлияет на доступ других пользователей к устройству.

Режим мульти-аутентификации нельзя настроить одновременно с гостевой VLAN или аутентификацией MAB. Если интерфейс находится в режиме мульти-аутентификации, все пользователи интерфейса будут аутентифицированы повторно.

Запустите следующие команды в режиме настройки интерфейса, чтобы активировать мульти-аутентификацию 802.1x:

Команда	Описание
dot1x authentication multiple-hosts	Включение режима аутентификации «множества хостов». Порт активируется только в том случае, если один пользователь проходит аутентификацию
dot1x authentication multiple-auth	Включение режима «множества аутентификаций». Пользователи не зависят друг от друга

18.3 Настройка повторной аутентификации 802.1x

В целях безопасности рекомендуется периодически повторять процедуру проверки подлинности успешно вошедшего пользователя.

В этом случае необходимо включить функцию повторной аутентификации. После запуска данной функции запрос аутентификации будет периодически отправляться на хост.

Выполните следующие команды, чтобы настроить функцию повторной аутентификации.

Команда	Описание
dot1x re-authentication	Включает функцию повторной аутентификации
dot1x timeout re-authperiod *time*	Настраивает временной интервал повторной аутентификации

18.4 Настройка количества повторных аутентификаций 802.1x

После сбоя аутентификации коммутатор повторно отправит пакет запроса для прохождения аутентификации. Если количество повторных аутентификаций превысит определенное число, а достоверного ответа по-прежнему не последует, аутентификация будет приостановлена.

Запустите следующую команду в команде настройки интерфейса, чтобы установить максимальное количество повторных аутентификаций:

Команда	Описание
dot1x reauth-max *times*	Устанавливает число повторных аутентификаций

18.5 Настройка частоты передачи сообщений 802.1x

Во время процесса аутентификации между хостом (клиентом или соискателем) и сервером аутентификации происходит обмен текстовыми сообщениями. Изменяя частоту передачи, можно управлять ответом хоста, что помогает избежать тайм-аутов, разрывов соединений и других проблем, которые могут возникнуть из-за неподходящих временных диапазонов обмена сообщениями.

Для настройки частоты передачи запустите следующую команду:

Команда	Описание
dot1x timeout tx-period *time*	Установка частоты передачи сообщений 802.1x

18.6 Настройка привязки пользователя 802.1x

При выполнении аутентификации 802.1x вы можете привязать пользователя к определенному порту, чтобы обеспечить безопасность доступа. Выполните следующую команду в режиме настройки интерфейса, чтобы создать привязку пользователя 802.1x:

Команда	Описание
dot1x user-permit *xxxz*	Настройка пользователя, привязанного к порту

18.7 Настройка метода аутентификации 802.1x для порта

Аутентификация 802.1x может выполняться разными методами на разных портах. В конфигурации по умолчанию аутентификация 802.1x использует метод **default**.

Запустите следующую команду в режиме конфигурации интерфейса, чтобы настроить метод аутентификации 802.1x:

Команда	Описание
dot1x authentication method *yyy*	Настройка метода аутентификации 802.1x

18.8 Выбор типа аутентификации 802.1x для порта

Вы можете выбрать тип аутентификации 802.1x. Тип определяет, использует ли AAA аутентификацию CHAP или EAP. Аутентификация EAP поддерживает режим MD5-challenge и режим EAP-TLS. Когда используется аутентификация CHAP, вызов (challenge), необходимый для проверки пользователя согласно MD5, генерируется локально. В случае применения аутентификации EAP вызов генерируется на сервере аутентификации. Каждый порт принимает только один тип аутентификации. Тип аутентификации, выставленный в режиме глобальной конфигурации, принимается по умолчанию. После того, как для порта установлен тип аутентификации, порт будет использовать его, если вы не запустите команду **no**, чтобы восстановить настройки по умолчанию.

EAP-TLS использует электронный сертификат в качестве гарантии аутентификации и соответствует правилам установления связи в Translation Layer Security (TLS). Таким образом гарантируется высокая безопасность.

Запустите следующую команду в режиме глобальной конфигурации, чтобы назначить тип аутентификации:

Команда	Описание
dot1x authen-type {**chap** | **eap**}	Выбор CHAP или EAP

Также выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
dot1x authentication type {**chap** | **eap**}	Выбрать для порта CHAP, EAP или тип, настроенный в глобальной конфигурации

18.9 Настройка аутентификации MAB

Если одноранговое устройство не может запустить клиентское программное обеспечение 802.1x, коммутатор перейдет в режим аутентификации MAB, а затем MAC-адрес одноранговой устройства будет отправлен как имя пользователя и пароль на RADIUS-сервер для аутентификации.

Вы можете запустить команду **dot1x mabformat** на коммутаторе, указав идентификатор учетной записи и формат пароля, чтобы убедиться, что они совпадают с данными на RADIUS-сервере.

Когда MAB включен, а одноранговое устройство не отправляет пакет eapol_start, не отвечает на пакет request_identity и превышает пороговое значение тайм-аута, коммутатор считает, что одноранговое устройство не поддерживает клиент аутентификации 802.1x, а затем переключается на аутентификацию MAB.

Режим аутентификации MAB не совместим с режимом множественной аутентификации.

Чтобы разрешить аутентификацию MAB на порту, запустите следующую команду:

Команда	Описание
dot1x mab	Включает аутентификацию MAB на порту

Чтобы установить формат MAC-адреса, вы можете запустить следующую команду в режиме глобальной конфигурации:

Команда	Описание
dot1x mabformat{1|2|3|4|5|6}	Выбирает один из шести форматов MAC-адреса, от 1 до 6. Формат по умолчанию – 1

18.10 Настройка учета 802.1x

Аутентификация и учет 802.1x могут выполняться одновременно. Механизм работы следующий: после подтверждения аутентификации dot1x определите, включена ли функция учета на интерфейсе аутентификации; если функция учета включена, отправьте запрос на учет через интерфейс AAA; когда модуль AAA возвращает сообщение об успешном ответе на запрос, интерфейс AAA сможет пересылать тексты.

После начала учёта данных, dot1x периодически отправляет сообщения Update на сервер через интерфейс AAA для получения правильной информации об учёте. В зависимости от конфигурации AAA, AAA-модуль определяет, стоит ли отправлять сообщение Update.

В то же время вам необходимо включить функцию повторной аутентификации dot1x, чтобы коммутатор мог определить, когда клиент работает некорректно.

Выполните следующие команды в режиме настройки интерфейса, чтобы включить учет dot1x и настроить метод учета:

Команда	Описание
dot1x accounting enable	Включает функцию учета dot1x
dot1x accounting method {*method name*}	Выбирает метод учёта. Значение по умолчанию – **default**

18.11 Настройка гостевой VLAN 802.1x

Гостевая VLAN предоставляет соответствующим портам некоторые права доступа (например, загрузку клиентского программного обеспечения), когда клиент не отвечает. Гостевой может быть любая настроенная виртуальная сеть в системе. Если настроенная гостевая VLAN не соответствует необходимым условиям, порты не смогут в ней работать.

В случае неудачной аутентификации право доступа к гостевой VLAN отсутствует.

Запустите следующую команду в режиме глобальной конфигурации, чтобы включить гостевую VLAN:

Команда	Описание
dot1x guest-vlan	Включает гостевую VLAN на всех портах

Если для каждого порта изначально не настроен идентификатор гостевой VLAN, она не сможет работать, даже если функция включена в глобальном режиме. Для успешной работы гостевой VLAN требуется прямо указать ее идентификатор в режиме настройки интерфейса. Запустите следующую команду в режиме настройки интерфейса, чтобы настроить идентификатор гостевой VLAN:

Команда	Описание
dot1x guest-vlan {id(1-4094)}	Указывает ID гостевой VLAN. Допустимый диапазон 1 – 4094

18.12 Запрет использования нескольких сетевых карт

Запретите соискателю использование нескольких сетевых адаптеров, чтобы предотвратить работу агентов. Запустите следующую команду в режиме настройки интерфейса:

Команда	Описание
dot1x forbid multi-network-adapter	Запрещает соискателю использование нескольких сетевых карт

18.13 Возобновление настроек 802.1x по умолчанию

Выполните следующую команду, чтобы восстановить всю глобальную конфигурацию до значений по умолчанию:

Команда	Описание
dot1x default	Восстанавливает настройки 802.1x по умолчанию

18.14 Мониторинг конфигурации и состояния аутентификации 802.1x

Чтобы отслеживать конфигурацию и состояние аутентификации 802.1x и решить, какой параметр 802.1x необходимо настроить, выполните следующую команду в режиме управления:

Команда	Описание
show dot1x {*interface* | *statistics* | *misc-mab-db*}	Отображает настройки и состояние аутентификации 802.1x

18.15 Пример настройки

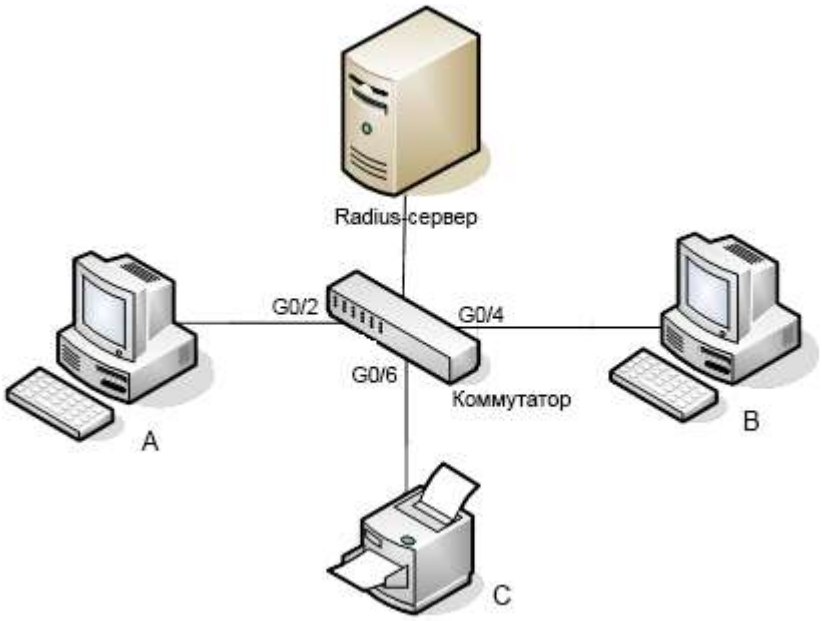

Рисунок 18-1 – Схема аутентификации 802.1x

Хост A подключается к порту G0/2 коммутатора. Хост B подключается к порту G0/4. Хост C подключается к порту G0/6. IP-адрес RADIUS-сервера – 192.168.20.2. Ключ RADIUS – TST. Порт G0/2 поддерживает удаленную аутентификацию RADIUS, привязку пользователя и повторную аутентификацию. Порт G0/4 использует локальную аутентификацию типа EAP и позволяет использовать множество хостов и гостевую виртуальную сеть. Порт G0/6 использует аутентификацию MAB, а формат MAC-адреса – AA:BB:CC:DD:EE:FF.

Общая настройка

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-G0/2 group radius
aaa authentication dot1x TST-G0/4 local
aaa authentication dot1x TST-G0/6 group radius
aaa accounting network dot1x_acc start-stop group radius
dot1x enable
dot1x re-authentication
dot1x timeout re-authperiod 10
dot1x mabformat 2
```

dot1x guest-vlan

interface VLAN1

ip address 192.168.20.24 255.255.255.0

!

vlan 1-2

radius-server host 192.168.20.2 auth-port 1812 acct-port 1813

radius-server key TST

Настройка порта G0/2

interface GigaEthernet0/2

dot1x port-control auto

dot1x authentication method TST-G0/2

dot1x user-permit radius-TST

dot1x accounting enable

dot1x accounting method dot1x_acc

Настройка порта G0/4

Interface GigaEthernet0/4

dot1x authentication multiple-hosts

dot1x port-control auto

dot1x authentication method TST-G0/4

dot1x guest-vlan 2

Настройка порта G0/6

interface GigaEthernet0/6

dot1x mab

dot1x authentication method TST-G0/6

19. Настройка GVRP

19.1 Введение

GVRP (GARP VLAN Registration Protocol) – это приложение GARP, которое обеспечивает оптимизацию VLAN, совместимую с IEEE 802.1Q, и динамическое создание VLAN на магистральных портах 802.1Q. С помощью GVRP коммутатор может обмениваться информацией о конфигурации VLAN с другими коммутаторами GVRP, отсекать ненужный широковещательный и неизвестный одноадресный трафик, а также динамически создавать и управлять сетями VLAN на коммутаторах, которые подключены через транковые порты 802.1Q.

Задачи настройки

- Глобальное включение/отключение GVRP
- Включение/отключение динамической поддержки и управления VLAN
- Включение/отключение GVRP на интерфейсе
- Мониторинг и обслуживание GVRP

19.2 Глобальное включение/отключение GVRP

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
[**no**] **gvrp**	Включает/отключает GVRP глобально

По умолчанию функция отключена.

19.3 Включение/отключение динамической поддержки и управления VLAN

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
[**no**] **gvrp dynamic-vlan-pruning**	Включает/отключает автоматическое удаление портов, не являющихся членами определенной VLAN

После включения этой функции динамическая VLAN вступает в силу только для тех портов, на которых она зарегистрирована. После запуска этой команды, если порт не зарегистрировал динамическую VLAN, он не будет принадлежать данной VLAN, даже если является магистральным и пропускает ее трафик.

По умолчанию функция отключена.

19.4 Включение/отключение GVRP на интерфейсе

Выполните следующую настройку в режиме конфигурации интерфейса:

Команда	Описание
[**no**] **gvrp**	Включает/отключает интерфейс GVRP

Чтобы порт стал активным участником GVRP, сначала необходимо включить GVRP глобально, а порт должен быть магистральным портом 802.1Q.

По умолчанию функция включена.

19.5 Мониторинг и обслуживание GVRP

Выполните следующие операции в режиме EXEC:

Команда	Описание
show gvrp statistics [**interface** port_list]	Отображает статистику GVRP
show gvrp status	Отображает информацию о глобальном состоянии GVRP
[**no**] **debug gvrp** [**packet** | **event**]	Включает/отключает отображение отладочной информации о GVRP на устройстве. **packet** – включает отладочную информацию о пакетах GVRP, предоставляя подробности о пакетах, передаваемых и получаемых устройством. **event** – включает отладочную информацию о событиях GVRP, оповещая о начатых или завершенных действиях сетевого устройства, таких как регистрация или удаление VLAN

Отображение статистики GVRP

Switch# show gvrp statistics interface Tthernet0/1

GVRP statistics on port Ethernet0/1

GVRP Status: Enabled

GVRP Failed Registrations: 0

GVRP Last Pdu Origin: 0000.0000.0000

GVRP Registration Type: Normal

Отображение информации о глобальном состоянии GVRP

Switch# show gvrp status

GVRP is enabled

19.6 Пример настройки

Чтобы сделать информацию о конфигурации VLAN коммутатора A и коммутатора B идентичной, вы можете включить GVRP на коммутаторе A и коммутаторе B. Конфигурация выглядит следующим образом:

Рисунок 19-1 – Настройка GVRP

1) Настройте порт 1, через который коммутатор A подключается к коммутатору B в качестве транкового:

Switch_config_g0/1# switchport mode trunk

2) Включите глобальный GVRP коммутатора A:

Switch_config# gvrp

3) Включите GVRP интерфейса 1 коммутатора A:

Switch_config_g0/1#gvrp

4) Настройте VLAN 10, Vlan 20 и Vlan30 на коммутаторе A:

Switch_config# vlan 10,20,30

5) Настройте порт 2, через который коммутатор B подключается к коммутатору A в качестве транкового:

Switch_config_g0/2# switchport mode trunk

6) Включите глобальный GVRP коммутатора B:

Switch_config# gvrp

7) Включите GVRP интерфейса 2 коммутатора B:

Switch_config_g0/2#gvrp

8) Настройте VLAN 40, Vlan 50 and Vlan60 на коммутаторе B:

Switch_config# vlan 40,50,60

После завершения настройки информация о конфигурации VLAN будет отображаться соответственно на коммутаторе A и коммутаторе B, то есть VLAN10, VLAN20, VLAN30, VLAN40, VLAN50 и VLAN60 на обоих коммутаторах.

20. Настройка VLAN

20.1 Введение

Понятие VLAN (виртуальная локальная сеть) относится к группе логических сетевых устройств в одной или нескольких локальных сетях, которые настроены таким образом, что могут взаимодействовать так же, как если бы были физически подключены к одному и тому же проводу, хотя на самом деле они расположены в нескольких разных сегментах сети. В 1999 году IEEE разработал проект стандарта протокола IEEE 802.1Q, используемый для стандартизации методов реализации VLAN. Поскольку VLAN основаны на логических, а не физических соединениях, они предоставляют очень широкие возможности для управления пользователями/хостами, а также распределения полосы пропускания и оптимизации ресурсов.

Существует несколько различных типов виртуальных локальных сетей и различные режимы работы их портов-участников.

- VLAN на основе портов (Port-Based): каждый порт физического коммутатора настраивается со списком доступа, определяющим членство в определенных VLAN.
- Интерфейс поддерживает магистральный режим 802.1Q (trunk mode).
- Интерфейс поддерживает режим доступа (access mode).

Port-Based VLAN предназначена для назначения порта одному из подмножеств VLAN, поддерживаемых коммутатором. Если в этом подмножестве виртуальных локальных сетей имеется только одна виртуальная локальная сеть, то этот порт является портом доступа. Если в этом подмножестве имеется несколько виртуальных локальных сетей, то этот порт является магистральным (транковым). Среди множества виртуальных сетей есть одна сеть по умолчанию, и каждому порту назначается PVID (идентификатор порта VLAN), соответствующий этой VLAN.

- На интерфейсе поддерживается диапазон допустимых VLAN (VLAN-allowed range).

Параметр VLAN-allowed используется для управления диапазоном виртуальных локальных сетей, которому принадлежит порт. Параметр VLAN-untagged используется при настройке порта для отправки пакетов без тега VLAN в соответствующую виртуальную сеть.

VLAN можно классифицировать по MAC-адресу, IP-подсети, протоколу и порту.

20.2 Туннель Dot1Q

20.2.1 Описание

Dot1Q Tunnel, так же известный как туннель QinQ – это название туннельного протокола, основанного на инкапсуляции 802.1Q, определенной в IEEE 802.1ad. Его основная идея состоит в том, чтобы инкапсулировать тег VLAN частной сети в тег публичной сети, что позволяет провайдерам обслуживать клиентские VLAN, не завися от их идентификаторов, так как клиентский трафик проходит через сеть провайдера вложенным во внешний тег VLAN (S-тег), назначенный провайдером. Это позволяет избежать конфликтов идентификаторов VLAN между клиентскими и сетевыми VLAN, а также обеспечивает дополнительный уровень изоляции, предоставляя пользователям относительно простой VPN-туннель второго уровня. Протокол Dot1Q Tunnel – это управляемый протокол, который реализуется посредством статической настройки без поддержки сигнализации и широко применяется в корпоративных сетях, которые в основном состоят из OLT или небольших MAN.

Являясь дешевым и компактным решением VPN L2, Dot1Q Tunnel становится все более популярным среди все пользователей малых сетей, когда требуется VPN. Внутри сети оператора P-устройству не обязательно поддерживать функцию туннеля Dot1Q. То есть традиционные коммутаторы L3 могут полностью удовлетворить требования, что делает сеть простой и экономичной. Коммутатор выполняет следующие функции:

- Включает Dot1Q Tunnel глобально.
- Поддерживает взаимную трансляцию между VLAN клиента и SPVLAN на порту нисходящей линии связи, включая трансляцию в плоском режиме и в режиме QinQ.
- Поддерживает настройку восходящего порта.

20.2.2 Реализация

Существует два режима реализации туннеля Dot1Q: туннель Dot1Q на основе порта и туннель Dot1Q на основе внутренней классификации тегов CVLAN.

1. Туннель Dot1Q на основе порта:

Когда порт коммутатора получает пакеты, независимо от того, имеют ли пакеты тег VLAN, коммутатор добавит к этим пакетам тег VLAN по умолчанию, к которой относится данный порт. Таким образом, если полученный пакет имеет тег VLAN, пакет становится пакетом с двойными тегами; если полученный пакет не помечен, к этому пакету будет добавлен тег VLAN по умолчанию для этого порта.

Пакет с одним тегом VLAN имеет следующую структуру, как показано в таблице 20-1:

Таблица 20-1 – Пакет с одним тегом VLAN

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Пакет с двумя тегами VLAN имеет следующую структуру, как показано в таблице 20-2:

Таблица 20-2 – Пакет с двумя тегами VLAN

DA (6B)	SA (6B)	**ETYPE(8100) (2B)**	**SPVLAN Tag (2B)**	ETYPE(8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

2. Туннель Dot1Q на основе внутреннего тега CVLAN:

Служба функционирует в соответствии с зоной CVLAN ID внутреннего тега CVLAN туннеля Dot1Q. Зону CVLAN можно преобразовать в идентификатор SPVLAN. Существует два режима трансляции VLAN: плоская (Flat) и QinQ. В режиме трансляции VLAN QinQ, когда один и тот же пользователь использует разные службы с разными идентификаторами CVLAN, услуги могут распределяться в соответствии с этими идентификаторами. Например, идентификатор CVLAN службы передачи данных (bandwidth service) находится в диапазоне от 101 до 200. Идентификатор CVLAN службы VOIP находится в диапазоне от 201 до 300. Идентификатор CVLAN службы IPTV находится в диапазоне от 301 до 400. В соответствии с диапазоном идентификаторов CVLAN, когда PE-устройство получает пользовательские данные, оно добавляет SPVLAN-тег с ID 1000 к услуге передачи данных и SPVLAN-тег с ID 3000 к услуге IPTV.

Основное различие между режимами Flat VLAN и QinQ VLAN заключается в том, как SPVLAN-тег добавляется или заменяет существующий CVLAN-тег:

- В режиме Flat VLAN трансляции, SPVLAN-тег заменяет CVLAN-тег напрямую, не добавляясь как внешний слой.
- В режиме QinQ VLAN трансляции, SPVLAN-тег добавляется к внешнему слою CVLAN-тега, создавая двойную тегированную структуру, что облегчает управление трафиком и сегментацию сети, особенно для поставщиков услуг.

20.3 Добавление/удаление VLAN

Являясь виртуальной логической сетью, VLAN имеет те же атрибуты, что и физическая локальная сеть, но позволяет группировать конечные станции, даже если они не расположены в одном сегменте локальной сети. VLAN может иметь несколько портов, и все Одноадресные, многоадресные и широковещательные сообщения будут пересылаться только на устройства внутри одной VLAN, т. е. по умолчанию они не будут передаваться на устройства в других VLAN. Если данные необходимо передать в другую VLAN, их следует пересылать через маршрутизатор или мост.

Запустите следующую команду для настройки VLAN:

Команда	Описание
vlan vlan-id	Вход в режим настройки VLAN
name str	Имя в режиме настройки VLAN
exit	Выход из режима настройки с сохранением созданной VLAN
vlan vlan-range	Одновременное создание нескольких VLAN
no vlan vlan-id | vlan-range	Удаление одной или нескольких VLAN

VLAN могут быть динамически добавлены и удалены через протокол управления VLAN GVRP.

20.4 Настройка порта коммутатора

Порт коммутатора поддерживает следующие режимы: режим доступа, режим ретрансляции, туннельный режим, туннельный режим транслирования VLAN и режим восходящего канала туннеля VLAN.

- Режим доступа (access mode) указывает, что этот порт подчиняется одной виртуальной локальной сети, отправляя и принимая только нетегированные кадры Ethernet.
- Режим ретрансляции (relay mode) указывает, что порт соединяет другие коммутаторы, и может передавать и принимать тегированный кадр Ethernet.
- Туннельный режим транслирования VLAN (VLAN translating tunnel mode) является подрежимом, основанным на режиме ретрансляции. В этом режиме порт осуществляет поиск в таблице трансляции VLAN на основе VLAN-тега принятых пакетов, чтобы получить соответствующую SPVLAN. Затем коммутационный чип заменяет исходный тег на SPVLAN или добавляет тег SPVLAN к внешнему слою оригинального тега. При передаче пакетов из порта, SPVLAN заменяется на исходный тег или же тег SPVLAN удаляется в обязательном порядке. Таким образом, коммутатор пропускает различные VLAN-разделы, имеющие доступ к сети, и передает их без изменений в другую подсеть, подключенную к другому порту того же клиента, обеспечивая прозрачную передачу данных.
- Режим внешней связи VLAN-туннеля (VLAN tunnel uplink mode) также является подрежимом, основанным на режиме ретрансляции. Для отправки пакетов через порт необходимо установить значение SPVLAN. Если пакеты находятся в диапазоне нетегированных, они передаются через порт без изменений. При получении пакетов портом происходит проверка их TPID. В случае обнаружения различий или если пакеты нетегированные, им добавляется SPVLAN-тег с их собственным TPID в качестве тега внешнего уровня.

Каждый порт имеет одну VLAN по умолчанию и один PVID, и все данные без тега VLAN, полученные на порту, относятся к пакетам данных VLAN.

Trunk-режим позволяет присваивать порту сразу несколько сетей VLAN и также настраивать, какие типы пакетов будут пересылаться и к какому числу VLAN относится порт. То есть, пакеты, отправленные через этот порт, могут быть помечены тегами (таким образом порт является членом нескольких VLAN) или быть без тегов, а список VLAN, к которым относится порт, определяется системой управления сетью.

Выполните следующую команду, чтобы настроить порт коммутатора:

Команда	Описание
switchport pvid *vlan-id*	Настройка PVID порта коммутатора
switchport mode {**access** | **trunk** | **dot1q-translating-tunnel** | **dot1q-tunnel-uplink**}	Настройка режима порта коммутатора
switchport trunk vlan-allowed …	Настройка списка VLAN, разрешенных для передачи по сетевому интерфейсу. Эта команда ограничивает передачу трафика только разрешенным VLAN, предотвращая возможность обращения устройств к другим VLAN через данный сетевой интерфейс
switchport trunk vlan-untagged …	Определяет VLAN, которая будет использоваться для немаркированного трафика, проходящего через данный магистральный порт

20.5 Создание/удаление интерфейса VLAN

Интерфейс VLAN может быть установлен для реализации управления сетью или выполнения функций маршрутизации третьего уровня. Интерфейс VLAN можно использовать для указания IP-адреса и маски. Выполните следующую команду для настройки интерфейса VLAN:

Команда	Описание
[**no**] **interface vlan** *vlan-id*	Создание/удаление интерфейса VLAN

20.6 Мониторинг конфигурации и состояния VLAN

Выполните следующие команды в режиме EXEC, чтобы отслеживать настройки и состояние VLAN:

Команда	Описание
show vlan [**id** *x* | **interface** *intf* | **dot1q-tunnel** [**interface** *intf*] | **mac-**	Отображение конфигурации и состояния VLAN или туннеля Dot1Q

vlan | **subnet** | **protocol-vlan** | **dot1q-translating-tunnel**]	
show interface vlan *x*	Отображение состояния выбранного интерфейса VLAN

20.7 Включение туннеля Dot1Q

После включения туннелирования Dot1Q на коммутаторе, порты со значением по умолчанию могут быть назначены как downlink-порты для туннеля Dot1Q, и к входящим пакетам будет добавлен тег SPVLAN для обеспечения изоляции трафика и идентификации на уровне провайдера услуг.

Команда включения Dot1Q -туннеля показана в следующей таблице:

Команда	Описание
dot1q-tunnel	Включение туннелирования Dot1Q на коммутаторе

20.8 Примеры настройки туннеля Dot1Q

Следующие типичные решения показывают, как применить туннель Dot1Q.

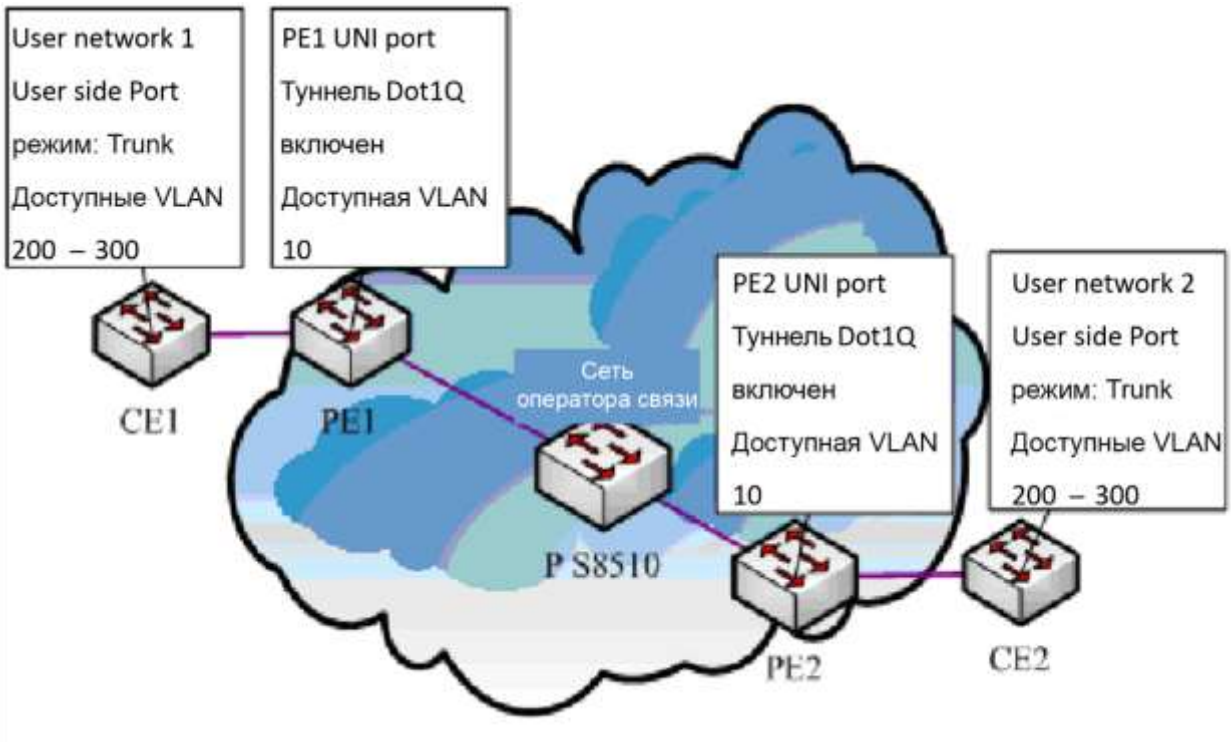

Рисунок 20-1 – Настройка туннеля Dot1Q

Как показано на рисунке выше, порт F0/1 CE1 соединяет порт F0/1 (или порт G0/1) PE1; PE1 подключается к S8510 на порту F0/2 (или порту G0/2); PE2 подключается к S8510 на порту F0/2 (или порту G0/2); а порт F0/1 (или порт G0/1) PE2 соединяет порт F0/1 CE1.

Порты PE настроены как порты доступа VLAN 10, и на них включен туннель Dot1Q. Однако портам CE по-прежнему требуется Trunk VLAN 200 – 300, что позволяет каналу между CE и PE быть асимметричным. В этом случае общедоступной сети достаточно предоставить пользователям только идентификатор VLAN, равный 10. Независимо от того, сколько идентификаторов VLAN частной сети запланировано в сети пользователя, вновь распространяемый идентификатор VLAN общедоступной сети будет в обязательном порядке внесен в тегированные пакеты, когда они попадают в магистральную сеть интернет-провайдера. Затем эти пакеты с идентификатором общедоступной сети проходят через магистральную сеть, достигают другой ее стороны, то есть устройств PE, избавляются от тега VLAN общедоступной сети, возобновляют передачу пользовательских пакетов и в конечном итоге передаются на CE-устройства пользователей. Таким образом, пакеты, пересылаемые в магистральной сети, имеют два уровня заголовков тегов 802.1Q, один из которых является тегом общедоступной сети, а другой – тегом частной сети. Подробный процесс пересылки пакетов показан ниже:

1. Поскольку выходной порт CE1 является магистральным портом, все пакеты, передаваемые пользователями в PE1, содержат тег VLAN частной сети (в диапазоне от 200 до 300). Один из таких пакетов показан в таблице 20-3.

Таблица 20-3 – Структура пакета CE1

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

2. Когда пакеты поступают на устройство PE1, оно, игнорирует тег VLAN частной сети, поскольку входной порт является портом доступа туннеля Dot1Q, но добавляет в эти пакеты тег дефолтной VLAN 10, как показано в таблице 20-4.

Таблица 20-4 – Структура пакета PE1

DA (6B)	SA (6B)	ETYPE(8100) (2B)	SPVLAN Tag (2B)	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

3. В магистральной сети пакеты передаются по порту VLAN 10. Тег частной сети сохраняется в прозрачном состоянии до тех пор, пока эти пакеты не достигнут PE2.

4. PE2 обнаруживает, что порт, через который он соединен с CE2, является портом доступа VLAN 10, удаляет заголовок тега VLAN 10 согласно 802.1Q, восстанавливает изначальные пакеты пользователей и передает их на CE2, как показано в таблице 20-5.

Таблица 20-5 – Структура пакета PE2

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Если смотреть на поток пересылки, Dot1Q Tunnel очень лаконичен. Особенность данной технологии заключается в отсутствии необходимости сигнализации для поддержания установления туннеля, что обеспечивает простоту использования и статическую конфигурацию.

Что касается типичной конфигурации Dot1Q Tunnel, коммутаторы настраиваются следующим образом, когда они работают как PE (PE1 имеет ту же конфигурацию, что и PE2):

Switch_config#dot1q-tunnel

Switch_config_g0/1#switchport pvid 10

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#switchport trunk vlan-untagged 1-9,11-4094

21. Частная VLAN

21.1 Обзор

Если провайдер предоставляет каждому пользователю отдельную VLAN, поддержка одним устройством 4094 VLAN ограничивает общее количество пользователей, обслуживаемых интернет-провайдером. Частная VLAN (PVLAN) успешно решает эту проблему.

21.2 Тип PVLAN и тип порта в PVLAN

Частная VLAN разделяет широковещательный домен L2 VLAN на несколько субдоменов, каждый из которых состоит из пары частных VLAN: первичной (основной) и вторичной. Один частный домен VLAN может иметь несколько пар частных VLAN, и каждая пара частных VLAN представляет собой субдомен. В домене частной VLAN имеется только одна основная VLAN, и все пары частных VLAN используют одну и ту же основную VLAN. Идентификаторы вторичных VLAN в каждом субдомене отличаются друг от друга.

21.2.1 PVLAN с одной основной VLAN

- В этом случае используется одна основная VLAN для группировки портов. Она относится к порту прослушивания (promiscuous) и соединяется с одной или несколькими вторичными VLAN, которые изолируют трафик между портами и контролируют передачу данных. Каждый порт в основной VLAN является ее членом

21.2.2 PVLAN с двумя вторичными VLAN

- Изолированная VLAN: связь второго уровня не может осуществляться между двумя портами в одной изолированной VLAN. Кроме того, в частной VLAN имеется только одна изолированная VLAN. Изолированная VLAN должна быть связана с основной через ее promiscuous-порт.

- VLAN сообщества: связь второго уровня может осуществляться между двумя портами в одной VLAN, но они не имеют связи с портами в другой VLAN сообщества. Одна частная VLAN может содержать несколько VLAN сообщества. VLAN сообщества должна быть связана с основной через ее promiscuous-порт.

21.2.3 Типы портов в рамках PVLAN

- Порт прослушивания (promiscuous port): принадлежит основной VLAN. Обычно связывается с портом маршрутизатора или межсетевого экрана. Он может взаимодействовать со всеми другими портами, включая изолированный порт и порт сообщества вторичной VLAN в той же PVLAN.
- Изолированный порт (isolated port): это хост-порт в изолированной VLAN. В той же PVLAN изолированный порт полностью изолирован на уровне L2 от других портов, за исключением promiscuous-порта, поэтому только на него могут быть перенаправлены потоки, полученные от изолированного порта.
- Порт сообщества (community port): эта настройка позволяет создавать подгруппы портов в рамках общей PVLAN. Устройства, подключенные к портам сообщества, могут общаться друг с другом в пределах своего определенного сообщества и с promiscuous-портами. Однако порты сообществ не могут взаимодействовать с портами из других сообществ или изолированными портами в PVLAN.

21.2.4 Изменение полей в VLAN TAG

Эта функция позволяет изменять идентификатор VLAN и приоритет в теге VLAN. Кроме того, она определяет, будут ли исходящие пакеты частной VLAN содержать тег VLAN или нет.

21.3 Настройка PVLAN

Задачи настройки

- Определение частной VLAN
- Настройка ассоциации доменов частных VLAN
- Настройка порта L2 частной VLAN в качестве хост-порта
- Настройка порта L2 частной VLAN в качестве promiscuous-порта
- Изменение связанных полей исходящих пакетов в частной VLAN.
- Отображение информации о конфигурации частной VLAN

21.3.1 Определение частной VLAN

Используйте следующие команды, чтобы определить VLAN как частную и задать её базовые функции:

Команда	Описание
vlan *vlan-id*	Вход в режим VLAN
private-vlan {**primary** | **community** | **isolated**}	Настраивает функции частной VLAN
no private-vlan {**primary** | **community** | **isolated**}	Удаляет функции частной VLAN
show vlan private-vlan	Отображает конфигурацию частной VLAN
exit	Выход из режима настройки VLAN

21.3.2 Настройка ассоциации доменов частных VLAN

Выполните следующие команды, чтобы связать первичную и вторичную VLAN.

Команда	Описание
vlan *vlan-id*	Вход в режим настройки первичной VLAN
private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}	Устанавливает связанную вторичную VLAN
no private-vlan association	Очищает все ассоциации между текущей основной и всеми вторичными VLAN
exit	Выход из режима настройки VLAN

21.3.3 Настройка порта L2 частной VLAN в качестве хост-порта

Выполните следующие команды, чтобы настроить порт L2 частной VLAN в качестве порта хоста:

Команда	Описание
interface *interface*	Вход в режим настройки интерфейса
switchport mode private-vlan host	Устанавливает порт L2 в режим порта хоста
no switchport mode	Удаляет настройку режима PVLAN для порта L2
switchport private-vlan host-association *p_vid s_vid*	Связывает порт L2 хоста с частной VLAN
no switchport private-vlan host-association	Удаляет связь между портом L2 хоста и частной VLAN
exit	Выход из режима настройки интерфейса

21.3.4 Настройка порта L2 частной VLAN в качестве promiscuous-порта

Выполните следующие команды, чтобы установить для порта L2 PVLAN режим прослушивания и настроить его в качестве promiscuous-порта:

Команда	Описание
Interface *interface*	Вход в режим настройки интерфейса
switchport mode private-vlan promiscuous	Переводит порт L2 в promiscuous-режим
no switchport mode	Удаляет конфигурацию режима частной VLAN порта L2
switchport private-vlan mapping *p_vid* {*svlist* | *add svlist* | **remove** *svlist*}	Связывает promiscuous-порт L2 с частной VLAN
no switchport private-vlan mapping	Удаляет связь между promiscuous-портом L2 и частной VLAN
exit	Выход из режима настройки интерфейса

21.3.5 Изменение связанных полей выходных пакетов в частной VLAN

Выполните следующие команды, чтобы изменить связанные поля исходящих пакетов в частной VLAN:

Команда	Описание
interface *interface*	Вход в режим настройки интерфейса
switchport private-vlan tag-pvid *vlan-id*	Настраивает поле VLAN ID в теге исходящего пакета
switchport private-vlan tag-pri *pri*	Настраивает поле приоритета в теге исходящего пакета
[**no**] **switchport private-vlan untagged**	Настраивает, имеют ли выходные пакеты тег или нет
exit	Выход из режима настройки интерфейса

21.3.6 Отображение информации о конфигурации частной VLAN

Выполните следующие команды в режиме глобальной конфигурации, настройки интерфейса или VLAN, чтобы отобразить информацию о настройках для PVLAN и порта L2 PVLAN:

Команда	Описание
show vlan private-vlan	Отображает конфигурацию частной VLAN
show vlan private-vlan interface *interface*	Отображает конфигурацию порта L2 в частной VLAN

21.4 Пример настройки

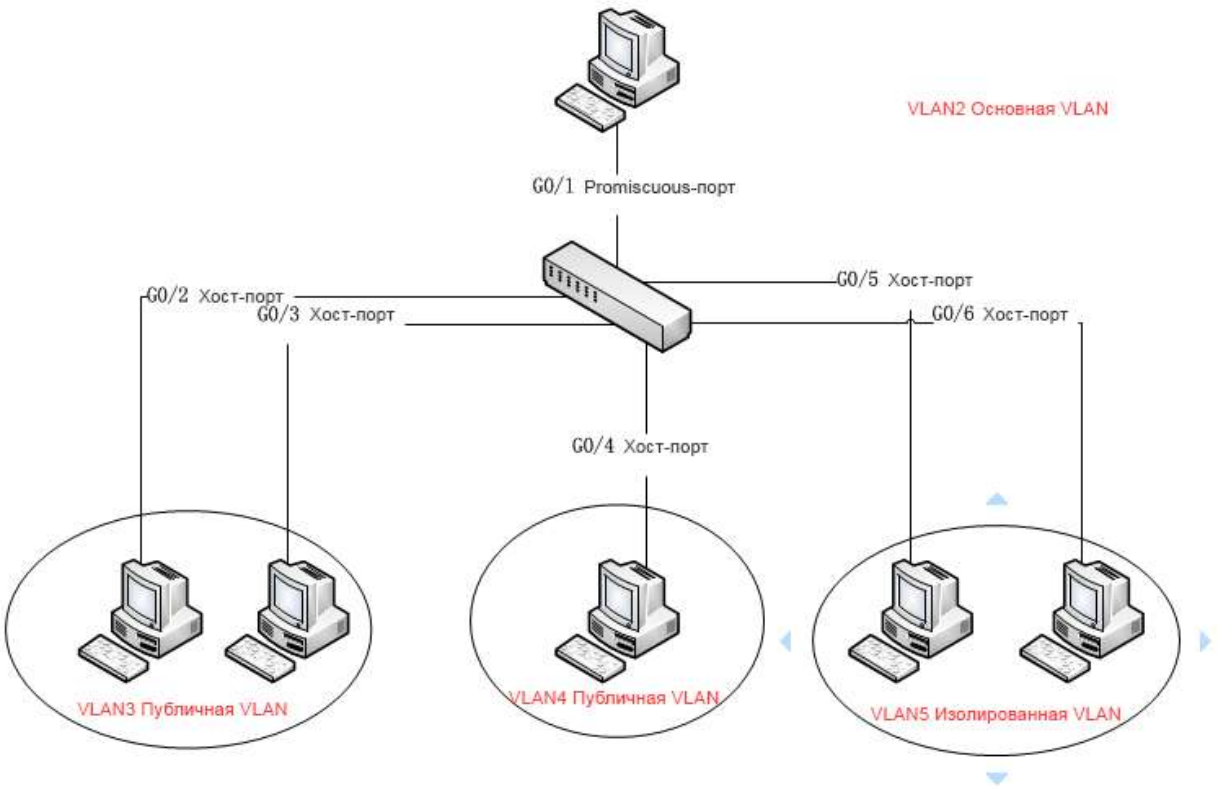

Рисунок 21-1 – Типовая настройка PVLAN

Как показано на рисунке 21-1, порт G0/1 – это promiscuous-порт в основной VLAN 2, а порты G0/2 – G0/6 – это хост-порты, среди которых порты G0/2 и G0/3 – это хост-порты (общедоступные порты) сообщества VLAN 3, порт G0/4 – это порт сообщества VLAN 4, а порты G0/5 и G0/6 – хост-порты изолированной VLAN 5.

Согласно определению частной VLAN, связь L2 может осуществляться между promiscuous-портом G0/1 и хост-портами всех субдоменов VLAN, то есть между хост-портами G0/2 и G0/3 сообщества VLAN 3, но они не могут осуществлять связь L2 с другими хост-портами

вторичных VLAN. Связь L2 не может осуществляться между портами G0/5 и G0/6 в изолированной VLAN 5, но эти два порта могут осуществлять связь L2 с promiscuous-портом G0/1.

Ниже показаны команды, которые необходимо запустить на коммутаторе, для проведения настройки:

```
Switch_config#interface GigaEthernet0/1
Switch_config_g0/1#switchport mode private-vlan promiscuous
Switch_config_g0/1#switchport private-vlan mapping 2 3-5
Switch_config_g0/1#switchport pvid 2

Switch_config#interface GigaEthernet0/2
Switch_config_g0/2#switchport mode private-vlan host
Switch_config_g0/2#switchport private-vlan host-association 2 3
Switch_config_g0/2#switchport pvid 3

Switch_config#interface GigaEthernet0/3
Switch_config_g0/3#switchport mode private-vlan host
Switch_config_g0/3#switchport private-vlan host-association 2 3
Switch_config_g0/3#switchport pvid 3

Switch_config#interface GigaEthernet0/4
Switch_config_g0/4#switchport mode private-vlan host
Switch_config_g0/4#switchport private-vlan host-association 2 4
Switch_config_g0/4# switchport pvid 4

Switch_config#interface GigaEthernet0/5
Switch_config_g0/5#switchport mode private-vlan host
Switch_config_g0/5#switchport private-vlan host-association 2 5
Switch_config_g0/5#switchport pvid 5

Switch_config#interface GigaEthernet0/6
```

Switch_config_g0/5#switchport mode private-vlan host

Switch_config_g0/5#switchport private-vlan host-association 2 5

Switch_config_g0/5#switchport pvid 5

Switch_config#vlan 2

Switch_config_vlan2#private-vlan primary

Switch_config_vlan2#private-vlan association 3-5

Switch_config#vlan 3

Switch_config_vlan3#private-vlan community

Switch_config#vlan 4

Switch_config_vlan4#private-vlan community

Switch_config#vlan 5

Switch_config_vlan5#private-vlan isolated

Switch_config#show vlan private-vlan

Primary	Secondary	Type	Ports
2	3	community	g0/1, g0/2, g0/3
2	4	community	g0/1, g0/4
2	5	isolated	g0/1, g0/5, g0/6

22. STP

22.1 Введение

Стандарт «протокол связующего дерева» (STP) определен в IEEE 802.1D. Это упрощает топологию локальной сети, состоящую из нескольких мостов в единое связующее дерево, предотвращая возникновение сетевых петель и обеспечивая стабильную работу сети.

Алгоритм STP создает активную топологию сети с простыми соединениями, выбирая одно дерево, которое охватывает все узлы сети. В активной топологии некоторые порты, которые участвуют в процессе выбора корневого моста и определения пути к корню дерева (bridging ports), могут пропускать кадры, в то время как другие находятся в состоянии блокировки и не могут передавать информацию. В зависимости от состояния сети порты могут быть включены или исключены из активной топологии.

Когда сетевое устройство становится неэффективным или добавляется в сеть, или удаляется из нее, порты могут изменять своё состояние, например, переходить в состояние передачи (transmitting state).

В топологии STP мост может рассматриваться как корневой (root). Для каждого сегмента локальной сети есть порт моста, который передает данные от своего сегмента к корневому мосту. Такой порт считается назначенным портом (designated port) сетевого раздела. Мост, на котором располагается этот порт, считается назначенным мостом (designated bridge) локальной сети. Корневой мост является назначенным мостом для всех сетевых сегментов, к которым он подключен.

Среди портов каждого моста порт, который ближе всего к корневому мосту, является корневым портом (root port) моста. Только корневой порт и назначенный порт (если он есть) находятся в состоянии передачи данных. Порты другого типа не отключены, но они не являются ни корневыми, ни назначенными. Такие порты называются резервными (standby ports).

Следующие параметры определяют структуру стабилизированной активной топологии:

- идентификатор каждого моста;
- стоимость пути для каждого порта;
- идентификатор порта для каждого порта моста.

В качестве корневого выбирается мост с наивысшим приоритетом (значение идентификатора наименьшее). Порты каждого моста имеют атрибут Root Path Cost, то есть минимальное значение стоимости пути всех портов от корня до моста. Назначенный порт – это порт, через который происходит пересылка трафика для определенного сегмента сети. Он выбирается на основе наименьшей стоимости пути от коммутатора до корня топологии сети (или корневого коммутатора).

Когда два порта коммутатора являются частью петли, настройки приоритета порта связующего дерева и стоимости пути определяют, какой порт будет переведен в состояние пересылки, а какой – в состояние блокировки. Значение приоритета порта связующего дерева представляет расположение порта в топологии сети и то, насколько удачно он

расположен для передачи трафика. Значение стоимости пути представляет скорость передачи информации.

Данная серия коммутаторов поддерживает два режима протокола связующего дерева: 802.1D STP и 802.1w RSTP. Некоторые модели поддерживают режим распределения STP по VLAN и протоколу связующего дерева MSTP. Для получения более подробной информации обратитесь к разделу «Настройка RSTP».

В этой главе описывается настройка стандартного протокола связующего дерева, поддерживаемого коммутатором.

802.1D STP и 802.1w RSTP в этой статье обозначаются сокращенно SSTP и RSTP. SSTP означает «единое связующее дерево».

22.2 Настройка STP

Задачи настройки

- Выбор режима STP
- Отключение/включение STP
- Запрет/разрешение STP для порта
- Настройка приоритета коммутатора
- Настройка времени приветствия
- Настройка максимального возраста
- Настройка времени задержки пересылки
- Настройка приоритета порта
- Настройка стоимости пути
- Мониторинг состояния STP
- Настройка передачи trap-сообщений

22.2.1 Выбор режима STP

Выполните следующую команду, чтобы настроить режим STP:

Команда	Описание
spanning-tree mode {sstp | pvst | rstp | mstp}	Выбор конфигурации STP

22.2.2 Отключение/включение STP

По умолчанию связующее дерево включено. Отключайте связующее дерево только в том случае, если вы уверены, что в топологии сети нет петель.

Выполните следующие действия, чтобы отключить связующее дерево:

Команда	Описание
no spanning-tree	Отключает STP

Чтобы включить связующее дерево, используйте следующую команду:

Команда	Описание
spanning-tree	Включает режим STP по умолчанию (SSTP)
spanning-tree mode {**sstp** | **pvst** | **rstp** | **mstp**}	Включает определенный режим STP

22.2.3 Запрет/разрешение STP для порта

По умолчанию протокол STP работает на всех портах коммутации (физических портах и портах агрегации). Работа STP запрещается в режиме настройки порта следующей командой:

Команда	Описание
no spanning-tree	Запрещает порту работать с протоколом STP

После запрета работы STP на порту, порт останется в заданном режиме, но не будет отправлять BPDU. Тем не менее, во всех режимах STP по-прежнему будет выполняться проверка типов и подсчет BPDU, полученных портом. Информация о границах и топологии также будет обновляться.

Когда используется команда **no spanning-tree**, порты со статусами «корневой», «альтернативный», «мастер» или «резервный» в режимах RSTP/MSTP обрабатывают информацию о протоколе и, когда она становится устаревшей, превращаются в «назначенные». В режимах SSTP/PVST порт сохраняет свою прежнюю роль в течение некоторого времени, и информация становится устаревшей после истечения времени таймера. Каждый режим STP поддерживает функцию BpduGuard на порту, настроенном «без связующего дерева».

22.2.4 Настройка приоритета коммутатора

Вы можете настроить приоритет коммутатора и повысить вероятность того, что автономный коммутатор или коммутатор в стеке будет выбран в качестве корневого коммутатора.

Выполните следующие действия, чтобы настроить приоритет коммутатора:

Команда	Описание
spanning-tree sstp priority *value*	Изменяет значение приоритета SSTP
no spanning-tree sstp priority	Возвращает приоритет SSTP к значению по умолчанию (32768)

22.2.5 Настройка времени приветствия

Пользователь может настроить интервал между блоками данных STP, отправляемыми корневым коммутатором, изменив время приветствия.

Используйте следующую команду для настройки времени приветствия SSTP:

Команда	Описание
spanning-tree sstp hello-time *value*	Настраивает время приветствия SSTP
no spanning-tree sstp hello-time	Возвращает время приветствия SSTP к значению по умолчанию (2 с)

22.2.6 Настройка максимального возраста

Используйте параметр max-age (максимальный возраст) SSTP, чтобы настроить значение интервала времени (в секундах), которое коммутатор ждет перед тем, как попытаться изменить конфигурацию связующего дерева при отсутствии приходящих конфигурационных сообщений. Если в течение указанного времени коммутатор не получает новых сообщений от других устройств, он считает текущую топологию устаревшей и начинает процесс реконфигурации.

Выполните следующие действия, чтобы настроить время max-age:

Команда	Описание
spanning-tree sstp max-age *value*	Настраивает значение max-age SSTP
no spanning-tree sstp max-age	Возвращает max-age к значению по умолчанию (20 с)

22.2.7 Настройка времени задержки пересылки

Настройте задержку пересылки SSTP, чтобы определить количество секунд, в течение которых интерфейс ожидает перехода из состояний обучения и прослушивания связующего дерева в состояние пересылки.

Используйте следующую команду для настройки задержки пересылки SSTP:

Команда	Описание
spanning-tree sstp forward-time *value*	Настраивает время пересылки SSTP
no spanning-tree sstp forward-time	Возвращает время пересылки к значению по умолчанию (15 с)

22.2.8 Настройка приоритета порта

Если возникает петля, связующее дерево использует приоритет порта при выборе интерфейса для перевода в состояние пересылки. Вы можете назначить более высокие значения приоритета (более низкие числовые значения) интерфейсам, которые вы хотите выбрать первыми, и значения более низкого приоритета (более высокие числовые значения), для интерфейсов, которые будут выбираться в последнюю очередь. Если все интерфейсы имеют одинаковое значение приоритета, связующее дерево переводит интерфейс с наименьшим номером в состояние пересылки и блокирует остальные.

Выполните следующие действия, чтобы настроить приоритет интерфейса:

Команда	Описание
spanning-tree port-priority *value*	Настраивает значение приоритета порта для интерфейса
spanning-tree sstp port-priority *value*	Изменяет приоритет порта SSTP
no spanning-tree sstp port-priority	Возвращает приоритет порта к значению по умолчанию (128)

22.2.9 Настройка стоимости пути

Выполните следующие действия, чтобы настроить стоимость пути для интерфейса:

Команда	Описание
spanning-tree cost *value*	Настраивает стоимость пути для интерфейса
spanning-tree sstp cost *value*	Изменяет стоимость пути SSTP
no spanning-tree sstp cost	Возвращает стоимость пути к значению по умолчанию

22.2.10 Мониторинг состояния STP

Чтобы отслеживать конфигурацию и состояние STP, используйте следующие команды в режиме управления:

Команда	Описание

show spanning-tree	Отображает информацию связующего дерева только на активных интерфейсах
show spanning-tree detail	Отображает подробную сводку информации о связующем дереве на всех интерфейсах
show spanning-tree interface	Отображает информацию о связующем дереве для указанного интерфейса

22.2.11 Настройка передачи trap-сообщений

Вы можете отслеживать изменение STP в коммутаторе удаленно при помощи программного обеспечения управления сетью, настроив функцию передачи trap-сообщений.

Протоколы STP поддерживают два типа таких сообщений: newRoot (новый корень) и topologyChange (изменение топологии). Когда коммутатор становится корневым, он отправляет сообщение newRoot Trap; когда коммутатор обнаруживает изменение топологии, например, переход неграничного порта из состояния блокировки в состояние пересылки, коммутатор отправляет сообщение topologyChange Trap.

Для получения trap-сообщений необходимо использовать программное обеспечение управления сетью. Оно должно поддерживать протокол Trap и импортировать соответствующий набор данных (Bridge-MIB). Идентификатор объекта (OID) 1.3.6.1.2.1.17 используется для указания на события, связанные с протоколом Spanning Tree в стандартной MIB-структуре.

Используйте следующие команды для запуска STP Trap в режиме глобальной конфигурации:

Команда	Описание
spanning-tree management trap [**newroot** | **topologychange**]	Инициирование STP Trap. Если тип сообщений не определен, одновременно будут инициированы оба типа
no spanning-tree management trap	Завершить работу STP Trap

22.2.12 Настройка VLAN STP

В режиме SSTP для всей сети существует только один экземпляр связующего дерева, а состояние порта коммутатора в связующем дереве определяет его состояние в VLAN. В случае нескольких виртуальных локальных сетей в сети изоляция между одним протоколом связующего дерева и топологией виртуальной локальной сети может привести к блокировке нормальной связи в сегменте сети. Коммутатор поддерживает запуск

независимого SSTP в определенном количестве VLAN, гарантируя, что порты в них могут иметь разные состояния. В то же время может быть реализован баланс трафика между VLAN. Важно отметить, что количество VLAN, которые могут независимо запускать протокол связующего дерева, зависит от фактической версии, а другие топологии VLAN, превышающие ограничение по количеству, не будут контролироваться STP.

Чтобы настроить свойства SSTP в VLAN, выполните эти команды в режиме глобальной конфигурации:

Команда	Описание
spanning-tree mode pvst	Запуск режима выделения STP для VLAN
spanning-tree vlan *vlan-list*	Назначение экземпляра STP указанной VLAN
no spanning-tree vlan *vlan-list*	Удаление экземпляра связующего дерева из указанной VLAN
spanning-tree vlan *vlan-list* **priority** *value*	Настройка уровня приоритета связующего дерева в указанной VLAN
no spanning-tree *vlan-list* **priority**	Сброс приоритета связующего дерева в VLAN на значение по умолчанию
spanning-tree vlan *vlan-list* **forward-time** *value*	Настройка задержки пересылки для указанной VLAN
no spanning-tree vlan *vlan-list* **forward-time**	Сброс задержки пересылки для указанной VLAN на значение по умолчанию
spanning-tree vlan *vlan-list* **max-age** *value*	Настройка максимального возраста для указанной VLAN
no spanning-tree vlan *vlan-list* **max-age**	Сброс максимального возраста для указанной VLAN на значение по умолчанию
spanning-tree vlan *vlan-list* **hello-time** *value*	Настройка времени приветствия для указанной VLAN
no spanning-tree vlan *vlan-list* **hello-time**	Сброс времени приветствия указанной VLAN на значение по умолчанию

Чтобы настроить свойства порта, выполните следующие команды в режиме настройки интерфейса:

Команда	Описание
spanning-tree vlan *vlan-list* **cost**	Настройка стоимости пути порта в указанной VLAN
no spanning-tree vlan *vlan-list* **cost**	Сброс стоимости пути порта в указанной VLAN на значение по умолчанию
spanning-tree vlan *vlan-list* **port-priority**	Настройка приоритета порта в указанной VLAN

no spanning-tree vlan *vlan-list* **port-priority**	Сброс приоритета порта в указанной VLAN на значение по умолчанию

Запустите эти команды, чтобы проверить состояние связующего дерева в указанной VLAN в режиме управления:

Команда	Описание
show spanning-tree vlan *vlan-list*	Проверка состояния связующего дерева в VLAN
show spanning-tree pvst instance-list	Проверка связи между экземпляром PVST и VLAN

23. RSTP

RSTP (Rapid Spanning Tree Protocol) – это протокол быстрого связующего дерева, который применяется в компьютерных сетях для обеспечения высокой доступности и избегания петель в топологии. RSTP является улучшенной версией протокола STP и предназначен для более быстрого обнаружения изменений в сети и перестройки топологии после сбоев или изменений в структуре сети. Он был введен для устранения недостатков оригинального STP, обеспечивая более быстрое восстановление работы сети при изменениях в топологии. RSTP также известен как IEEE 802.1w.

23.1 Настройка RSTP

Задачи настройки

- Включение/отключение RSTP на коммутаторе
- Настройка приоритета коммутатора
- Настройка времени задержки пересылки
- Настройка времени приветствия
- Настройка максимального возраста
- Настройка стоимости пути
- Настройка приоритета порта
- Настройка граничного порта
- Настройка типа подключения порта
- Перезапуск проверки конвертации протоколов

23.1.1 Включение/отключение RSTP на коммутаторе

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
spanning-tree mode rstp	Включает RSTP

no spanning-tree mode	Возвращает STP в режим по умолчанию (SSTP)

23.1.2 Настройка приоритета коммутатора

Вы можете настроить приоритет коммутатора и повысить вероятность того, что автономный коммутатор или коммутатор в стеке будет выбран в качестве корневого.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
spanning-tree rstp priority *value*	Изменяет значение приоритета RSTP
no spanning-tree rstp priority	Возвращает приоритету RSTP значение по умолчанию

Если приоритет всех мостов во всей сети коммутаторов имеет одно и то же значение, то в качестве корневого моста будет выбран мост с наименьшим MAC-адресом. В ситуации, когда протокол RSTP включен, изменение значения приоритета моста приведет к перерасчету связующего дерева.

По умолчанию значение приоритета моста равно 32768.

23.1.3 Настройка времени задержки пересылки

Сбои канала могут привести к тому, что сеть пересчитает структуру связующего дерева. Но сообщение об обновлении конфигурации не может быть передано по всей сети единовременно. И, если вновь выбранный корневой порт и назначенный порт немедленно начнут пересылку данных, это может привести к появлению временного замкнутого пути, (петли). Поэтому протокол использует своего рода «механизм перехода состояний». Прежде чем корневой порт и назначенный порт начинают пересылать данные, они проходят через промежуточное состояние. После прохождения времени задержки (Forward Delay Time), они переходят в состояние пересылки данных. Это время задержки гарантирует, что вновь настроенное сообщение будет передано по всей сети. Характеристика задержки пересылки моста связана с диаметром сети коммутатора. Как правило, чем больше диаметр сети и количество переходов, тем дольше должно быть время задержки.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
spanning-tree rstp forward-time *value*	Настраивает задержку пересылки
no spanning-tree rstp forward-time	Возвращает время задержки пересылки к значению по умолчанию (15 с)

Если настроить время задержки пересылки на относительно небольшое значение, это может привести к временному перенасыщению путей. При слишком большом значении система может не возобновить подключение в течение неоправданно длительного времени. Рекомендуется использовать значение по умолчанию.

Время задержки по умолчанию составляет 15 секунд.

23.1.4 Настройка времени приветствия

Правильное значение времени приветствия может гарантировать, что мост обнаружит сбои каналов в сети, не занимая слишком много сетевых ресурсов.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
spanning-tree rstp hello-time *value*	Настраивает время приветствия
no spanning-tree rstp hello-time	Возвращает время приветствия к значению по умолчанию

Следует отметить, что слишком большое значение времени приветствия может привести к тому, что сетевой мост не сможет получить сообщение «Hello» из-за потери пакетов канала. Таким образом, сетевой мост решит, что соединение нарушено, и пересчитает связующее дерево. Если значение времени приветствия слишком короткое, это может привести к тому, что сетевой мост будет часто отправлять сообщения о конфигурации, нерационально занимая при этом полосу пропускания. Это увеличивает нагрузку на сеть и процессор. Предполагается, что пользователь использует значение по умолчанию.

Рекомендуется использовать значение по умолчанию, которое составляет 2 секунды.

23.1.5 Настройка максимального возраста

Максимальный возраст (max-age) определяет время жизни каждого BPDU (пакета данных протокола моста) до того, как он должен быть отброшен. Если корневой мост не получает BPDU из определенного порта в течение этого времени, он считает, что связь через данный порт неактивна и начинает искать другой путь через связующее дерево.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
spanning-tree rstp max-age *value*	Настраивает значение max-age

no spanning-tree rstp max-age	Возвращает max-age к значению по умолчанию (20 с)

Рекомендуется использовать значение по умолчанию.

Очень низкое значение может привести к частым перерасчетам и ненужным блокировкам, в то время как слишком высокое значение может привести к тому, что изменения состояния узлов останутся без внимания, что также может быть проблемой для стабильности сети.

По умолчанию значение max-age для моста составляет 20 секунд.

23.1.6 Настройка стоимости пути

Значение по умолчанию стоимости пути (path cost) связующего дерева выводится из скорости передачи интерфейса. Если возникает петля, связующее дерево использует значение стоимости при выборе интерфейса для перевода в состояние пересылки. Вы можете назначить более низкие значения стоимости для интерфейсов, которые желательно выбрать в первую очередь, и более высокие – для интерфейсов, которые вы хотите выбрать последними. Если все интерфейсы имеют одинаковое значение стоимости, связующее дерево переводит в состояние пересылки интерфейс с наименьшим номером, а остальные блокирует.

Для настройки стоимости пути выполните следующие действия в режиме настройки интерфейса:

Команда	Описание
spanning-tree rstp cost *value*	Настраивает стоимость пути для интерфейса
no spanning-tree rstp cost	Возвращает стоимость пути к значению по умолчанию

Изменение стоимости пути для порта Ethernet приведет к перерасчету связующего дерева. Рекомендуется использовать значение по умолчанию и позволить протоколу RSTP рассчитать стоимость пути для текущего интерфейса.

Когда скорость порта составляет 10 Мбит/с, стоимость пути интерфейса Ethernet составляет 2000000. Когда скорость порта составляет 100 Мбит/с, стоимость пути интерфейса Ethernet составляет 200000.

23.1.7 Настройка приоритета порта

Если возникает петля, связующее дерево использует приоритет порта при выборе интерфейса для перевода в состояние пересылки. Вы можете назначить более высокие значения приоритета (более низкие числовые значения) интерфейсам, которые вы хотите выбрать первыми, и значения более низкого приоритета (более высокие числовые значения) для интерфейсов, которые будут выбираться в последнюю очередь. Если все интерфейсы имеют одинаковое значение приоритета, связующее дерево переводит интерфейс с наименьшим номером в состояние пересылки и блокирует остальные.

Выполните следующие действия в режиме настройки интерфейса:

Команда	Описание
spanning-tree rstp port-priority *value*	Настраивает приоритет порта для интерфейса
no spanning-tree rstp port-priority	Возвращает приоритет порта к значению по умолчанию

Изменение приоритета интерфейса Ethernet приведет к перерасчету связующего дерева.

Приоритет интерфейса Ethernet по умолчанию – 128.

23.1.8 Настройка граничного порта

Граничный или конечный порт (edge port) означает, что этот порт подключается к терминальному устройству в сети. Обязательный граничный порт будет находиться в состоянии пересылки сразу после подключения, минуя состояние прослушивания и обучения. Для настройки граничного порта RSTP используйте следующую команду в режиме настройки интерфейса:

Команда	Описание
spanning-tree rstp edge	Настройка порта в качестве граничного

При автоматическом определении режима протокола, если порт в течение определенного времени не получает BPDU, он считается граничным (конечным) портом.

23.1.9 Настройка типа подключения порта

Если коммутаторы, работающие по протоколу RSTP, соединяются друг с другом по принципу «точка-точка», они могут быстро установить топологию с помощью механизма квитирования.

Если порт работает в дуплексном режиме, протокол будет считать подключение порта реализованным как точка-точка (point-to-point). Если порт работает в полудуплексном режиме, протокол будет считать подключение порта реализованным как общее (shared).

Если подтвердится, что коммутатор, подключенный к порту, работает по протоколу RSTP или MSTP, тип подключения порта можно настроить как «точка-точка», чтобы гарантировать возможность быстрого подтверждения связи.

Для указания типа подключения порта используйте следующую команду в режиме настройки интерфейса:

Команда	Описание
spanning-tree rstp point-to-point [**force-true** | **force-false** | **auto**]	Настройка порта «точка-точка» **force-true**: принудительное использование типа «точка-точка»; **force-false**: принудительное отключение типа «точка-точка»; **auto**: протокол автоматически определяет тип порта

23.1.10 Перезапуск проверки конвертации протоколов

Протокол RSTP позволяет коммутатору работать совместно с традиционным коммутатором 802.1D STP с помощью механизма преобразования протокола. Если один порт коммутатора получает информацию о конфигурации STP, этот порт перестроится на отправку только сообщений STP.

Если порт перестает получать STP BPDU после нахождения в состоянии совместимости со стандартом 802.1D STP, он автоматически возвращается к RSTP. В то же время через команду **spanning-tree rstp migration-check** можно запустить проверку преобразования протокола портом и восстановление порта в RSTP-режим.

Команду можно запустить в режиме глобальной конфигурации для проверки конвертации протоколов на всех портах, или в режиме настройки интерфейса для проверки отдельного указанного порта.

Команда	Описание
spanning-tree rstp migration-check	Перезапуск проверки процесса преобразования протокола всех портов или текущего порта

24. MTSP

24.1 Обзор

24.1.1 Введение

Протокол множественного связующего дерева (MSTP) используется для предотвращения петель во взаимосвязанных сегментах сетей, построенных на основе Ethernet. Он позволяет сетевым администраторам настроить более одного дерева связанных устройств на сетевой сегмент, что снижает время восстановления сети в случае отказа коммутатора. MSTP совместим с более ранним протоколом связующего дерева (STP) и протоколом быстрого связующего дерева (RSTP).

И STP, и RSTP могут создавать единую топологию STP. Все сообщения VLAN пересылаются через единственное связующее дерево. STP работает медленнее, в то время как RSTP обеспечивает более быструю и надежную топологию, благодаря механизму квитирования для управления взаимодействием между сетевыми устройствами.

MSTP наследует механизм быстрого установления связи, использованный в RSTP. В то же время MST позволяет распределять разные VLAN по разным связующим деревьям, создавая в сети несколько топологий. В сетях, созданных по протоколу MSTP, кадры разных VLAN могут пересылаться по разным путям, реализуя баланс нагрузки данных VLAN.

MSTP позволяет использовать несколько VLAN внутри одной топологии STP и эффективно сократить количество STP, необходимых для поддержки множества VLAN, что улучшает производительность и уменьшает нагрузку на сеть. Таким образом, MSTP предлагает более эффективный способ управления VLAN, чем STP.

24.1.2 Домен MST

В MSTP связь между VLAN и STP описывается с помощью таблицы конфигурации MSTP. Таблица, имя и номер редактирования конфигурации составляют идентификатор конфигурации MST.

В сети взаимосвязанные мосты с одинаковым идентификатором конфигурации MST рассматриваются в одном и том же регионе MST. Мосты в одном и том же регионе всегда имеют одинаковую конфигурацию VLAN, что гарантирует успешную отправку кадров VLAN в регионе MST.

24.1.3 IST, CST, CIST и MSTI

На рисунке 24-1 показана сеть MSTP, включающая три региона MST и коммутатор, работающий по протоколу 802.1D STP.

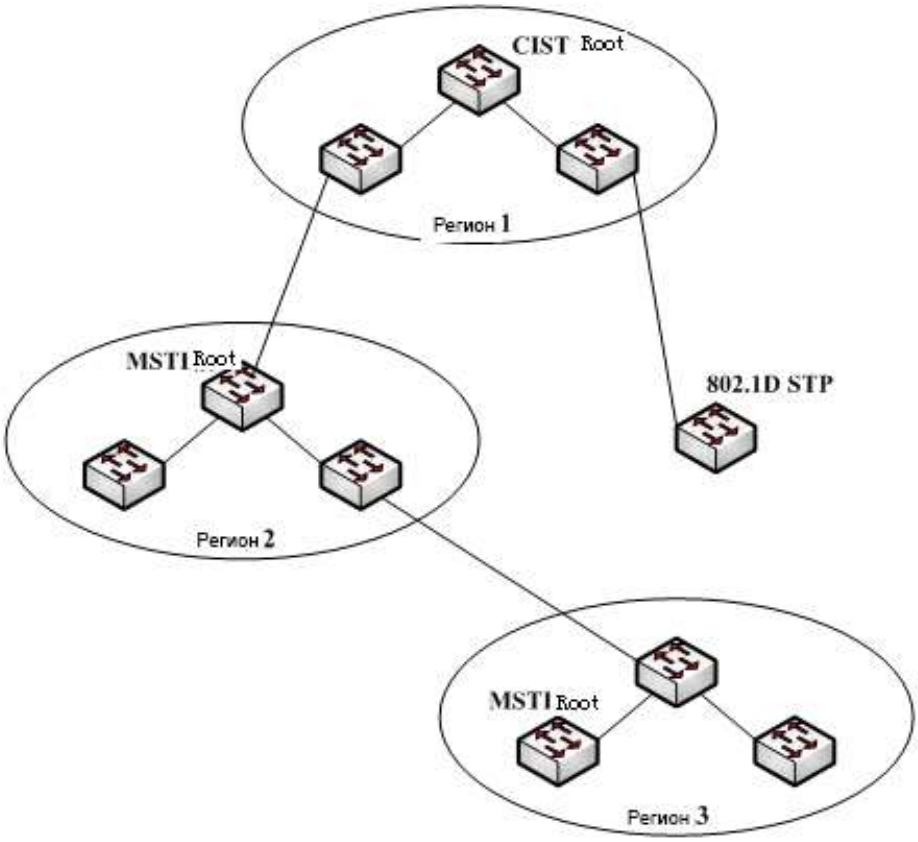

Рисунок 24-1 – Топология MSTP

1. CIST

Общее и внутреннее связующее дерево (CIST) означает связующее дерево, состоящее из всех отдельных коммутаторов и взаимосвязанных локальных сетей. Эти коммутаторы могут принадлежать разным регионам MST. Это могут быть коммутаторы, работающие по традиционному протоколу STP или RSTP. Коммутаторы, использующие STP или RSTP в регионах MST, считаются находящимися в своих регионах.

После того как топология сети стабилизируется, все узлы CIST выбирает корневой мост CIST. В каждом регионе будет выбран внутренний корневой мост, который является кратчайшим путем от центра региона к корню CIST.

2. CST

Если каждый регион MST рассматривать как один коммутатор, общее связующее дерево (CST) – это связующее дерево, соединяющее все «одиночные коммутаторы». Как показано на рисунке 24-1, регионы 1, 2 и 3 и коммутаторы STP составляют сеть CST.

3. IST

Внутреннее связующее дерево (IST) относится к части CIST, которая находится в регионе MST, то есть IST и CST вместе составляют CIST.

4. MSTI

Протокол MSTP позволяет распределять разные VLAN по разным связующим деревьям. Затем создается несколько экземпляров связующего дерева (MSTI). Обычно экземпляр связующего дерева № 0 относится к дереву CIST, которое можно расширить на всю сеть. Каждый экземпляр связующего дерева, начиная с № 1, находится в определенном регионе. Каждый экземпляр связующего дерева может быть распределен по нескольким VLAN. В исходном состоянии все VLAN распределены в CIST.

MSTI в регионах MST является независимыми. Они могут выбирать разные коммутаторы в качестве собственных корней.

24.1.4 Роли порта

Порты в MSTP могут выполнять разные роли, подобно портам в RSTP.

1. Корневой порт (root port)

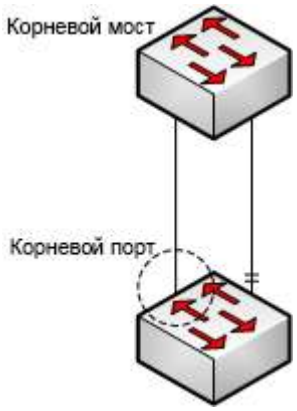

Рисунок 24-2 – Корневой порт

Корневой порт – это наилучший порт для создания соединения между текущим коммутатором и корневым мостом, который имеет минимальную стоимость пути.

2. Альтернативный порт (alternate port)

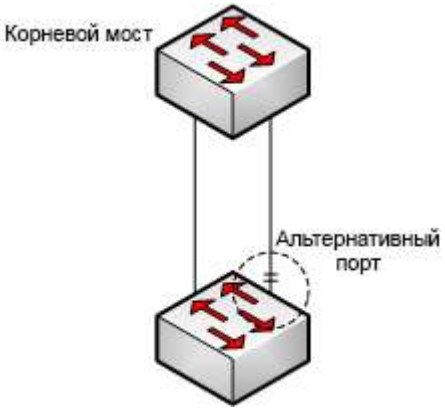

Рисунок 24-3 – Альтернативный порт

Альтернативный порт – это резервный порт для связи между текущим коммутатором и корневым мостом. Если соединение корневого порта выходит из строя, альтернативный порт может быстро превратиться в новый корневой порт без прерывания связи.

3. Назначенный порт (designated port)

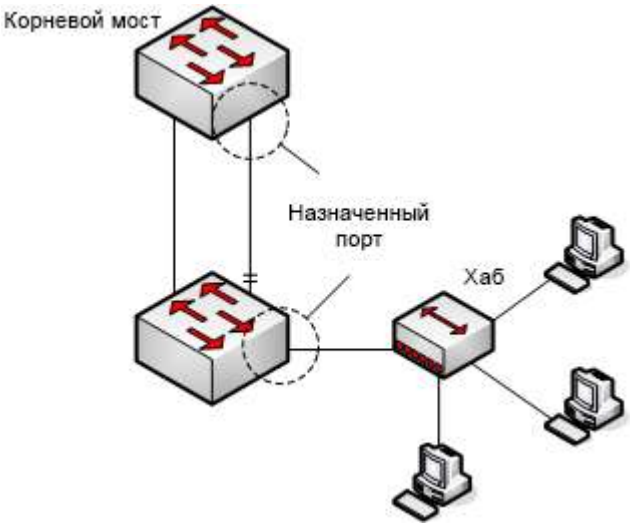

Рисунок 24-4 – Назначенный порт

Назначенный порт может подключаться к коммутаторам или локальной сети в следующем регионе. Это путь между текущей локальной сетью и корневым мостом.

4. Резервный порт (backup port)

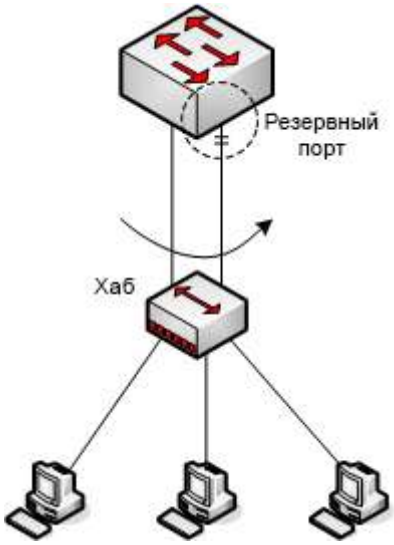

Рисунок 24-5 – Резервный порт

Когда два порта коммутатора подключаются напрямую или оба подключаются к одной и той же локальной сети, порт с более высоким приоритетом должен быть назначенным портом, а другой порт – резервным. Если назначенный порт выходит из строя, резервный берёт на себя его роль для продолжения бесперебойной работы.

5. Мастер-порт (master port)

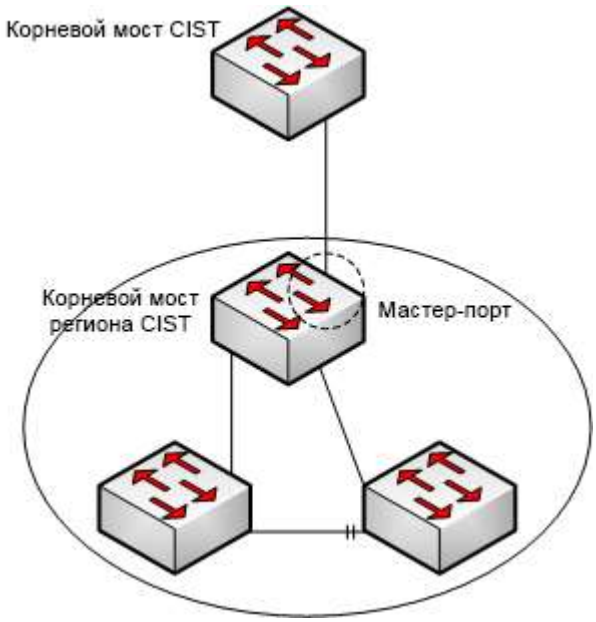

Рисунок 24-6 – Мастер-порт

Мастер-порт – порт, который соединяет регион MST с общим корневым мостом и имеет к нему кратчайший путь. Мастер-порт – это корневой порт корневого моста в регионе CIST.

6. Граничный порт (boundary port)

Граничные порты, относящиеся к CIST, имеют небольшое отличие от поведения граничных портов других экземпляров MSTI. Граничный порт внутри MSTI ограничивает расширение связующего дерева через этот порт, что может быть полезным при разделении сети на несколько взаимосвязанных областей.

7. Конечный порт (edge port)

В протоколе RSTP или протоколе MSTP конечный порт означает порт, напрямую соединяющий сетевой хост. Эти порты могут напрямую переходить в состояние пересылки, минуя состояния прослушивания (listening) и обучения (learning) и не создавая петель в сети.

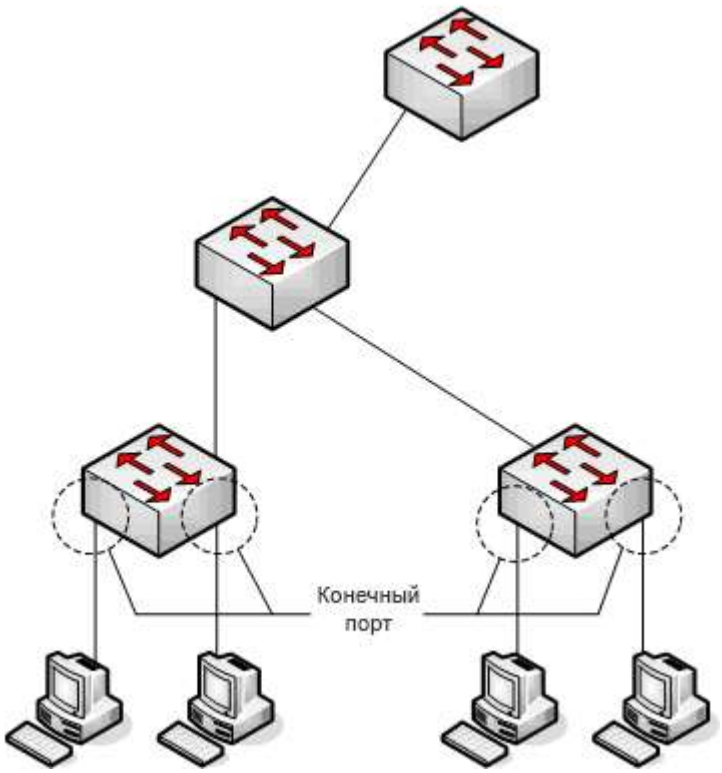

Рисунок 24-7 – Конечный порт

В исходном состоянии MTSP и RSTP не используют все порты в качестве конечных, что обеспечивает возможность быстрого создания топологии сети. Если порт получает BPDU от других коммутаторов, он возобновляет работу в нормальном режиме. Если порт получает 802.1D STP BPDU, он должен подождать время, равное удвоенному значению задержки пересылки, а затем перейти в состояние передачи данных.

24.1.5 MSTP BPDU

Подобно STP и RSTP, коммутаторы, работающие под управлением MSTP, могут взаимодействовать друг с другом при помощи обмена сообщениями, в которых содержится блок данных протокола моста (BPDU). Вся информация о конфигурации CIST и MSTI может передаваться через BPDU. В таблицах 24-1 и 24-2 представлена структура BPDU, используемая MSTP.

Таблица 24-1 – MSTP BPDU

Имя поля	Номер байта
Protocol Identifier (идентификатор протокола)	1–2
Protocol Version Identifier (идентификатор версии протокола)	3
BPDU Type (тип BPDU)	4
CIST Flags (флаги CIST)	5
CIST Root Identifier (идентификатор корневого моста CIST)	6–13
CIST External Root Path Cost (затраты на внешний путь корневого моста CIST)	14–17
CIST Regional Root Identifier (идентификатор регионального корневого моста CIST)	18–25
CIST Port Identifier (идентификатор порта CIST)	26–27
Message Age (возраст сообщения)	28–29
Max Age (максимальный возраст)	30–31
Hello Time (время приветствия)	32–33
Forward Delay (задержка пересылки)	34–35
Version 1 Length (длина версии 1)	36
Version 3 Length (длина версии 3)	37–38
Format Selector (выбор формата)	39
Configuration Name (название конфигурации)	40–71
Revision (ревизия)	72–73
Configuration Digest (дайджест конфигурации)	74–89
CIST Internal Root Path Cost (затраты на внутренний корневой путь CIST)	90–93
CIST Bridge Identifier (идентификатор моста CIST)	94–101
CIST Remaining Hops (оставшиеся хопы CIST)	102
MSTI Configuration Messages (сообщения о конфигурации MSTI)	103 ~

Таблица 24-2 – Информация о конфигурации MSTI

Имя поля	Номер байта
MSTI FLAGS (флаги MSTI)	1
MSTI Regional Root Identifier (идентификатор регионального корневого моста MSTI)	2–9
MSTI Internal Root Path Cost (затраты на внутренний корневой путь MSTI)	10–13
MSTI Bridge Priority (приоритет моста MSTI)	14
MSTI Port Priority (приоритет порта MSTI)	15
MSTI Remaining Hops (оставшиеся переходы MSTI)	16

24.1.6 Стабильное состояние

Коммутатор MSTP выполняет вычисления и сравнивает операции в соответствии с полученными BPDU и, наконец, гарантирует, что:

1. Один коммутатор выбирается в качестве корня CIST всей сети.
2. Каждый коммутатор и сегмент локальной сети могут определить минимальную стоимость пути к корню CIST, обеспечивая устойчивое соединение и предотвращая образование петель.
3. Каждый регион имеет коммутатор в качестве регионального корня CIST. Коммутатор имеет путь к корню CIST с минимальной стоимостью.
4. Каждый MSTI может независимо выбирать коммутатор в качестве регионального корня MSTI.
5. Каждый коммутатор в регионе и сегменте локальной сети может определить путь с минимальной стоимостью к корню MSTI.
6. Корневой порт CIST обеспечивает путь с минимальной стоимостью между региональным корнем CIST и корнем CIST.
7. Назначенный порт CIST предоставляет своей локальной сети путь с минимальной стоимостью к корню CIST.
8. Альтернативный порт и резервный порт обеспечивают соединение, когда коммутатор, порт или локальная сеть не работают или отключены.
9. Корневой порт MSTI обеспечивает путь с минимальной стоимостью к региональному корню MSTI.
10. Назначенный порт MSTI обеспечивает путь с минимальной стоимостью к региональному корню MSTI.
11. Мастер-порт обеспечивает соединение между регионом и корнем CIST. В регионе корневой порт регионального корня CIST функционирует как мастер-порт всех MSTI в регионе.

24.1.7 Подсчет переходов

В отличие от STP и RSTP, протокол MSTP не использует возраст сообщения и максимальный возраст в BPDU для расчета топологии сети. Чтобы решить эту задачу, MSTP использует счетчик переходов (хопов).

Чтобы предотвратить зацикливание информации, MSTP связывает передаваемую информацию с атрибутом количества переходов в каждом связующем дереве. Атрибут количества переходов для BPDU обозначается региональным корнем CIST или региональным корнем MSTI и уменьшается на каждом принимающем порту. Если счетчик переходов на порту становится равным 0, информация будет удалена, а сам порт станет назначенным.

24.1.8 Совместимость с STP

MSTP позволяет коммутатору работать с традиционным коммутатором STP посредством механизма преобразования протокола. Если один порт коммутатора получает сообщение конфигурации STP, этот порт затем передает только сообщение STP. В то же время порт, который получает информацию STP, считается граничным (boundary) портом.

Когда порт находится в состоянии STP-совместимости, он не перейдет автоматически в состояние MSTP, даже если порт больше не получает сообщений STP. В этом случае вы можете запустить команду **spanning-tree mstp migration-check**, чтобы очистить сообщения STP, полученные портом, и вернуть порт в состояние MSTP.

Коммутатор, использующий протокол RSTP, может идентифицировать и обрабатывать сообщение MSTP, не требуя при этом преобразования протокола.

24.2 Настройка MSTP

Задачи настройки

- Конфигурация MSTP по умолчанию
- Включение и отключение MSTP
- Настройка области MSTP
- Настройка корневого моста сети
- Настройка вторичного корневого моста
- Настройка приоритета моста
- Настройка временных параметров STP

- Настройка диаметра сети
- Настройка максимального количества переходов
- Настройка приоритета порта
- Настройка стоимости пути для порта
- Настройка конечного порта
- Настройка типа подключения порта
- Активация режима совместимости с MST
- Перезапуск проверки конвертации протоколов
- Настройка ограничения роли порта
- Настройка ограничения TCN порта
- Проверка информации MSTP

24.2.1 Конфигурация MSTP по умолчанию

Атрибут	Настройки по умолчанию
STP mode (режим STP)	SSTP (PVST, RSTP и MSTP не запущены)
Area name (имя региона)	Строка символов MAC-адреса
Area edit level (уровень редактирования региона)	0
MST configuration list (список настроек MST)	Все VLAN сопоставлены с CIST (MST00)
Spanning-tree priority (CIST and all MSTI) (приоритет связующего дерева (CIST и все MSTI)	32768
Spanning-tree port priority (CIST and all MSTI) (приоритет порта связующего дерева (CIST и все MSTI)	128
Path cost of the spanning-tree port (CIST and all MSTI) (стоимость пути порта связующего дерева (CIST и все MSTI)	1000 Мбит/с: 20000 100 Мбит/с: 200000 10 Мбит/с: 2000000
Hello Time (время приветствия)	2 с
Forward Delay (задержка пересылки)	15 с
Maximum-aging Time (максимальное время устаревания)	20 с
Maximum hop count (максимальное количество переходов)	20

24.2.2 Включение и отключение MSTP

Протокол STP по умолчанию может быть запущен в режиме PVST или SSTP. Вы можете остановить его работу, если связующее дерево не требуется.

Выполните следующую команду, чтобы перевести STP в режим MSTP:

Команда	Описание
spanning-tree	Включает STP в режиме по умолчанию
spanning-tree mode mstp	Включает MSTP

Выполните следующую команду, чтобы отключить STP:

Команда	Описание
no spanning-tree	Выключает STP

24.2.3 Настройка региона MST

Область MST, в которой находится коммутатор, определяется тремя атрибутами: именем конфигурации, номером ревизии, сопоставлением VLAN и MSTI. Вы можете настроить их с помощью команд настройки региона. Обратите внимание, что изменение любого из трех атрибутов приведет к изменению конфигурации региона, в котором находится коммутатор.

В исходном состоянии имя конфигурации MST представляет собой строку символов MAC-адреса коммутатора. Номер ревизии равен 0, и все VLAN отображаются в CIST (MST00). Поскольку разные коммутаторы имеют разные MAC-адреса, коммутаторы, работающие под управлением MSTP, в исходном состоянии находятся в разных регионах. Вы можете запустить команду **spanning-tree mstp instance *instance-id* vlan *vlan-list***, чтобы создать новый MSTI и сопоставить с ним назначенную VLAN. Если MSTI удален, все эти VLAN снова сопоставляются с CIST.

Выполните следующую команду, чтобы настроить информацию о регионе MST:

Команда	Описание
spanning-tree mstp name *string*	Настраивает имя конфигурации MST. **string** означает строку символов имени конфигурации. Она содержит до 32 символа, с учетом заглавных букв. Значением по умолчанию является строка символов MAC-адреса. Устанавливает для имени конфигурации MST значение по умолчанию
no spanning-tree mstp name	Устанавливает для имени конфигурации MST значение по умолчанию
spanning-tree mstp revision *value*	Устанавливает номер ревизии MST.

	value представляет номер в диапазоне от 0 до 65535. Значение по умолчанию – 0
no spanning-tree mstp revision	Возвращает номер ревизии MST к значению по умолчанию
spanning-tree mstp instance *instance-id* **vlan** *vlan-list*	Соотносит VLAN с MSTI. **instance-id** означает номер экземпляра связующего дерева, то есть MSTI. Значение варьируется от 1 до 15. **vlan-list** означает список VLAN, сопоставленных со связующим деревом. Диапазон значений – от 1 до 4094. **instance-id** это независимое значение, представляющее экземпляр связующего дерева. **vlan-list** может представлять группу VLAN, например, «1,2,3», «1-5» и «1,2,5-10»
no spanning-tree mstp instance *instance-id*	Отменяет сопоставление VLAN MSTI и отключает экземпляр связующего дерева. **instance-id** означает номер экземпляра связующего дерева, то есть MSTI. Значение варьируется от 1 до 15

Запустите следующую команду, чтобы проверить настройки региона MSTP:

Команда	Описание
show spanning-tree mstp region	Отображает конфигурацию региона MSTP

24.2.4 Настройка корневого моста сети

В MSTP каждый экземпляр связующего дерева имеет идентификатор моста, содержащий значение приоритета и MAC-адрес коммутатора. При построении топологии связующего дерева в качестве корня сети выбирается коммутатор со сравнительно небольшим идентификатором моста.

Команда **spanning-tree mstp** *instance-id* **root** используется для изменения значения приоритета коммутатора в экземпляре связующего дерева от значения по умолчанию на достаточно маленькое значение, чтобы обеспечить то, что коммутатор станет корнем (root) в этом экземпляре связующего дерева

После выполнения предыдущей команды протокол автоматически проверяет идентификатор моста текущего корня сети, а затем устанавливает поле приоритета идентификатора моста на 24576, когда значение 24576 гарантирует, что текущий коммутатор станет корнем связующего дерева.

Если значение приоритета корня сети меньше значения 24576, MSTP автоматически устанавливает приоритет связующего дерева текущего моста на значение, которое на 4096 меньше значения приоритета корня. Обратите внимание, что число 4096 является шагом изменения значения сетевого приоритета.

При настройке корня вы можете запустить команду с параметром **diameter** для определения диаметра сети связующего дерева. Ключевое слово действует только в том случае, если идентификатор экземпляра связующего дерева равен 0. После установки диаметра сети MSTP автоматически вычисляет правильные параметры времени STP, чтобы обеспечить стабильность сходимости сети. Параметры времени включают время приветствия, задержку пересылки и максимальный возраст. Подкоманду **hello-time** можно использовать для установки нового значения времени приветствия взамен настроек по умолчанию.

Выполните следующую команду, чтобы установить коммутатор в режим корневого моста:

Команда	Описание
spanning-tree mstp *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Настраивает коммутатор в качестве корневого в выбранном связующем дереве. **instance-id** означает номер экземпляра связующего дерева в диапазоне от 0 до 15. **net-diameter** означает диаметр сети, который является необязательным параметром. Эта настройка работает, когда **instance-id** равен 0. Диапазон – от 2 до 7. **seconds** означает единицу времени приветствия в диапазоне от 1 до 10
no spanning-tree mstp *instance-id* **root**	Отменяет корневую настройку коммутатора в связующем дереве. **instance-id** означает номер экземпляра связующего дерева в диапазоне от 0 до 15

Выполните следующую команду, чтобы проверить состояние MSTP:

Команда	Описание
show spanning-tree mstp [**instance** *instance-id*]	Отображает информацию о текущем состоянии MSTP

24.2.5 Настройка вторичного корневого моста

После настройки корня сети вы можете запустить команду **spanning-tree mstp** *instance-id* **root secondary**, чтобы назначить один или несколько коммутаторов вторичными (или резервными) корневыми мостами. Они станут корнем сети, если предыдущий корневой мост по определенным причинам не работает.

В отличие от конфигурации основного корня, во время запуска команды MSTP устанавливает приоритет связующего дерева коммутатора равным 28672. Если приоритетные значения других коммутаторов в сети остаются на значениях по умолчанию (32768), то текущий коммутатор может быть назначен вторичным корнем.

При настройке вторичного корня вы можете запустить подкоманды **diameter** и **hello-time** для обновления параметров времени STP. Когда вторичный корень становится первичным корнем и начинает работать, все эти параметры активизируются.

Выполните следующую команду, чтобы настроить коммутатор в качестве вторичного корня сети:

Команда	Описание
spanning-tree mstp *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Настраивает коммутатор в качестве резервного корневого в назначенном связующем дереве. **instance-id** означает номер экземпляра связующего дерева в диапазоне от 0 до 15. **net-diameter** означает диаметр сети, который является необязательным параметром. Эта настройка работает, когда **instance-id** равен 0. Диапазон – от 2 до 7. **seconds** означает единицу времени приветствия в диапазоне от 1 до 10
no spanning-tree mstp *instance-id* **root**	Отменяет корневую настройку коммутатора в связующем дереве. **instance-id** означает номер экземпляра связующего дерева в диапазоне от 0 до 15

Выполните следующую команду, чтобы проверить состояние MSTP:

Команда	Описание
show spanning-tree mstp [**instance** *instance-id*]	Отображает информацию о текущем состоянии MSTP

24.2.6 Настройка приоритета моста

В некоторых случаях вы можете напрямую, не запуская подкоманду **root**, настроить коммутатор в качестве корня сети, настроив приоритет моста. Значение приоритета коммутатора независимо в каждом экземпляре связующего дерева. Поэтому приоритет можно установить самостоятельно.

Выполните следующую команду, чтобы настроить приоритет моста:

Команда	Описание

spanning-tree mstp *instance-id* **priority** *value*	Устанавливает приоритет коммутатора. идентификатор экземпляра означает номер экземпляра связующего дерева в диапазоне от 0 до 15. **value** означает приоритет моста. Это может быть одно из следующих значений: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
no spanning-tree mstp *instance-id* **priority**	Возвращает приоритет моста коммутатора к значению по умолчанию. **instance-id** означает номер экземпляра связующего дерева в диапазоне от 0 до 15.

24.2.7 Настройка временных параметров STP

Ниже приведены параметры времени STP:

- **Hello Time (время приветствия)**

  Интервал отправки сообщения о конфигурации на назначенный порт, когда коммутатор выполняет функции корня сети.

- **Forward Delay (задержка пересылки)**

  Время, необходимое порту при переходе из состояния блокировки в состояние обучения и в состояние пересылки в режиме STP.

- **Max Age (максимальный возраст)**

  Максимальный срок действия информации о конфигурации связующего дерева.

Для снижения вероятности шока топологии сети должны выполняться следующие требования к временным параметрам:

- 2 x (fwd_delay - 1,0) >= max_age
- max_age >= (hello_time + 1) x 2

Выполните следующую команду, чтобы настроить временные параметры протокола множественного связующего дерева:

Команда	Описание
spanning-tree mstp hello-time *seconds*	Устанавливает время приветствия. Параметр **seconds** – это единица измерения времени приветствия в диапазоне от 1 до 10 секунд. Его значение по умолчанию – две секунды

no spanning-tree mstp hello-time	Возвращает время приветствия к значению по умолчанию
spanning-tree mstp forward-time *seconds*	Устанавливает задержку пересылки. Параметр **seconds** – это единица измерения задержки пересылки в диапазоне от 4 до 40 секунд. Его значение по умолчанию – 15 секунд
no spanning-tree mstp forward-time	Возвращает задержку пересылки к значению по умолчанию
spanning-tree mstp max-age *seconds*	Устанавливает максимальный возраст. Параметр **seconds** – это единица измерения максимального возраста в диапазоне от 6 до 40 секунд. Его значение по умолчанию – 20 секунд
no spanning-tree mstp max-age	Возвращает максимальный возраст к значению по умолчанию

Рекомендуется изменять временные параметры STP, настроив корневой мост или диаметр сети. Это обеспечивает правильное изменение параметров времени.

Вновь установленные временные параметры действительны, даже если они не соответствуют требованиям вышеуказанной формулы. Обратите внимание на уведомления консоли при выполнении настройки.

24.2.8 Настройка диаметра сети

Диаметр сети означает максимальное количество коммутаторов между двумя хостами в сети, что отражает масштаб сети.

Вы можете установить диаметр сети MSTP, выполнив команду **spanning-tree mstp diameter** *net-diameter*. Параметр **net-diameter** действителен только для CIST. После настройки три временных параметра STP автоматически обновляются до оптимальных значений.

Запустите следующую команду, чтобы настроить сетевой диаметр:

Команда	Описание
spanning-tree mstp diameter *net-diameter*	Настраивает диаметр сети. Параметр **net-diameter** находится в диапазоне от 2 до 7. Значение по умолчанию – 7
no spanning-tree mstp diameter	Возвращает диаметр сети к значению по умолчанию

Параметр **net-diameter** не сохраняется на коммутаторе не сохраняется как отдельная настройка. Временной параметр сохраняется только при изменении параметра диаметра сети.

24.2.9 Настройка максимального количества переходов

Выполните следующую команду, чтобы настроить максимальное количество переходов (хопов) между узлами в топологии сети.

Команда	Описание
spanning-tree mstp max-hops *hop-count*	Указывает максимальное количество переходов. Диапазон **hop-count** от 1 до 40. Значение по умолчанию – 20
no spanning-tree mstp *hop-count*	Восстановить значение **hop-count** по умолчанию

24.2.10 Настройка приоритета порта

Если между двумя портами коммутатора возникает петля, порт с более высоким приоритетом перейдет в состояние пересылки, а порт с более низким приоритетом блокируется. Если все порты имеют одинаковый приоритет, порт с меньшим номером первым перейдет в состояние пересылки.

В режиме настройки интерфейса выполните следующие команды, чтобы установить приоритет порта STP:

Команда	Описание
spanning-tree mstp *instance-id* **port-priority** *priority*	Устанавливает приоритет порта STP. **instance-id** обозначает номер экземпляра связующего дерева в диапазоне от 0 до 15. **priority** означает приоритет порта. Это может быть одно из следующих значений: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240
spanning-tree port-priority *value*	Устанавливает приоритет порта во всех экземплярах связующего дерева. **value** обозначает приоритет порта. Это может быть одно из следующих значений: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240
no spanning-tree mstp *instance-id* **port-priority**	Возвращает приоритет порта к значению по умолчанию
no spanning-tree port-priority	Возвращает приоритет порта к значению по умолчанию во всех экземплярах связующего дерева

24.2.11 Настройка стоимости пути порта

В MSTP значение стоимости пути порта по умолчанию зависит от скорости соединения. Если между двумя коммутаторами возникает петля, порт с меньшей стоимостью пути перейдет в состояние пересылки. Чем меньше стоимость пути, тем выше скорость порта. Если все порты имеют одинаковую стоимость пути, порт с меньшим номером первым перейдет в состояние пересылки.

В режиме настройки интерфейса выполните следующую команду, чтобы установить стоимость пути порта:

Команда	Описание
spanning-tree mstp *instance-id* **cost** *cost*	Устанавливает стоимость пути для порта. **instance-id** обозначает номер экземпляра связующего дерева в диапазоне от 0 до 15. **cost** означает стоимость пути порта, которая колеблется от 1 до 200000000
spanning-tree cost *value*	Устанавливает стоимость пути порта во всех экземплярах связующего дерева. **value** обозначает стоимость пути, которая находится в диапазоне от 1 до 200000000
no spanning-tree mstp *instance-id* **cost**	Возвращает стоимость пути порта к значению по умолчанию
no spanning-tree cost	Возвращает стоимость пути порта к значению по умолчанию во всех экземплярах связующего дерева

24.2.12 Настройка конечного порта

Конечный, или граничный порт (edge port) означает, что этот порт подключается к терминальному устройству в сети. Настроенный принудительно конечный порт будет находиться в состоянии пересылки сразу после установления соединения, минуя состояние прослушивания и обучения. Используйте следующую команду для настройки конечного порта MSTP в режиме настройки интерфейса:

Команда	Описание
spanning-tree mstp edge	Принудительно настраивает порт в качестве конечного
no spanning-tree mstp edge	Восстановление режима конечного порта, проверяемого автоматически

24.2.13 Настройка типа подключения порта

Если соединение между коммутаторами с поддержкой MSTP является прямым соединением «точка-точка», коммутаторы могут быстро установить соединение с

помощью механизма квитирования. При настройке типа подключения порта установите режим «точка-точка».

Протокол решает, использовать ли соединение «точка-точка» или нет, в зависимости от атрибута дуплекса. Если порт работает в полнодуплексном режиме, протокол считает соединение двухточечным. Если порт работает в полудуплексном режиме, протокол считает соединение общим.

Если подтвердится, что коммутатор, подключенный к порту, работает по протоколу RSTP или MSTP, тип подключения порта можно настроить как точка-точка, чтобы гарантировать возможность быстрого подтверждения связи.

Для указания типа подключения порта используйте следующую команду в режиме настройки интерфейса:

Команда	Описание
spanning-tree mstp point-to-point force-true	Устанавливает тип подключения порта «точка-точка»
spanning-tree mstp point-to-point force-false	Устанавливает тип подключения порта «общий»
spanning-tree mstp point-to-point auto	Автоматически проверяет тип подключения порта
no spanning-tree mstp point-to-point	Восстанавливает тип подключения порта до настроек по умолчанию

24.2.14 Активация режима совместимости MST

Протокол MSTP, который поддерживают данные коммутаторы, основан на IEEE 802.1s. Чтобы быть совместимым с другими протоколами MSTP, особенно с тем, который поддерживают коммутаторы Cisco, протокол может работать в режиме MST-совместимости. Коммутаторы, работающие в режиме совместимости, могут идентифицировать структуру сообщений других MSTP, проверять содержащийся региональный идентификатор MST и устанавливать регион MST.

MST- и STP-совместимые режимы основаны на механизме преобразования протокола MSTP. Если какой-либо порт коммутатора получает BPDU в совместимом режиме, он автоматически переходит в нужный режим и в нем отправляет BPDU. Чтобы возобновить работу порта в стандартном режиме MST, вы можете запустить команду **spanning-tree mstp migration-check**.

В режиме глобальной конфигурации выполните следующие команды, чтобы включить или отключить режим MST-совместимости:

Команда	Описание
spanning-tree mstp mst-compatible	Включает MST-совместимый режим коммутатора
no spanning-tree mstp mst-compatible	Отключает MST-совместимый режим коммутатора

- Основная функция режима совместимости – создание области MST, в которой будут коммутаторы, работающие по протоколу MSTP. В реальной сети убедитесь, что коммутатор имеет то же имя конфигурации и тот же номер редактирования. Рекомендуется настроить узел, работающий с другими протоколами MSTP, в качестве корня CIST, гарантируя, что коммутатор перейдет в режим совместимости путем получения сообщения.
- Если режим совместимости с MST не включен, то коммутатор будет неспособен корректно обрабатывать контент, совместимый с BPDU, и не сможет правильно взаимодействовать с другим коммутатором, который поддерживает MST. Из-за этого такие два коммутатора не смогут работать в одном регионе.
- Порт в режиме совместимости не может автоматически возобновить отправку стандартного MST BPDU, даже если этот режим отключен глобально. В этом случае запустите **migration-check**.

24.2.15 Перезапуск проверки конвертации протоколов

MSTP позволяет коммутатору работать с традиционным коммутатором STP посредством механизма преобразования протокола. Если один порт коммутатора получает сообщение о конфигурации STP, этот порт затем передает только сообщения STP. В то же время порт, который получает информацию STP, считается граничным портом.

Когда порт находится в состоянии STP-совместимости, он не перейдет автоматически в режим MSTP, даже если больше не получает сообщений STP. В этом случае вы можете запустить команду **spanning-tree mstp migration-check**, чтобы очистить сообщения STP, полученные портом, и вернуть порт в режим MSTP.

Коммутатор, использующий протокол RSTP, может идентифицировать и обрабатывать сообщение MSTP. Таким образом, коммутатор MSTP не требует преобразования протокола при работе с коммутатором RSTP.

В режиме глобальной конфигурации выполните следующую команду, чтобы очистить всю информацию STP, обнаруженную всеми портами коммутатора:

Команда	Описание
spanning-tree mstp migration-check	Очищает всю информацию STP, обнаруженную всеми портами коммутатора

В режиме настройки интерфейса выполните следующую команду, чтобы очистить информацию STP, обнаруженную выбранным портом:

Команда	Описание
spanning-tree mstp migration-check	Очищает всю информацию STP, обнаруженную выбранным портом

24.2.16 Настройка ограничения ролей порта

Функция настройки ограничения роли порта может привести к тому, что порт не будет выбран в качестве корневого.

Используйте следующую команду для настройки ограничения роли порта в режиме настройки интерфейса:

Команда	Описание
spanning-tree mstp restricted-role	Запрещает выбирать порт в качестве корневого

24.2.17 Настройка ограничения TCN порта

Настройка ограничения TCN может запретить порту распространять сообщения об изменения топологии на другие порты.

В режиме настройки интерфейса используйте следующую команду для запрета отправки портом TCN-сообщений:

Команда	Описание
spanning-tree mstp restricted-tcn	Запрещает порту распространять сообщения изменения топологии на другие порты

24.2.18 Проверка информации MSTP

В командном режиме системного мониторинга, глобальной конфигурации или настройки интерфейса выполните следующие команды, чтобы проверить всю информацию о настройках MSTP.

Команда	Описание
show spanning-tree	Отображает информацию MSTP. (Можно проверить информацию о SSTP, PVST, RSTP и MSTP)
show spanning-tree detail	Отображает детальную информацию MSTP. Можно проверить информацию о SSTP, PVST, RSTP и MSTP

show spanning-tree interface *interface-id*	Отображает информацию STP-порта. Можно проверить информацию о SSTP, PVST, RSTP и MSTP
show spanning-tree mstp	Отображает все экземпляры MST
show spanning-tree mstp region	Отображает настройки региона MST
show spanning-tree mstp instance *instance-id*	Отображает указанный экземпляр MST
show spanning-tree mstp detail	Отображает детальную информацию MST
show spanning-tree mstp interface *interface-id*	Отображает настройки MST-порта
show spanning-tree mstp protocol-migration	Отображает статус преобразования протокола на порту

25. Дополнительные функции STP

25.1 Введение

Модуль протокола связующего дерева коммутатора поддерживает семь дополнительных функций. Эти функции не настроены по умолчанию. Они поддерживаются в различных режимах протокола связующего дерева следующим образом:

Дополнительные функции	SSTP	PVST	RSTP	MSTP
Port Fast	Да	Да	Нет	Нет
BPDU Guard	Да	Да	Да	Да
BPDU Filter	Да	Да	Нет	Нет
Uplink Fast	Да	Да	Нет	Нет
Backbone Fast	Да	Да	Нет	Нет
Root Guard	Да	Да	Да	Да
Loop Guard	Да	Да	Да	Да

25.1.1 Port Fast

Port Fast (быстрый порт) немедленно переводит интерфейс, настроенный как порт доступа или транковый порт, в состояние пересылки из состояния блокировки, минуя состояния прослушивания и обучения. Вы можете использовать Port Fast на интерфейсах, подключенных к одной рабочей станции или серверу, чтобы позволить этим устройствам немедленно подключаться к сети, не дожидаясь сходимости связующего дерева.

Интерфейсы, подключенные к одной рабочей станции или серверу, не должны получать блоки данных протокола моста (BPDU). Однако использование Port Fast может привести к появлению петель в сети, если на порт будет подключен другой коммутатор или устройство, которое может создать дополнительные соединения. Поэтому рекомендуется

использовать Port Fast только на портах, подключенных к устройствам конечных пользователей.

Функцию Port Fast можно настроить как в режиме глобальной конфигурации, так и в режиме настройки интерфейса. Если настроен глобальный режим, все порты будут считаться портами Port Fast и быстро перейдут в состояние пересылки. Таким образом будет увеличена вероятность создания сетевых петель. Чтобы предотвратить это, вы можете использовать функции BPDU Guard или BPDU Filter для защиты портов.

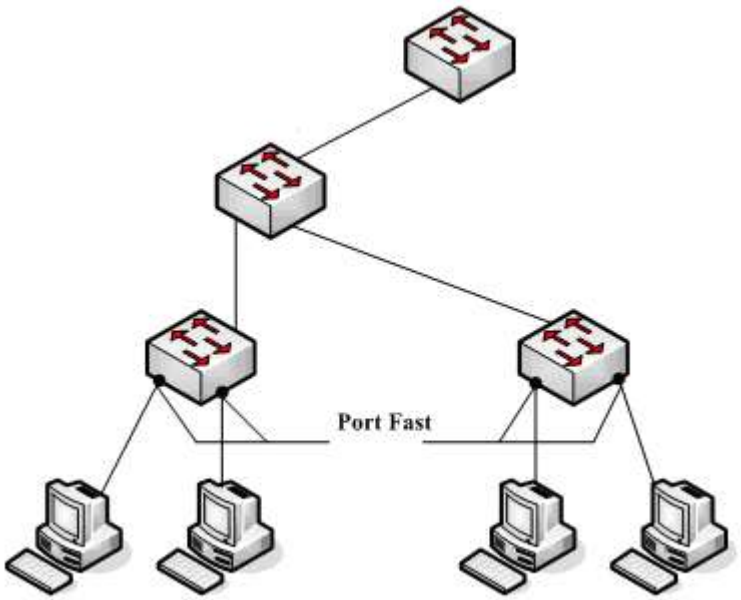

Рисунок 25-1 – Port Fast

Быстрые протоколы связующего дерева RSTP и MSTP могут немедленно перевести интерфейс в состояние пересылки, поэтому в таком случае нет необходимости использовать функцию Port Fast.

25.1.2 BPDU Guard

Если порт с поддержкой Port Fast получает BPDU, это может быть связано с плохой конфигурацией сети. Функция BPDU Guard (защита BPDU) пассивно защищает порт после получения BPDU.

BPDU Guard ведет себя по-разному в разных протоколах связующего дерева. В режиме SSTP/PVST порт с поддержкой Port Fast, который также имеет настройку BPDU Guard, принудительно отключается после получения BPDU, и в дальнейшем пользователь может только вручную настроить его для восстановления работы. В режиме RSTP/MSTP обычный

порт, настроенный с помощью BPDU Guard, будет переведен в состояние блокировки на определенный период времени, если он получит BPDU.

Функцию BPDU Guard можно настроить независимо от функции Port Fast. Во всех режимах протокола связующего дерева порт, настроенный с BPDU Guard, по-прежнему будет отправлять BPDU, а также получать и обрабатывать BPDU. В режиме RSTP/MSTP настройка BPDU Guard на порту может предотвратить получение BPDU устройствами, подключенными к коммутатору.

Функцию BPDU Guard можно настроить в режиме глобальной конфигурации или в режиме настройки интерфейса. В глобальном режиме использование команды **spanning-tree portfast bpduguard** не помешает порту отправлять BPDU. Важно отметить, что в более сложной сети неправильное использование функции BPDU Guard может привести к образованию петель.

25.1.3 BPDU Filter

Функция фильтрации BPDU может быть включена глобально на коммутаторе или для каждого интерфейса, но эта функция работает с некоторыми отличиями.

В режиме SSTP/PVST, если порт Port Fast с настроенным фильтром BPDU получает BPDU, функции BPDU Filter и Port Fast на порту будут автоматически отключены, и порт снова станет обычным портом. Прежде чем перейти в состояние пересылки, такой порт должен находиться в состояниях прослушивания и обучения.

Функцию фильтра BPDU можно настроить глобально или в режиме настройки интерфейса. В режиме глобальной конфигурации запустите команду **spanning-tree portfast bpdufilter**, чтобы заблокировать все порты для отправки BPDU. Однако порт по-прежнему может получать и обрабатывать BPDU.

25.1.4 Uplink Fast

Функция Uplink Fast (быстрый восходящий канал) позволяет новым корневым портам быстро переходить в состояние пересылки, когда соединение между коммутатором и корневым мостом разрывается.

Сложная сеть всегда содержит несколько уровней устройств, как показано на рисунке 25-2. И уровень агрегации, и уровень доступа коммутатора имеют резервные соединения с верхним уровнем. Эти резервные соединения обычно блокируются STP, чтобы избежать петель.

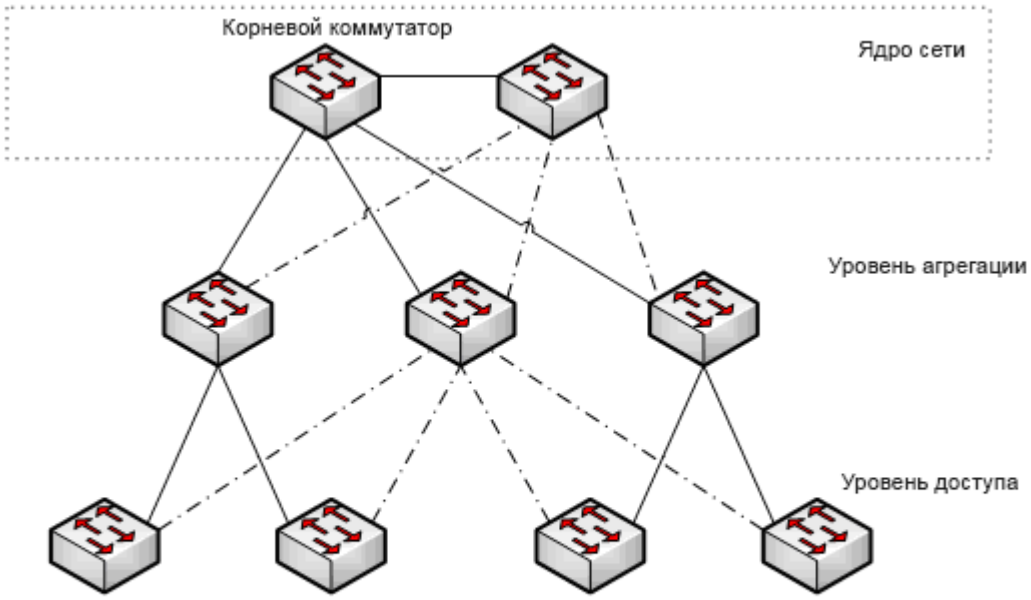

Рисунок 25-2 – Топология сети

Предположим, что соединение между коммутатором и верхним уровнем разорвано (это называется отказом прямого канала), STP выбирает альтернативный порт на линии резервирования в качестве корневого порта. Перед переходом в состояние пересылки альтернативный порт должен находиться в состоянии прослушивания и обучения. Если функция Uplink Fast настроена путем запуска команды **spanning-tree uplinkfast** в режиме глобальной конфигурации, новый корневой порт может напрямую перейти в состояние пересылки, возобновляя соединение между коммутатором и верхним уровнем.

На рисунке 25-3 показан принцип работы функции Uplink Fast. Порт коммутатора C, находясь в исходном состоянии, является резервным портом для подключения коммутатора B. Когда соединение между коммутатором C и корневым коммутатором A разрывается, альтернативный порт выбирается в качестве нового корневого порта и немедленно начинается пересылка.

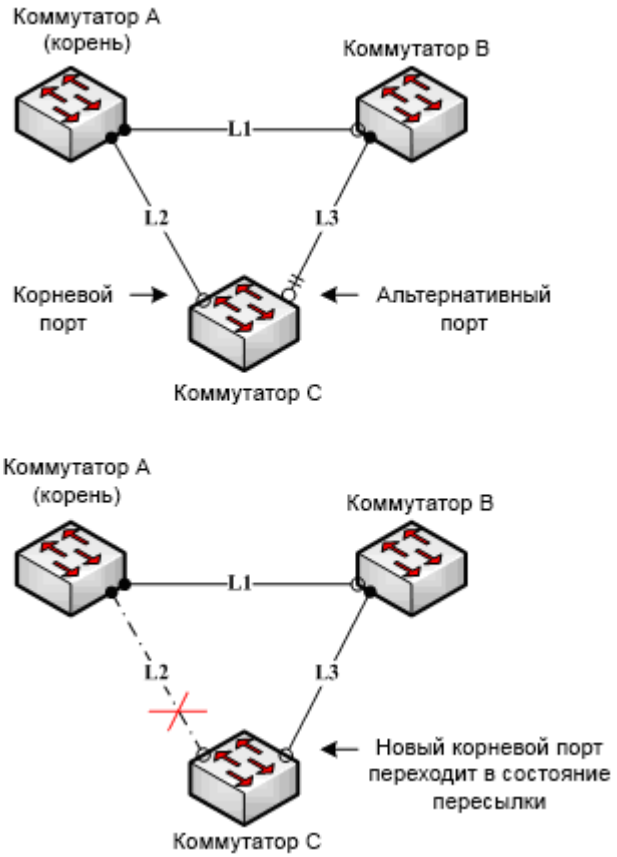

Рисунок 25-3 – Uplink Fast

Функция Uplink Fast оптимизирует поведение коммутатора при медленной сходимости протоколов STP (SSTP) и PVST, что обеспечивает более быстрое восстановление связности после обрыва пути. Однако в других протоколах, таких как RSTP и MSTP, новый корневой порт может быстро перейти в состояние пересылки без использования функции Uplink Fast. В этих протоколах быстродействие восстановления связности уже заложено в характеристики протокола, и Uplink Fast не требуется для ускорения процесса.

25.1.5 Backbone Fast

Функция Backbone Fast (быстрое магистральное соединение) является дополнением технологии Uplink Fast. Технология Uplink Fast обеспечивает быструю работу резервной линии в случае разрыва прямого соединения с назначенным коммутатором, а технология Backbone Fast помогает обнаруживать косвенные сетевые разрывы (проблемы с соединением) на верхнем уровне сети и ускоряет процесс изменения состояния портов.

На рисунке 25-3 соединение L2 между коммутатором C и коммутатором A называется прямым соединением между коммутатором C и корневым коммутатором A. Если

соединение разорвано, функция Uplink Fast может решить проблему. Соединение L1 между коммутаторами A и B называется косвенным каналом коммутатора C. Отключенное косвенное соединение называется косвенным сбоем, который обрабатывается функцией Backbone Fast.

Принцип работы функции Backbone Fast показан на рисунке 25-4.

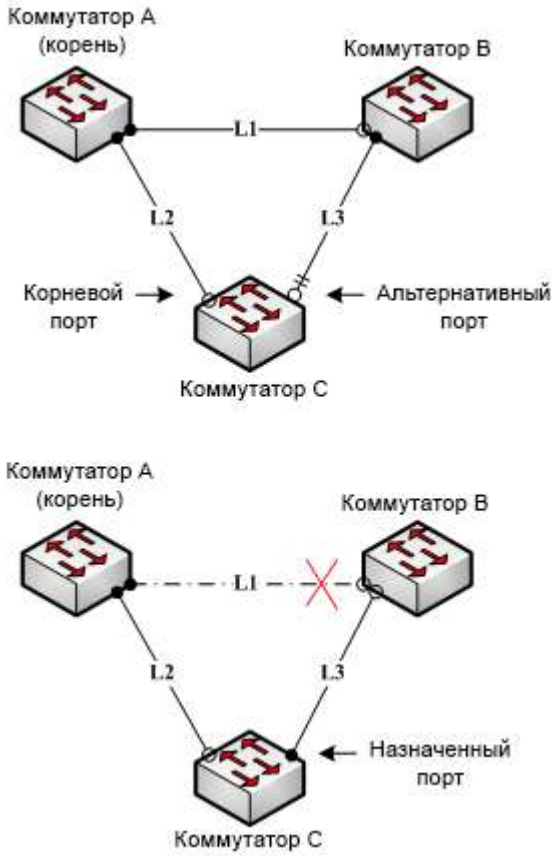

Рисунок 25-4 – Backbone Fast

Предположим, что приоритет моста коммутатора C выше, чем приоритет моста коммутатора B. Когда L1 отключен, коммутатор B выбирается для отправки BPDU коммутатору C, поскольку приоритет моста используется в качестве корневого приоритета. Что касается коммутатора C информация, содержащаяся в BPDU, не приоритетна информации, содержащейся в нем самом. Если Backbone Fast не включен, порт между коммутатором C и коммутатором B ожидает информацию в течение установленного времени устаревания, а затем становится назначенным портом. Это обычно занимает несколько секунд. После того, как функция включена в режиме глобальной конфигурации с помощью команды **spanning-tree backbonefast**, когда альтернативный порт коммутатора C получает BPDU с более низким приоритетом, коммутатор C считает, что соединение по косвенному каналу, способное достигнуть корневого коммутатора, на порту

отключено. После этого коммутатор С незамедлительно переводит порт в статус назначенного, не дожидаясь окончания времени устаревания.

После включения функции Backbone Fast, если на разных портах будут получены BPDU с низким приоритетом, коммутатор будет выполнять разные действия. Если альтернативный порт получает сообщение, он становится назначенным. Если корневой порт получает сообщение с низким приоритетом и нет другого резервного порта, коммутатор сам становится корневым коммутатором.

Обратите внимание, что функция Backbone Fast просто не учитывает время устаревания информации. Новый назначенный порт по-прежнему должен следовать порядку изменения состояния: состояние прослушивания, затем состояние обучения и, наконец, состояние пересылки.

Подобно Uplink Fast, функция Backbone Fast эффективна в режимах SSTP и PVST, но не имеет смысла в RSTP и MSTP.

25.1.6 Root Guard

Функция Root Guard (защита корня) предотвращает переход порта в статус корневого из-за получения высокоприоритетного BPDU.

Сеть второго уровня поставщика услуг (SP) может включать в себя множество подключений к коммутаторам, которые не принадлежат самому поставщику услуг. В такой топологии связующее дерево может переконфигурироваться и выбрать пользовательский коммутатор в качестве корневого. Вы можете избежать этой ситуации, включив Root Guard на интерфейсах коммутатора SP, которые подключаются к коммутаторам в сети вашего клиента. Если расчеты связующего дерева приводят к выбору интерфейса в сети клиента в качестве корневого порта, Root Guard затем переводит интерфейс в заблокированное состояние, чтобы коммутатор клиента не стал корневым коммутатором или мостом на пути к корню.

Если коммутатор вне сети SP становится корневым коммутатором, интерфейс блокируется, и связующее дерево выбирает новый корневой коммутатор. Коммутатор клиента не становится корневым коммутатором и не находится на пути к корню.

Если коммутатор работает в режиме множественного связующего дерева (MST), Root Guard принудительно определяет интерфейс на роль назначенного порта. Если граничный порт заблокирован во внутреннем экземпляре связующего дерева (IST) из-за Root Guard, интерфейс также блокируется во всех экземплярах MST. Граничный порт – это интерфейс, который подключается к локальной сети, назначенным коммутатором которой является либо коммутатор IEEE 802.1D, либо коммутатор с другой конфигурацией региона MST.

Функция Root Guard, включенная на интерфейсе, применяется ко всем сетям VLAN, к которым принадлежит интерфейс. Сети VLAN можно сгруппировать и сопоставить с экземпляром MST.

Эту функцию можно включить на интерфейсе с помощью команды **spanning-tree guard root**.

Функция Root Guard действует по-разному в SSTP/PVST и RSTP/MSTP. В режиме SSTP/PVST корневой порт всегда блокируется Root Guard. В режиме RSTP/MSTP корневой порт не будет заблокирован до получения BPDU более высокого уровня. Порт, который ранее играл роль корневого, не будет заблокирован.

25.1.7 Loop Guard

Функция Loop Guard (защита от петель) может быть использована, чтобы предотвратить превращение альтернативных или корневых портов в назначенные из-за сбоя, который приводит к однонаправленному соединению. Эта функция наиболее эффективна, когда она включена во всей коммутируемой сети. Loop Guard не позволяет альтернативным и корневым портам стать назначенными портами, а связующее дерево не отправляет BPDU на корневые или альтернативные порты.

Вы можете включить эту функцию с помощью команды **spanning-tree loopguard default** в режиме глобальной конфигурации.

Когда коммутатор работает в режиме PVST+ или Rapid-PVST+, Loop Guard предотвращает превращение альтернативных и корневых портов в назначенные порты, а связующее дерево не отправляет BPDU на корневые или альтернативные порты.

Когда коммутатор работает в режиме MST, BPDU не отправляются на неграничные порты только если Loop Guard блокирует интерфейс во всех экземплярах MST. На граничном порту Loop Guard блокирует интерфейс во всех экземплярах MST.

Функция Loop Guard действует по-разному в SSTP/PVST и RSTP/MSTP. В режиме SSTP/PVST нестабильный порт всегда блокируется функцией Loop Guard. В режиме RSTP/MSTP порт будет заблокирован только в том случае, если он стал назначенным из-за недоступности для приема BPDU. Loop Guard не будет блокировать порт, который выполняет роль назначенного из-за получения BPDU нижнего уровня.

25.2 Настройка дополнительных функций STP

25.2.1 Настройка Port Fast

Интерфейс с включенной функцией Port Fast переводится непосредственно в состояние пересылки сообщений связующего дерева, не дожидаясь окончания времени стандартной задержки пересылки. Эта функция недействительна в других режимах связующего дерева.

Используйте следующую команду для настройки функции Port Fast в режиме глобальной конфигурации:

Команда	Описание
spanning-tree portfast default	Глобально включает функцию Port Fast. Действительно для всех интерфейсов
no spanning-tree portfast default	Глобально отключает функция Port Fast. Не влияет на конфигурацию интерфейса

Функция Port Fast применяется только к интерфейсу, который подключается к хосту. BPDU Guard или BPDU Filter должны быть настроены одновременно с глобальной настройкой Port Fast.

Используйте следующую команду для включения функции Port Fast в режиме настройки интерфейса:

Команда	Описание
spanning-tree portfast	Включает функцию Port Fast на интерфейсе
no spanning-tree portfast	Отключает функцию Port Fast на интерфейсе. Это не влияет на глобальную конфигурацию

25.2.2 Настройка BPDU Guard

Функция BPDU Guard пассивно защищает порт после получения BPDU, при этом порт продолжает отправлять BPDU.

BPDU Guard ведет себя по-разному в разных протоколах связующего дерева. В режиме SSTP/PVST порт с поддержкой Port Fast, который также настроен с помощью BPDU Guard, принудительно отключается после получения BPDU, после чего пользователь может только вручную настроить его для восстановления работы. В режиме RSTP/MSTP обычный порт, настроенный с помощью BPDU Guard, будет переведен в состояние блокировки на определенный период времени, если он получит BPDU.

В режиме глобальной конфигурации выполните следующие действия, чтобы глобально включить функцию BPDU Guard:

Команда	Описание
spanning-tree portfast bpduguard	Глобально включает функцию BPDU Guard. Это действительно для всех интерфейсов
no spanning-tree portfast bpduguard	Глобально отключает функцию BPDU Guard

Глобальное включение функции Port Fast может привести к широковещательному шторму. В целях защиты необходимо настроить BPDU Guard или BPDU Filter.

Выполните следующие действия, чтобы включить функцию защиты BPDU в режиме настройки интерфейса:

Команда	Описание
spanning-tree bpduguard enable	Включает функцию BPDU Guard на интерфейсе
spanning-tree bpduguard disable **no spanning-tree bpduguard**	Отключает функцию BPDU Guard на интерфейсе. Это не влияет на глобальную конфигурацию

25.2.3 Настройка BPDU Filter

Вам следует включить BPDU Filter в режиме SSTP/PVST, чтобы интерфейс не отправлял BPDU, что также является еще одним методом защиты порта Fast Port.

В режиме глобальной конфигурации выполните следующие действия, чтобы глобально включить функцию BPDU Filter:

Команда	Описание
spanning-tree portfast bpdufilter	Глобально включает функцию BPDU Filter. Это действительно для всех интерфейсов
no spanning-tree portfast bpdufilter	Глобально отключает функцию BPDU Filter

Глобальное включение функции Port Fast может привести к широковещательному шторму. В целях защиты необходимо настроить BPDU Guard или BPDU Filter.

Выполните следующие действия, чтобы включить функцию BPDU Filter в режиме настройки интерфейса:

Команда	Описание
spanning-tree bpdufilter enable	Включает функцию BPDU Filter на интерфейсе
spanning-tree bpdufilter disable **no spanning-tree bpdufilter**	Отключает функцию BPDU Filter на интерфейсе. Это не влияет на глобальную конфигурацию

25.2.4 Настройка Uplink Fast

Функция Uplink Fast позволяет новому корневому порту быстро перейти в состояние пересылки, когда соединение между коммутатором и корневым мостом сети прерывается.

Функция Uplink Fast действительна только в режиме SSTP/PVST.

В режиме глобальной конфигурации выполните следующие шаги, чтобы глобально включить UplinkFast:

Команда	Описание
spanning-tree uplinkfast	Включает функцию UplinkFast
no spanning-tree uplinkfast	Выключает функцию UplinkFast

25.2.5 Настройка Backbone Fast

Функция Backbone Fast дополняет технологию Uplink Fast. Uplink Fast позволяет резервным линиям быстро начать работу, когда прямое соединение с назначенным коммутатором прерывается. Backbone Fast может обнаруживать сбои в косвенных каналах сети верхнего уровня, не связанных напрямую с коммутатором, и ускорять изменение статуса портов.

Функция Backbone Fast действительна только в режиме SSTP/PVST.

В режиме глобальной конфигурации выполните следующие шаги, чтобы глобально включить Backbone Fast:

Команда	Описание
spanning-tree backbonefast	Включает функцию Backbone Fast
no spanning-tree backbonefast	Выключает функцию Backbone Fast

25.2.6 Настройка Root Guard

Функция Root Guard может предотвратить превращение порта с высокоприоритетным BPDU в корневой порт.

Функция Root Guard действует по-разному в SSTP/PVST и RSTP/MSTP. В режиме SSTP/PVST корневой порт всегда блокируется Root Guard. В режиме RSTP/MSTP корневой порт не будет заблокирован до получения BPDU более высокого уровня. Порт, который ранее играл роль корневого, не будет заблокирован.

Выполните следующие действия, чтобы включить Root Guard на интерфейсе:

Команда	Описание
spanning-tree guard root	Включает функцию Root Guard на интерфейсе
no spanning-tree guard	Отключает функции Root Guard и Loop Guard на интерфейсе
spanning-tree guard none	

25.2.7 Настройка Loop Guard

Функция Loop Guard защищает корневой порт или альтернативный порт после того, как он становится назначенным портом. Это предотвращает образование петель на порту, вызванных отсутствием приема BPDU.

Функция Loop Guard в разных режимах действует по-разному. В режиме STP/PVST Loop Guard отслеживает порты, которые находятся в состоянии блокировки и отклонения (так называемые «нестабильные» порты). Если на таком порту пропадает протокольное сообщение BPDU, означающее, что порт перестал получать информацию о топологии сети, Loop Guard активируется и порт переведется в состояние «заблокирован», чтобы предотвратить возможность создания петель.

В режиме RSTP/MSTP Loop Guard следит за портами, на которых должен быть прием сообщений перевыбора корневого моста. Если порт не получает сигнала перевыбора в течение определенного времени, Loop Guard срабатывает и порт переводится в состояние «заблокирован».

Выполните следующие действия, чтобы включить Loop Guard в режиме глобальной конфигурации:

Команда	Описание
spanning-tree loopguard default	Глобально включает функцию Loop Guard. Действительно для всех интерфейсов
no spanning-tree loopguard default	Глобально отключает Loop Guard

Выполните следующие действия, чтобы включить Loop Guard в режиме настройки интерфейса:

Команда	Описание
spanning-tree guard loop	Включает функцию Loop Guard на интерфейсе
no spanning-tree guard	Отключает функции Root Guard и Loop Guard на интерфейсе
spanning-tree guard none	

25.2.8 Настройка Loop Fast

Функция Loop Fast (быстрая обработка петель) применяется для улучшения производительности и сходимости сети, ограниченно в специальной сетевой среде. Например, эта функция включена на каждом порту, составляющем кольцевую сеть, состоящую из десятков коммутаторов.

Используйте следующую команду для включения Loop Fast на всех портах в режиме глобальной конфигурации:

Команда	Описание

spanning-tree loopfast	Глобально включает функцию Loop Fast для всех портов
no spanning-tree loopfast	Глобально отключает Loop Fast

Используйте следующие команды для настройки Loop Fast в режиме настройки интерфейса:

Команда	Описание
spanning-tree loopfast	Включение функции Loop Fast на порту
no spanning-tree loopfast	Отмена всех настроек Loop Fast для порта. При настройке глобального Loop Fast эта функция по-прежнему действительна для остальных портов
spanning-tree loopfast disable	Отключает функцию Loop Fast порта

25.2.9 Настройка ATAP

Address Table Aging Protection (ATAP) – это функция, которая защищает MAC-адреса в таблице MAC-адресов от быстрого истечения их времени жизни.

MAC-адреса хранятся в таблице MAC-адресов коммутатора в течение определенного периода времени, называемого временем жизни записи таблицы. Когда этот период истекает, запись удаляется из таблицы, и при следующем запросе на этот MAC-адрес коммутатору нужно будет выполнить процедуру обучения снова. Это может привести к простою сети и задержкам, пока обучение не будет выполнено.

ATAP предотвращает истечение времени жизни записи таблицы MAC-адресов, когда коммутатор получает трафик от определенного MAC-адреса. Когда функция ATAP включена, коммутатор периодически проверяет записи в своей таблице MAC-адресов, чтобы убедиться, что каждый адрес, который получил трафик за последний промежуток времени, хранится в таблице на более длительный период времени. Если запись о MAC-адресе была обновлена благодаря трафику, то время жизни записи для этого адреса продлевается, и он сохраняется в таблице MAC-адресов на более длительный период.

Функцию быстрого устаревания записей MAC-адресов в протоколе STP можно полностью отключить с помощью команды **no spanning-tree fast-aging**. Прежде чем использовать эту настройку, убедитесь, что в сети нет петли. В противном случае после изменения топологии сети терминальным устройствам может потребоваться 5 минут или больше времени для восстановления связи друг с другом.

Используйте следующие команды для настройки функции ATAP в режиме глобальной конфигурации:

Команда	Описание
spanning-tree fast-aging	Включение/выключение функции быстрого устаревания таблицы адресов
spanning-tree fast-aging protection	Включение/выключение функции защиты от быстрого устаревания таблицы адресов.
spanning-tree fast-aging protection time	Настройка времени защиты таблицы адресов от устаревания. В пределах заданного интервала времени алгоритм Spanning Tree может вызвать устаревание и удаление записей из адресной таблицы только один раз. Время по умолчанию – 15 секунд

25.2.10 Настройка FDB-Flush

Протокол быстрого связующего дерева коммутатора (RSTP и MSTP) исключает старый MAC-адрес, используя метод быстрого устаревания таблицы адресов, а не метод FDB-Flush в конфигурации по умолчанию.

Используйте следующие команды для включения FDB-Flush в режиме глобальной конфигурации:

Команда	Описание
spanning-tree fast-aging flush-fdb	Включение FDB-Flush
no spanning-tree fast-aging flush-fdb	Отключение FDB-Flush

25.2.11 Настройка BPDU Terminal

По умолчанию коммутатор пересылает полученный BPDU, когда связующее дерево не работает. Функция BPDU Terminal может отключить пересылку BPDU, если связующее дерево не запущено.

Используйте следующие команды для включения функции BPDU Terminal в режиме глобальной конфигурации:

Команда	Описание
spanning-tree bpdu-terminal	Включение BPDU Terminal
no spanning-tree bpdu-terminal	Отключение BPDU Terminal

26. Агрегация портов

26.1 Обзор

Агрегация портов означает, что несколько физических портов с одинаковыми атрибутами объединяются, образуя логический канал. Метод агрегации портов может заключаться в статическом агрегировании нескольких физических портов независимо от того, соответствуют ли порты, подключенные к этим физическим портам, условиям агрегации. При использовании LACP (Link Aggregation Control Protocol) для агрегации, после того как порт обменяется соответствующей информацией с противоположным портом, он может быть агрегирован в логический канал.

Поддерживаемые функции

- Статическое управление агрегацией портов:

  возможность связывания физического порта с логическим портом независимо от того, могут ли они фактически связаться с логическим портом.

- Управление агрегацией с динамическим согласованием LACP:

  когда физический порт настроен на связывание с логическим портом, физический порт с LACP-согласованием может быть привязан к логическому порту. Другие порты не могут быть связаны с логическим портом.

- Балансировка потоков данных агрегированных портов:

  после агрегации портов данные потока агрегированного порта будут распределены на каждый агрегированный физический порт.

26.2 Настройка агрегации портов

Задачи настройки

- Настройка логического канала, используемого для агрегации
- Агрегация физических портов
- Выбор режима балансировки нагрузки агрегированных портов
- Отслеживание состояния агрегации портов

26.2.1 Настройка логического канала, используемого для агрегации

Прежде чем связывать все физические порты вместе, вам следует настроить логический порт. Логический порт используется для управления каналом, образованным этими связанными физическими портами.

Используйте следующую команду для настройки логического канала:

Команда	Описание
interface port-aggregator id	Создает логический канал агрегации

26.2.2 Агрегация физических портов

Чтобы объединить несколько физических портов в логический канал, вы можете использовать для согласования статическую агрегацию или протокол LACP.

В случае использования статической агрегации требуется, чтобы физический порт был активен и атрибуты VLAN на агрегированном порту и физическом порту совпадали. Только после этого порт будет объединен в логический канал, независимо от того, соответствует ли текущий порт условиям агрегации и соответствует ли порт, который связан с физическим портом, условиям агрегации.

При использовании протокола LACP агрегирование портов должно выполняться после того, как одноранговый узел подключился к порту и порт был согласован. Соединение порта должно быть установлено, и порт должен быть переведен в полнодуплексный режим. Скорость всех физических портов должна быть одинаковой во время процесса агрегации, то есть, если уже есть один успешно агрегированный физический порт с определенной скоростью передачи, то скорость второго физического порта должна быть такой же. Кроме того, атрибуты VLAN всех физических портов должны быть идентичны агрегированному порту.

LACP предоставляет два метода агрегирования: активный и пассивный. В активном режиме порт сам инициирует процесс согласования агрегации, а в пассивном – только принимает процесс согласования. Если оба порта используют пассивный метод, агрегация не произойдет. Это связано с тем, что обе стороны будут ждать, пока другая сторона начнет процесс переговоров по агрегированию.

Атрибуты VALN: PVID, транк, разрешенный диапазон VLAN и диапазон VLAN для пересылки нетегированных фреймов.

Используйте следующую команду для выполнения агрегации физических портов:

Команда	Описание
aggregator-group *agg-id* **mode** {**lacp** | **static**}	Настраивает опции агрегации физического порта

26.2.3 Выбор режима балансировки нагрузки агрегированных портов

Вы можете выбрать метод распределения нагрузки, чтобы все порты могли совместно использовать трафик данных после агрегирования. Коммутатор может обеспечить до шести стратегий балансировки нагрузки:

- src-mac

Совместное использование трафика данных в соответствии с MAC-адресом источника, то есть сообщение с одинаковыми атрибутами MAC-адреса должно пройти через физический порт.

- dst-mac

  Совместное использование трафика данных в соответствии с MAC-адресом назначения, то есть сообщение с одинаковыми атрибутами MAC-адреса должно пройти через физический порт.

- both-mac

  Разделение трафика данных в соответствии с MAC-адресами источника и назначения, то есть сообщение с одинаковыми атрибутами MAC-адреса должно пройти через физический порт.

- src-ip

  Разделение трафика данных в соответствии с исходным IP-адресом, то есть сообщение с одинаковыми атрибутами IP-адреса должно пройти через физический порт.

- dst-ip

  Разделение трафика данных в соответствии с IP-адресом назначения, то есть сообщение с одинаковыми атрибутами IP-адреса должно пройти через физический порт.

- both-ip

  Разделение трафика данных в соответствии с IP-адресами назначения и источника, то есть сообщение с одинаковыми атрибутами IP-адреса должно пройти через физический порт.

Используйте следующую команду для настройки метода балансировки нагрузки

Команда	Описание
aggregator-group load-balance	Настраивает метод распределения нагрузки

26.2.4 Отслеживание состояния агрегации портов

Используйте следующую команду для мониторинга состояния агрегации портов в режиме EXEC:

Команда	Описание
show aggregator-group [id] {**detail** | **brief** | **summary**}	Отображает состояния агрегации портов

27. Настройка PDP

27.1 Введение

PDP – протокол, который используется для обнаружения сетевого оборудования, то есть для поиска всех соседей определенного устройства. С его помощью программы управления сетью могут использовать SNMP для запроса данных у соседних устройств и получения информации о топологии сети.

Коммутаторы данной серии могут обнаруживать соседние устройства, но не принимают запросы SNMP. Таким образом, коммутаторы работают только на периферии сети или не могут получить полную сетевую топологию.

Задачи настройки PDP

- Конфигурация PDP по умолчанию
- Настройка частоты PDP и времени хранения информации
- Установка версии PDP
- Запуск PDP на коммутаторе
- Запуск PDP на порту
- Мониторинг и управление PDP

27.2 Конфигурация PDP по умолчанию

Функция	Настройки по умолчанию
Режим глобальной конфигурации	Выключено
Режим настройки интерфейса	Запускается
Тактовая частота PDP (частота передачи пакетов)	60 секунд
Хранение информации PDP	180 секунд
PDP-версия	2

27.3 Настройка частоты PDP и времени хранения информации

Чтобы установить частоту передачи пакетов PDP и время хранения информации PDP, вы можете выполнить следующие команды в режиме глобальной конфигурации:

Команда	Описание
pdp timer *seconds*	Устанавливает частоту передачи пакетов PDP
pdp holdtime *seconds*	Устанавливает время хранения информации PDP

27.4 Установка версии PDP

Чтобы установить версию PDP, вы можете запустить следующую команду в режиме глобальной конфигурации:

Команда	Описание
pdp version {**1**|**2**}	Устанавливает версию PDP

27.5 Запуск PDP на коммутаторе

Чтобы включить PDP, вы можете запустить следующую команду в режиме глобальной конфигурации:

Команда	Описание
pdp run	Включает PDP на коммутаторе

27.6 Запуск PDP на порту

Чтобы включить PDP на порту, вы можете запустить следующую команду в режиме настройки интерфейса:

Команда	Описание
pdp enable	Запускает PDP на порту коммутатора

27.7 Мониторинг и управление PDP

Для мониторинга PDP выполните следующие команды в режиме EXEC:

Команда	Описание
show pdp traffic	Отображает количество полученных и переданных пакетов PDP
show pdp neighbor [**detail**]	Отображает соседние устройства, которые обнаруживает PDP

27.8 Примеры настройки PDP

- Пример 1. Запуск PDP

  Switch_config# pdp run

  Switch_config# int g0/1

  Switch_config_g0/1#pdp enable

- Пример 2. Настройка частоты PDP и времени хранения информации

  Switch_config# pdp timer 30

  Switch_config# pdp holdtime 90

- Пример 3. Установка версии PDP

  Switch_config# pdp version 1

- Пример 4. Мониторинг PDP

  Switch_config# show pdp neighbor

  Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

  S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID	Local-Intf	Hldtme	Port-ID	Platform	Capability
Switch	Gig0/1	169	Gig0/1	COM, RISC	R S

28. LLDP

28.1 Обзор

Протокол обнаружения канального уровня (LLDP) 802.1AB помогает легко обнаруживать проблемы в сети и поддерживать ее топологию. Это позволяет соседним устройствам отправлять друг другу уведомления о своем состоянии. Каждый порт всех устройств хранит свою собственную определенную информацию. При необходимости порт может отправлять обновленную информацию на соседние, напрямую подключенные устройства. Устройство будет хранить информацию в стандартных MIB SNMP. Система управления сетью может запросить текущий статус соединения второго уровня из MIB. LLDP не настраивает и не контролирует сетевые элементы или трафик, он просто сообщает о конфигурации второго уровня.

Проще говоря, LLDP – это протокол обнаружения соседей. Он устанавливает стандартный метод передачи данных о конфигурации для сетевых устройств Ethernet, таких как коммутаторы, маршрутизаторы и точки доступа WAP. Это позволяет устройству Ethernet уведомлять о своем существовании другие узлы и сохранять информацию об обнаружении соседних устройств. Например, вся информация, включая конфигурацию и идентификацию устройства, может быть передана через протокол. В частности, LLDP определяет универсальный комплект информации для уведомлений, протокол отправки уведомлений и способ хранения всей информации, относящейся к уведомлениям. Устройство отправляет информацию, передавая множество уведомлений в одном пакете данных локальной сети. Формат передачи данных основан на структуре «тип-длина-значение» (TLV).

TLV имеет три обязательных типа: TLV идентификатора шасси, TLV идентификатора порта и TLV времени жизни.

Пять дополнительных типов: описание порта, имя системы, описание системы, возможности системы и адрес управления.

Три TLV расширения: DOT1 (идентификатор Vlan порта, идентификатор Vlan протокола, имя Vlan, идентификатор протокола); DOT3 (конфигурация/состояние MAC/PHY, питание через MDI, агрегация каналов, максимальный размер кадра); MED (возможности MED, сетевая политика, идентификация местоположения, расширенное питание через MDI, инвентаризация (версия аппаратного обеспечения, версия встроенного ПО, версия программного обеспечения, серийный номер, имя производителя, имя режима, идентификатор подтверждения).

LLDP – это однонаправленный протокол. Один агент LLDP передает информацию о своем состоянии и функциях через подключенный MSAP или получает информацию о текущем состоянии или информацию о функциях соседа. Однако агент LLDP не может запрашивать какую-либо информацию от партнера через протокол. Во время обмена сообщениями передача и прием сообщений не влияют друг на друга. Вы можете настроить только передачу или прием сообщений, или и то, и другое.

28.1.1 Инициализация протокола

LLDP может работать в трех режимах: только передача (transmit-only), только прием (receive-only) и передача и прием (transmit-and-receive). По умолчанию используется режим передачи и приема.

28.1.2 Инициализация режима передачи LLDP

Установите LLDP только на передачу в режиме настройки интерфейса. В режиме передачи интерфейс передает пакеты LLDP, когда состояние или значение одного или нескольких информационных элементов (объектов управления) локальной системы изменяются или истекает время таймера передачи. Интерфейс не будет передавать пакеты LLDP при отключении этой функции.

28.1.3 Инициализация режима приема LLDP

Установите LLDP только на прием в режиме настройки интерфейса. В режиме приема интерфейс может получать пакеты LLDP от соседей и сохранять TLV в удаленной MIB. Интерфейс будет отбрасывать пакеты LLDP при отключении этой функции.

28.1.4 Описание структуры пакета LLDP PDU

В соответствии с правилами, PDU LLDP включает три обязательных TLV в начале, один или несколько необязательных TLV в середине и обязательный TLV LLDPUD в конце, как показано в таблице 28-1.

Таблица 28-1 – Формат LLDP PDU

TLV ID шасси	TLV ID порта	TLV времени жизни	Дополнительный TLV	…	Дополнительный TLV	TLV окончания сообщения

- Три обязательных TLV должны быть перечислены последовательно в начале PDU LLDP:
  1. TLV идентификатора шасси
  2. TLV идентификатора порта
  3. TLV времени жизни
- Дополнительный TLV, выбранный управлением сети, может быть указан в случайном порядке.
  4. Описание порта
  5. Имя системы
  6. Описание системы
  7. Возможности системы
  8. Адрес управления

Три расширения (включая DOT1):

9. Идентификатор порта VLAN
10. Идентификатор протокола VLAN
11. Имя VLAN
12. Идентификация протокола

DOT3:

13. Конфигурация/статус MAC/PHY
14. Питание через MDI
15. Агрегация каналов
16. Максимальный размер кадра

MED (TLV MED не передается по умолчанию. Пакеты LLDP с MED TLV будут передаваться только при получении пакетов LLDP с MED TLV)

17. Возможности MED (TLV является обязательным, если добавляется MED TLV).
18. Сетевая политика
19. Идентификация местоположения
20. Дополнительное питание через MDI
21. Инвентаризация (включая версию аппаратного обеспечения, версию встроенного ПО, версию программного обеспечения, серийный номер, имя производителя, имя режима или идентификатор подтверждения)

- TLV окончания сообщения; должен быть последним в PDU LLDP.

28.2 Настройка LLDP

Задачи настройки

- Отключение/включение LLDP
- Настройка времени удержания
- Настройка таймера
- Настройка реинициализации
- Настройка TLV для отправки
- Настройка режима передачи или приема
- Указание IP-адреса управления порта
- Отправка trap-уведомлений в базу данных MIB
- Настройка информации о местонахождении
- Отображение информации LLDP
- Удаление информации LLDP

28.2.1 Отключение/включение LLDP

Когда LLDP включен, локальный порт периодически отправляет кадр LLDP, чтобы сообщить противоположной стороне информацию о локальном порте.

Запустите следующую команду в режиме глобальной конфигурации, чтобы включить LLDP:

Команда	Описание
config	Вход в режим глобальной конфигурации
lldp run	Включает LLDP

Выполните следующую команду, чтобы отключить LLDP:

Команда	Описание
config	Вход в режим глобальной конфигурации
no lldp run	Выключает LLDP

Только когда функция LLDP включена, полученное сообщение LLDP может быть обработано, в противном случае кадр LLDP будет перенаправлен напрямую.

28.2.2 Настройка времени удержания

Обычно удаленная информация, хранящаяся в MIB, обновляется до устаревания. Но она также может устаревать из-за потери кадра обновления в процессе отправки. Чтобы предотвратить это, рекомендуется настроить значение TTL так, чтобы кадры обновления LLDP отправлялись несколько раз в течение времени устаревания. Вы можете контролировать время ожидания передачи сообщения LLDP, изменяя время удержания:

Запустите следующую команду в режиме глобальной конфигурации, чтобы настроить время удержания:

Команда	Описание
config	Вход в режим глобальной конфигурации
lldp holdtime time	Настраивает время ожидания LLDP. Диапазон: от 0 до 65535, по умолчанию 120 с

Выполните следующую команду, чтобы восстановить значение тайм-аута по умолчанию

Команда	Описание
config	Вход в режим глобальной конфигурации
no lldp holdtime	Восстанавливает время ожидания по умолчанию, то есть 120 с

Чтобы гарантировать, что информация о соседе не будет потеряна из-за устаревания при приеме следующего кадра LLDP, время ожидания должно быть больше, чем интервал передачи пакетов LLDP.

28.2.3 Настройка таймера

Вы можете контролировать интервал передачи сообщений коммутатором, настроив таймер LLDP. Для этого запустите следующую команду в режиме глобальной конфигурации:

Команда	Описание
config	Вход в режим глобальной конфигурации
lldp timer time	Настраивает интервал передачи сообщений LLDP. Значение варьируется от 5 до 65534. Время по умолчанию – 30 с

Выполните следующую команду, чтобы вернуть интервалу значение по умолчанию:

Команда	Описание
config	Вход в режим глобальной конфигурации
no lldp timer	Восстанавливает интервал по умолчанию, то есть 30 с

28.2.4 Настройка реинициализации

Информация LLDP автоматически отправляется при изменении статуса или значения одного или нескольких информационных элементов (управляемых объектов) в локальной системе и при истечении таймера передачи. Поскольку одно изменение информации требует передачи кадров LLDP, непрерывная серия изменений может инициировать передачу множества кадров LLDP, так как в каждом кадре сообщается только об одном изменении. Чтобы избежать этой ситуации, управление сетью определяет время ожидания между двумя последовательными передачами кадров LLDP. Вы можете контролировать интервал непрерывной передачи двух сообщений, настроив повторную инициализацию LLDP.

Запустите следующую команду в режиме глобальной конфигурации, чтобы настроить повторную инициализацию LLDP:

Команда	Описание
config	Вход в режим глобальной конфигурации
lldp reinit time	Устанавливает интервал непрерывной передачи сообщений. Значение варьируется от 2 до 5. Значение интервала по умолчанию составляет 2 с

Выполните эту команду, чтобы возобновить повторную инициализацию по умолчанию:

Команда	Описание
config	Вход в режим глобальной конфигурации
no lldp reinit	Возобновляет интервал непрерывной передачи сообщений по умолчанию (2 с)

28.2.5 Настройка TLV для отправки

Вы можете выбрать TLV, который необходимо отправить, настроив **tlv-select** для LLDP. По умолчанию передаются все TLV.

Выполните следующие команды в режиме глобальной конфигурации, чтобы добавить или удалить TLV LLDP:

Команда	Описание
config	Вход в режим глобальной конфигурации
lldp tlv-select management-address	Необязательно. Передает TLV адреса управления. Адресом управления обычно является IP-адрес 3-го уровня, который должен быть прост в использовании
lldp tlv-select port-description	Необязательно. Передает TLV описания порта. В описании порта используются цифры или буквы
lldp tlv-select system-capabilities	Необязательно. Передает TLV с данными о производительности системы. Производительность системы относится к системе передачи пакетов, такой как коммутатор или маршрутизатор
lldp tlv-select system-description	Необязательно. Передает TLV с описанием системы. Описание системы состоит из текстов, включающих цифры и буквы. Должно включать полное название системы, версию аппаратного обеспечения, описание программного обеспечения и сетевого программного обеспечения
lldp tlv-select system-name	Необязательно. Передает TLV системного имени. Название системы должно совпадать с именем системы управления, т.е. с именем коммутатора

Выполните следующую команду, чтобы удалить подлежащий передаче TLV в режиме глобальной конфигурации:

Команда	Описание
config	Вход в режим глобальной конфигурации
no lldp tlv-select management-address	Необязательно. Передает TLV адреса управления. Адресом управления обычно является IP-адрес 3-го уровня, который должен быть прост в использовании

no lldp tlv-select port-description	Необязательно. Передает TLV описания порта. В описании порта используются цифры или буквы
no lldp tlv-select system-capabilities	Необязательно. Передает TLV с данными о производительности системы. Производительность системы относится к системе передачи пакетов, такой как коммутатор или маршрутизатор
no lldp tlv-select system-description	Необязательно. Передает TLV с описанием системы. Описание системы состоит из текстов, включающих цифры и буквы. Должно включать полное название системы, версию аппаратного обеспечения, описание программного обеспечения и сетевого программного обеспечения
no lldp tlv-select system-name	Необязательно. Передает TLV системного имени. Название системы должно совпадать с именем системы управления, т.е. с именем коммутатора

28.2.6 Указание конфигурации порта и выбор расширенного TLV для отправки

Посредством настройки **dot1-tlv-select** / **dot3-tlv-select** / **med-tlv-select** на порту вы можете выбрать расширенный TLV для отправки. По умолчанию будут передаваться TLV DOT1 и DOT3, тогда как TLV MED передаваться не будет.

Выполните следующие команды в режиме настройки интерфейса, чтобы добавить TLV для отправки:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface intf-type intf-id	Вход в режим настройки интерфейса
lldp dot1-tlv-select port-vlan-id	Необязательно. Отправляет TLV, определенный 802.1, и указывает PVID порта
lldp dot1-tlv-select protocol-vlan-id	Необязательно. Отправляет TLV, определенный 802.1, и указывает PPVID порта
lldp dot1-tlv-select vlan-name	Необязательно. Отправляет TLV, определенный 802.1, и указывает имя VLAN порта
lldp dot3-tlv-select macphy-confg	Необязательно. Отправляет TLV, определенный 802.3:

	а) скорость передачи данных и режим связи (дуплекс) на физическом уровне; б) текущий дуплекс и установленная скорость передачи данных; в) показывает, является ли настройка результатом автосогласования на начальном этапе подключения или принудительно установлена вручную
lldp dot3-tlv-select power	Необязательно. Отправляет TLV, определенный 802.3, и указывает на передачу информации о возможности подключения источника питания к устройству без собственной системы питания через сетевое соединение
lldp dot3-tlv-select link-aggregation	Необязательно. Отправляет TLV, определенный 802.3, и содержащий информацию о возможности агрегации каналов на определенном порту. Это используется для обнаружения возможностей сетевых портов и агрегации их каналов
lldp dot3-tlv-select max-frame-size	Необязательно. Отправляет TLV, определенный стандартом 802.3, и указывает максимальный размер кадра на порту
lldp med-tlv-select network-policy	Необязательно. Отправляет TLV, определенный MED, позволяет передавать дополнительную информацию о настройках VLAN и атрибутах 2-го и 3-го уровня. В результате интерфейс сетевого оборудования может эффективно обнаруживать и диагностировать ошибки, связанные с настройкой VLAN и свойствами соответствующих сетевых слоев
lldp med-tlv-select location	Необязательно. Отправляет TLV, определенный MED, и указывает адрес: а) LCI на основе координат, который определен в IETF 3825[6]; б) LCI городского адреса, определенный в IETF; в) код ELIN службы экстренного вызова
lldp med-tlv-select power-management	Необязательно. Отправляет TLV, определенный MED, и отображает информацию об источнике питания

lldp med-tlv-select inventory	Необязательно. Отправляет TLV, определенный MED, и показывает атрибут детальной инвентаризации
lldp dot1-tlv-select protocol-identity	Необязательно. Отправляет TLV, определенный 802.1, и указывает идентификатор протокола порта

Выполните следующие команды, чтобы удалить TLV, подлежащий отправке:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface intf-type intf-id	Вход в режим настройки интерфейса
no lldp dot1-tlv-select port-vlan-id	Необязательно. Удаляет TLV, определенный 802.1, с указанием PVID порта
no lldp dot1-tlv-select protocol-vlan-id	Необязательно. Удаляет TLV, определенный 802.1, с указанием PPVID порта
no lldp dot1-tlv-select vlan-name	Необязательно. Удаляет TLV, определенный 802.1, с указанием имени VLAN порта
no lldp dot3-tlv-select macphy-confg	Необязательно. Удаляет TLV, определенный 802.3: а) скорость передачи данных и режим связи (дуплекс) на физическом уровне; б) текущий дуплекс и установленная скорость передачи данных; в) указание, является ли настройка результатом автосогласования на начальном этапе подключения или принудительно установлена вручную
no lldp dot3-tlv-select power	Необязательно. Удаляет TLV, определенный 802.3, с указанием на передачу информации о возможности подключения источника питания к устройству без собственной системы питания через сетевое соединение
no lldp dot3-tlv-select link-aggregation	Необязательно. Удаляет TLV, определенный 802.3, и содержащий информацию о возможности агрегации каналов на определенном порту. Это используется для обнаружения возможностей сетевых портов и агрегации их каналов
no lldp dot3-tlv-select max-frame-size	Необязательно. Удаляет TLV, определенный стандартом 802.3, с указанием максимального размера кадра на порту

no lldp med-tlv-select network-policy	Необязательно. Удаляет TLV, определенный MED, позволяющий передавать дополнительную информацию о настройках VLAN и атрибутах 2-го и 3-го уровня
no lldp med-tlv-select location	Необязательно. Удаляет TLV, определенный MED, с указанием адреса: а) LCI на основе координат, который определен в IETF 3825[6]; б) LCI городского адреса, определенный в IETF; в) код ELIN службы экстренного вызова
no lldp med-tlv-select power-management	Необязательно. Удаляет TLV, определенный MED, с отображением информации об источнике питания
no lldp med-tlv-select inventory	Необязательно. Удаляет TLV, определенный MED, отображающий атрибут детальной инвентаризации
no lldp dot1-tlv-select protocol-identity	Необязательно. Удаляет TLV, определенный 802.1, с указанием идентификатора протокола порта

28.2.7 Настройка режима передачи или приема

LLDP может работать в трех режимах: только передача, только прием, передача и прием.

По умолчанию LLDP работает в режиме передачи и приема. Вы можете изменить рабочий режим LLDP с помощью следующих команд:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface intf-type intf-id	Вход в режим настройки интерфейса
no lldp transmit	Отключает для порта режим только передачи
no lldp receive	Отключает для порта режим только приема

Выполните следующие команды в режиме настройки интерфейса и установите LLDP в режим передачи и приема:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface intf-type intf-id	Вход в режим настройки интерфейса
lldp transmit	Включает режим передачи порта
lldp receive	Включает режим приема порта

Помимо вышеуказанного режима, интерфейс также можно настроить на режим только передачи или режим только приема.

28.2.8 Указание IP-адреса управления порта

В режиме настройки интерфейса вы можете произвольно настроить адрес управления порта, с которого передаются пакеты LLDP. Адрес управления должен быть IP-адресом, связанным с этим портом, и только таким образом можно гарантировать для этого порта нормальное соединение.

Выполните следующие команды в режиме настройки интерфейса, чтобы установить IP-адрес управления:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface intf-type intf-id	Вход в режим настройки интерфейса
lldp management-ip A.B.C.D	Устанавливает IP-адрес управления порта

Как команду **no lldp**, так и команду **management-ip** можно использовать для восстановления адреса управления порта по умолчанию. Адрес управления по умолчанию – это IP-адрес интерфейса VLAN, который соответствует PVID. Если соответствующий интерфейс VLAN не существует, адрес управления – 0.0.0.0.

28.2.9 Отправка trap-уведомлений в базу данных MIB

Выполните следующие команды в режиме глобальной конфигурации, чтобы отправить trap-уведомление в базу данных LLDP MIB или PTOPO MIB.

Команда	Описание
config	Вход в режим глобальной конфигурации
lldp trap-send lldp-mib	Отправляет trap-уведомление в базу данных LLDP MIB
lldp trap-send ptopo-mib	Отправляет trap-уведомление в базу данных PTOPO MIB

28.2.10 Настройка информации о местоположении

Конфигурация местоположения используется для определения адреса локального компьютера.

Выполните следующие команды в режиме глобальной конфигурации, чтобы настроить информацию о местоположении:

Команда	Описание
config	Вход в режим глобальной конфигурации
location elin identifier *id WORD*	Указывает информацию о местоположении ELIN, где id – это номер идентификатора ELIN, а WORD обозначает информацию ELIN, размер которой варьируется от 10 до 25 байт
location civic identifier *id*	Вход в режим настройки местоположения
language *WORD*	Указывает язык
state *WORD*	Указывает название региона
county *WORD*	Указывает название округа
city *WORD*	Указывает название города
division *WORD*	Указывает имя области
neighborhood *WORD*	Указывает название района
street *WORD*	Указывает название улицы
leading-street-dir *WORD*	Указывает направление главной улицы, например, N (север)
trailing-street-suffix *WORD*	Указывает суффикс переулка
street-suffix *WORD*	Указывает суффикс улицы или площади
number *WORD*	Указывает номер улицы
street-number-suffix *WORD*	Указывает суффикс номера улицы, например, номер 1/2 дороги A
landmark *WORD*	Указывает ориентир, например, Исторический музей
additional-location *WORD*	Указывает дополнительную информацию о местоположении
name *WORD*	Указывает информацию о контактном лице
postal-code *WORD*	Указывает почтовый индекс
building *WORD*	Указывает информацию о здании
unit *WORD*	Указывает информацию об объекте
floor *WORD*	Указывает информацию об этаже
room *WORD*	Указывает информацию о помещении
type-of-place *WORD*	Указывает тип места, например, офис
postal-community *WORD*	Указывает название почтового отделения
post-office-box *WORD*	Указывает номер почтового ящика, например, 12345
additional-code *WORD*	Указывает дополнительный код
country *WORD*	Указывает название страны
script *WORD*	Указывает сценарий

Выполните следующие команды в режиме глобальной конфигурации, чтобы удалить информацию о местоположении:

Команда	Описание
config	Вход в режим глобальной конфигурации
no location elin identifier *id*	Удаляет информацию ELIN ID
location civic identifier *id*	Вход в режим настройки местоположения
no language	Удаляет язык
no state	Удаляет название региона
no county	Удаляет название округа
no city	Удаляет название города
no division	Удаляет имя области
no neighborhood	Удаляет название района
no street	Удаляет название улицы
no leading-street-dir	Удаляет направление главной улицы, например, N (север)
no trailing-street-suffix	Удаляет суффикс переулка
no street-suffix	Удаляет суффикс улицы или площади
no number	Удаляет номер улицы
no street-number-suffix	Удаляет суффикс номера улицы, например, номер 1/2 дороги A
no landmark	Удаляет ориентир, например, Исторический музей
no additional-location	Удаляет дополнительную информацию о местоположении
no name	Удаляет информацию о контактном лице
no postal-code	Удаляет почтовый индекс
no building	Удаляет информацию о здании
no unit	Удаляет информацию об объекте
no floor	Удаляет информацию об этаже
no room	Удаляет информацию о помещении
no type-of-place	Удаляет тип места, например, офис
no postal-community	Удаляет название почтового отделения
no post-office-box	Удаляет номер почтового ящика, например, 12345
no additional-code	Удаляет дополнительный код
no country	Удаляет название страны
no script	Удаляет сценарий

28.2.11 Указание порта для отправки информации о местоположении

Следующие команды можно использовать чтобы настроить порт для работы с информацией о местоположении и ее передачи в TLV.

Выполните следующие команды в режиме настройки интерфейса, чтобы настроить информацию о местоположении:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface *intf-type intf-id*	Вход в режим настройки интерфейса
location civic *id*	Указывает civic ID
location elin *id*	Указывает ELIN ID

Чтобы удалить из настроек порта информацию о местоположении, выполните следующие команды:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface *intf-type intf-id*	Вход в режим настройки интерфейса
no location civic	Удаляет civic ID
no location elin	Удаляет ELIN ID

28.2.12 Отображение информации LLDP

Вы можете просмотреть информацию о соседнем устройстве, статистике или состоянии порта, полученную модулем LLDP, с помощью команд **show**.

Выполните следующие команды в режиме EXEC или глобальной конфигурации:

Команда	Описание
show lldp errors	Отображает информацию об ошибках модуля LLDP
show lldp interface *interface-name*	Отображает информацию о состоянии порта, то есть режиме передачи и режиме приема
show lldp neighbors	Отображает общую информацию о соседе
show lldp neighbors detail	Отображает детальную информацию о соседе
show lldp traffic	Отображает всю полученную и переданную статистическую информацию
show location elin	Отображает информацию ELIN
show location civic	Отображает подробную информацию о местоположении

28.2.13 Удаление информации LLDP

Вы можете удалить полученные списки соседних устройств и всю статистическую информацию, выполнив следующие команды в режиме EXEC:

Команда	Описание
clear lldp counters	Удаляет все статистические данные
clear lldp table	Удаляет всю полученную информацию о соседних устройствах

28.3 Примеры настройки

Настройте протокол LLDP на порту, соединяющем два коммутатора (см. рисунок 28-1).

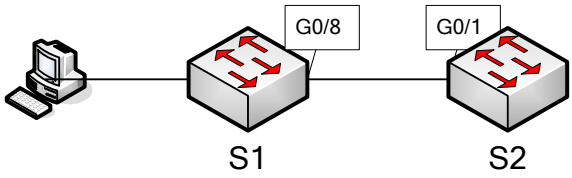

Рисунок 28-1 – Топология сети

28.3.1 Базовая настройка

Настройка коммутатора S1:

```
Switch_config# lldp run
Switch_config#
```

Настройка коммутатора S2:

```
Switch_config# lldp run
Switch_config#
```

Информация о соседнем устройстве отобразится на коммутаторе примерно через 1 минуту. Информация MED-TLV не отправляется по умолчанию.

S1:

```
Switch_config# show lldp neighbors
Capability Codes:
    (R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone
    (W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID      Local-Intf     Hldtme      Port-ID      Capability
Switch         Gig0/8         99          Gig0/1       B

Total entries displayed: 1
```

Switch_config# show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: Switch

system description: SWITCH Software, Version 4.1.0B

Serial: S24090103

Compiled: 2023-9-21 9:24:8 by WRL

Time remaining: 96

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID: 1

PPVID: 1

VLAN 1 name: Default

Auto Negotiation: supported, enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

Link Aggregation:

Aggregation capability: capable of being aggregated

Aggregation status: not currently in aggregation

Maximum frame size: 1500

Total entries displayed: 1

28.3.2 Настройка TLV

Настройка коммутатора S1:

Switch_config# lldp run

Switch_config#

Настройка коммутатора S2:

Switch_config# lldp run

Switch_config# no lldp tlv-select system-name

Switch_config# interface g0/8

Switch_config_g0/8#no lldp dot1-tlv-select port-vlan-id

Switch_config_g0/8#no lldp dot3-tlv-select max-frame-size

Switch_config_g0/8#

Информация о соседнем устройстве отобразится на коммутаторе примерно через 1 минуту.

S1:

Switch_config# show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
Switch	Gas0/8	92	Gig0/1	R B

Total entries displayed: 1

Switch_config# show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: -- not advertised

system description: SWITCH Software, Version 4.1.0B

Serial: S24090103

Compiled: 2023-9-21 9:24:8 by WRL

Time remaining: 95

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID -- not advertised

PPVID: 1

VLAN 1 name: Default

Auto Negotiation: supported, enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

Link Aggregation:

Aggregation capability: capable of being aggregated

Aggregation status: not currently in aggregation

Total entries displayed: 1

28.3.3 Настройка локации

Настройка коммутатора S1:

Switch_config# lldp run

Switch_config#

Настройка коммутатора S2:

Switch_config# lldp run

Switch_config# location elin identifier 1 1234567890 // Configure elin information

Switch_config# location civic identifier 1 // Enter location configuration mode

Switch_config_civic# language English

Switch_config_civic# city Gorod

Switch_config_civic# street Ulitsa

Switch_config_civic# script EN // Above configuring civic information

Switch_config_civic# quit

Switch_config# interface g0/8

Switch_config_g0/8# location elin 1 //Specify elin id for the port

Switch_config_g0/8# location civic 1 // Specify civic id for the port

Switch_config_g0/8# show location elin //Display elin configuration information

elin information:

elin 1: 1234567890

total: 1

Switch_config_g0/8# show location civic // Display civic configuration information

civic address information:

identifier: 1

City: Gorod

Language: English

Script: EN

Street: Ulitsa

---

total: 1

Switch_config_g0/8#

Информация о соседнем устройстве отобразится на коммутаторе примерно через 1 минуту.

S1:

Switch_config# show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID Local-Intf Hldtme Port-ID Capability

Switch Gig0/8 115 Gig0/1 B

Total entries displayed: 1

Switch_config# show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: Switch

system description: SWITCH Software, Version 4.1.0B

Serial: S24090103

Compiled: 2023-9-21 9:24:8 by WRL

Time remaining: 109

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID: 1

Auto Negotiation: supported, enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

MED Information:

MED Codes:

(CA)Capabilities, (NP)Network Policy, (LI)Location Identification

(PS)Power via MDI ¨CPSE, (PD)Power via MDI ¨CPD, (IN)Inventory

Hardware Revision: 0.4.0

Software Revision: 4.1.0B

Serial Number: S24090103

Manufacturer Name:

Model Name: SWITCH

Asset ID: S24090103

Capabilities: CA,NP,LI,PS,IN

Device type: Network Connectivity

Network Policy: Voice

Policy: Unknown

Power requirements:

Type: PSE Device

Source: Unknown

Priority: Low

Value: 150(0.1 Watts)

Civic address location:

Language: English

City: Gorod

Street: Ulitsa

Script: EN

ELIN location:

ELIN: 1234567890

Total entries displayed: 1

Switch_config#

29. Резервное соединение

29.1 Обзор

Двойное подключение (dual-uplink) – это распространённый подход в сетевых технологиях. В примере ниже (см. рисунок 29-1) коммутатор A подключен к коммутатору D двумя линиями через коммутаторы B и C. Таким образом, коммутатор A имеет два пути для обращения к коммутатору D, обеспечивая избыточность и повышенную надежность подключения.

Рисунок 29-1 – Сеть с резервным каналом

Хотя сеть с двойным восходящим каналом может обеспечить резервное соединение, петли в сети вызовут широковещательные штормы. Поэтому необходимо принять меры, чтобы избежать петель. В большинстве случаев петли можно устранить с помощью STP; но поскольку конвергенция STP занимает много времени, часть трафика будет потеряна.

Таким образом, STP неприменим к сетевой среде с более высокими требованиями ко времени конвергенции.

Технология резервного канала BackupLink обеспечивает резервирование линий связи через пару интерфейсов на канальном уровне и решает проблему медленной сходимости протокола STP. В одной группе портов BackupLink, один порт настраивается как основной, а другой – как альтернативный. Они могут быть портами обмена или портами агрегации. Если пользователь не использует протокол STP, BackupLink обеспечивает избыточность и резервирование каналов связи.

29.2 Резервирование портов BackupLink

29.2.1 Настройка резервного порта

Основная функция BackupLink – настроить для указанного порта коммутатора другой порт в качестве резервного. Среди этих двух портов одновременно только один может находиться в состоянии пересылки. Оба порта могут быть подключены к одному и тому же устройству или к разным.

- Два порта, которые дублируют друг друга, могут быть двумя физическими портами, двумя агрегированными портами или одним физическим и одним агрегированным портом.
- Резервный порт нельзя настраивать на тех портах, которые уже настроены с применением объединения каналов, безопасности портов или EAPS, а также других методов защиты в сети.
- Если для одного порта уже настроен резервный режим, он больше не может стать резервным для других портов.
- Порт, настроенный как резервный, нельзя использовать для объединения каналов, безопасности портов или EAPS, а также других методов сетевой защиты.
- На порту, настроенном с помощью BackupLink, можно включить оптимизацию определения состояния канала на физическом уровне, чтобы повысить эффективность сетевого схождения при изменении состояния соединений в сети.

29.2.2 Контроль состояния порта

Порты, настроенные в качестве резервных, должны быть удалены из модуля STP; BackupLink отвечает за установку статуса порта во всех VLAN [1-4094]; эти VLAN могут принадлежать разным MST (STG).

29.2.3 Роли и статус порта

Команды настройки должны иметь возможность указать роль по умолчанию для двух портов, которые дублируют друг друга: активный и резервный.

- В исходном случае, если статус связи активного и резервного портов – linkup, активный порт находится в состоянии пересылки, резервный – в состоянии блокировки.
- В исходном случае, если статус одного из портов linkdown, другой порт переходит в состояние пересылки независимо от того, выступает ли он изначально в роли активного.
- В момент, когда резервный порт находится в состоянии пересылки, активный порт находится в состоянии блокировки. Однако, если дважды применяется конфигурация резервного порта на один и тот же порт, могут возникнуть непредвиденные изменения в статусах портов. В результате, важно принудительно вернуть резервный порт в состояние блокировки, а активный – в состояние пересылки.

29.2.4 Обработка изменений статуса портов

В базовых функциях BackupLink изменение состояния связи в зависимости от статуса портов должно соответствовать следующим требованиям:

- если активный и резервный порты находятся в состоянии linkdown, соединение разрывается, что приводит к невозможности пересылки кадра данных;
- если активный порт находится в состоянии linkdown, а резервный порт – в состоянии linkup, но не в состоянии пересылки, резервный порт переходит в состояние пересылки;
- если активный порт находится в состоянии linkup, а резервный порт – в состоянии linkdown, активный порт переходит в состояние пересылки;
- если активный порт находится в состоянии linkup, а резервный порт – в состоянии linkup и в состоянии пересылки, активный порт продолжает находиться в состоянии блокировки, и кадр данных пересылается через резервный порт без активации режима приоритетного переключения;
- если активный порт находится в состоянии linkup, а резервный порт – в состоянии linkup и в состоянии пересылки, то в случае работы функции приоритетного переключения портов передающий и заблокированный порты будут определены в соответствии с различными стратегиями (см. раздел «Приоритетное переключение резервных портов»).

29.2.5 Приоритетное переключение резервных портов

В контексте технологии BackupLink, приоритетное переключение портов (port preemption) означает возможность автоматического переключения с активного порта на резервный, когда резервный порт становится более предпочтительным для использования. Это происходит на основе определенных условий или критериев, установленных в системе.

Если имеется два порта (например, A и B) и порт A сейчас активен, а порт B находится в резерве, то переключение портов позволяет автоматически перенаправить канал с порта A на порт B, если порт B становится более подходящим для передачи данных (например, из-за восстановления из состояния linkdown). Это обеспечивает более надежное и эффективное использование портов в сетевых системах с резервированием.

Данная функция должна быть включена с помощью команды; по умолчанию приоритетное переключение отключено.

Приоритетное переключение должно быть настроено независимо для каждой пары резервных портов; разные группы резервных портов могут использовать разные режимы переключения:

- переключение на основе роли порта. Оно основано на ролях, указанных во время настройки резервных портов; если резервный порт находится в состоянии пересылки, а активный порт находится в состоянии linkup, резервный порт блокируется, а активный порт переходит состояние пересылки;
- переключение на основе пропускной способности порта. Резервные порты должны поддерживать приоритетное состояние пересылки в зависимости от пропускной способности; порт с небольшой пропускной способностью всегда блокируется.

Конфигурация переключения для одной и той же группы резервных портов должна соответствовать следующим требованиям:

- Функция переключения вступает в силу после ее настройки на любом порту в группе резервирования; но, если конфигурация группы удалена, функция становится недействительной.
- Функцию переключения можно настроить на двух портах в группе резервирования, но режим переключения и параметры задержки должны быть согласованными.
- Два порта, параметры настройки переключения которых не совпадают, не могут быть настроены в качестве резервных.

29.2.6 Задержка перед переключением портов

Если порт B может заменить порт A, то приоритетное переключение портов происходит не мгновенно, а после определенной задержки – delay-time. Эта задержка перед

переключением должна быть настроена с помощью команды. Значение «0» указывает на мгновенное переключение без задержки.

29.3 Балансировка нагрузки VLAN

Балансировка нагрузки VLAN в резервируемом канале позволяет двум портам из группы портов BackupLink одновременно пересылать трафик в разные VLAN. Например, группа портов BackupLink настроена на пересылку трафика VLAN 1~100, где один порт перенаправляет трафик VLAN1~VLAN50, а другой – VLAN51~VLAN100. Если один порт находится в состоянии linkdown, то весь трафик будет пересылаться на другой порт.

29.3.1 Настройка балансировки нагрузки

Балансировка нагрузки VLAN настраивается только на резервном порту; пользователь указывает набор VLAN с помощью команды, и резервный порт имеет приоритет для перехода в состояние пересылки в этой группе VLAN. Таким образом, разделение трафика VLAN вступает в силу только после настройки функции резервирования на порту.

Разные группы резервных соединений могут быть настроены с использованием одинаковых или пересекающихся сегментов VLAN. Однако, если сегменты VLAN пересекаются, то система назначит им разные деревья MST (STG), и, следовательно, при работе порта в одной из групп это повлияет на состояния порта во всех MST. Поэтому, в целом, при конфигурации группы VLAN для балансировки нагрузки лучше выбирать VLAN, которые не пересекаются, чтобы избежать конфликтов и непредсказуемого поведения.

29.3.2 Контроль статуса порта при разделении трафика

- Создание нового MST (STG) для назначенной VLAN

Чтобы добиться дифференцированной настройки состояния портов в разных VLAN, необходимо назначить VLAN, указанную пользователем в команде управления трафиком, новому MST (STG).

BackupLink должен проверять указанную пользователем VLAN через интерфейс модуля L2; если указанная VLAN уже использовалась другими модулями протокола (например, в MSTP она закреплена за каким-либо MST или настроена как управляющая VLAN EAPS), эта VLAN больше не может использоваться для разделения VLAN-трафика. Такой случай необходимо рассматривать как ошибку конфигурации пользователя.

- Одна и та же VLAN используется несколькими группами резервных портов

BackupLink должен быть способен обрабатывать случай, когда разные группы резервных портов настроены на одну и ту же VLAN. Например, P1 и P2 взаимно резервируются, а разделение трафика VLAN настроено на P2; P3 и P4 взаимно резервируются, а VLAN настроена на P4. В это время:

1. в процессе загрузки конфигурации достаточно произвести операцию распределения MST в VLAN;

2. после удаления настройки разделения трафика VLAN из всех групп резервных портов, VLAN должна вернуться к настройкам MST по умолчанию.

- Обновление статуса порта после создания MST

Модификация MST VLAN может привести к неправильному состоянию некоторых портов в системной таблице STG; в это время:

1. L2 отвечает за уведомление модуля протокола, кроме BackupLink, об обновлении настроек статуса порта;

2. для каждого набора резервных портов модуль BackupLink активно обновляет их статус во всех VLAN.

- Настройка статуса порта

После настройки разделения трафика VLAN настройка статуса резервных портов должна соответствовать следующим правилам:

1. если два порта, которые взаимно резервируются, находятся в состоянии linkdown, их статус во всех VLAN [1-4094] настраивается как «заблокированные»;

2. если только один из двух портов находится в состоянии linkup, то статус этого порта во всех VLAN настраивается как «передающий»;

3. если оба порта находятся в состоянии linkup, порт, выбранный в качестве активного, устанавливается в состояние блокировки в VLAN с разделением трафика и в состояние пересылки в других VLAN; порт, выбранный в качестве резервного, устанавливается в состояние пересылки в VLAN с разделением трафика и в состояние блокировки в других VLAN.

29.4 Устаревание MAC-адреса

Функция BackupLink должна поддерживать уведомления об изменении топологии, чтобы справиться с петлями в сети восходящего канала, как показано ниже:

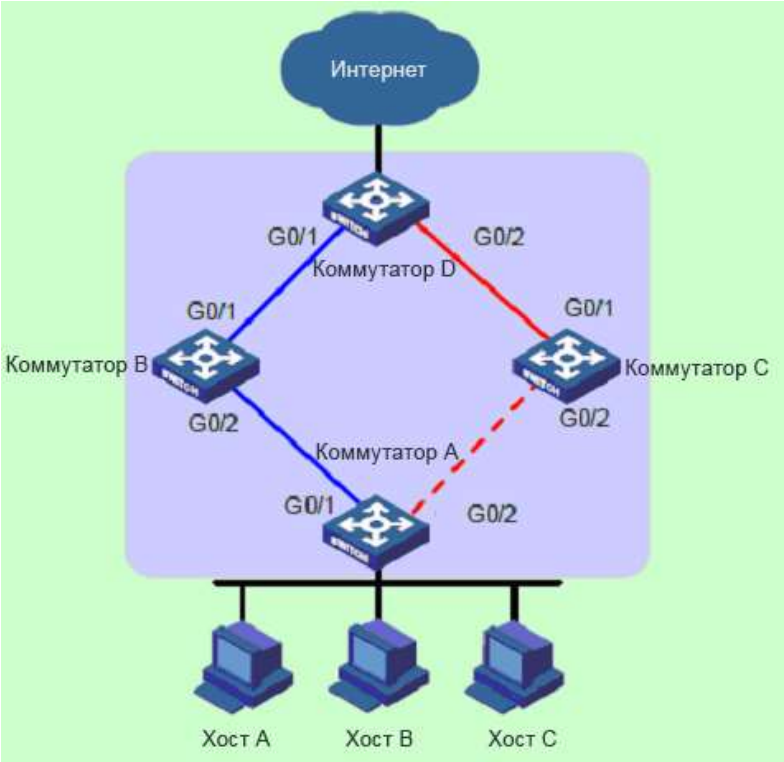

Рисунок 29-2 – BackupLink. Схема механизма устаревания адреса

29.4.1 Нормальный механизм работы канала

Как показано выше, порт коммутатора A G0/1 является основным; порт G0/2 является резервным. Когда двойные восходящие каналы в нормальном рабочем состоянии, основной порт находится в состоянии пересылки, а его канал является основным; вторичный порт заблокирован, и его канал является вторичным. Данные передаются по каналу, обозначенному синей линией; в сети не существует петель, провоцирующих широковещательный шторм.

29.4.2 Механизм обработки неисправностей нисходящей линии связи

При сбое основного канала коммутатора A основной порт G0/1 переключается в состояние ожидания, а вторичный порт G0/2 – в состояние пересылки. В такой ситуации записи таблицы пересылки MAC-адресов и записи таблицы ARP на устройствах в сети могут оказаться некорректными, поэтому необходимо обеспечить механизм обновления MAC-адресов и ARP для завершения быстрого переключения трафика, избегая потери данных. В настоящее время существует два вида механизма обновления.

- Уведомление устройства об обновлении записей таблицы через пакет обновления канала MMU.

Таким образом, вышестоящее устройство, например, коммутатор D, коммутатор B и коммутатор C (см. рисунок 29-2) может поддерживать функцию MMU BackupLink и определять ситуацию с пакетом MMU. Для достижения быстрого переключения каналов необходимо включить функцию отправки пакетов MMU на коммутатор A и функцию приема и обработки пакетов MMU на порту устройства, расположенного выше по топологии в сети с двойным восходящим каналом.

После переключения канала коммутатора A пакет MMU будет отправлен из нового основного канала, то есть из порта G0/2. Когда вышестоящее устройство получает пакет MMU, оно проверяет, допускается ли обработка этого пакета на порту, через который он поступил, в зависимости от того, настроена ли управляющая VLAN этого пакета в списке VLAN, предназначенных для приема на данном порту. Если ее нет в списке, устройство будет напрямую пересылать пакет MMU без обработки; если она находится в списке, устройство извлечет данные VLAN Bitmap из пакета MMU, а записи MAC и ARP, изученные устройством в этих VLAN, будут удалены.

После этого, если коммутатор D получает пакет данных коммутатора A в качестве устройства назначения для пакета, требующего перенаправления 2-го уровня, коммутатор D пересылает его способом широковещательной передачи 2-го уровня; для пакета, требующего пересылки 3-го уровня, устройство сначала обновит записи ARP, используя метод обнаружения ARP, а затем пересылает пакет. Таким образом, трафик данных может передаваться корректно.

- Автоматическое обновление записей через трафик

Этот подход применим к случаю стыковки с устройствами, не поддерживающими BackupLink (включая устройства других производителей), при условии, что инициируется восходящий трафик.

Если нет восходящего трафика от коммутатора A, который мог бы инициировать обновление записей MAC и ARP коммутатора D, когда коммутатор D в качестве устройства назначения получает пакет данных коммутатора A, он все равно пересылает его через порт G0/1; но пакет не может достичь коммутатора A. Трафик прерывается до тех пор, пока записи MAC или ARP не устареют автоматически.

В случае, если коммутатор A имеет восходящий трафик для отправки, поскольку его записи MAC и ARP также неверны, трафик не будет отправляться до тех пор, пока записи автоматически не устареют и таблицы не переобучатся. Когда восходящий трафик дойдет до коммутатора D через порт G0/2, коммутатор D обновит свои собственные записи MAC и ARP; затем, когда коммутатор D в качестве устройства назначения снова получит пакет данных от коммутатора A, он перешлет этот пакет через порт G0/2, и пакет сможет достичь коммутатора A через коммутатор C.

Используя механизм уведомления об обновлениях при помощи пакетов MMU, нет необходимости ждать, пока записи устареют, и время обновления записи может быть значительно сокращено.

29.4.3 Механизм обработки неисправностей восходящей линии связи

В сетевой среде, показанной на рисунке 29-2, функция BackupLink используется для резервирования канала на коммутаторе A; G0/1 – основной порт; G0/2 – вторичный порт. Когда основной канал, идущий через порт G0/1 неисправен, трафик в течение миллисекунд переключается на вторичный канал, идущий через порт G0/2, обеспечивая эффективное надежное резервирование и высокую скорость конвергенции.

Тем не менее, когда происходит сбой на канале, в котором находится порт G0/1 коммутатора B, для коммутатора A, настроенного на использование группы BackupLink, этот канал все еще считается рабочим, поскольку его первичный порт G0/1 имеет нормальную связь с коммутатором B. И коммутатор A не переключается на резервное соединение, хотя фактически трафик уже не может проходить до коммутатора D.

Для решения этой проблемы используется механизм MonitorLink. Этот механизм отслеживает изменения в топологии сети и позволяет переключать соединение на локальном устройстве (коммутатор A) на более надежное резервное соединение в случае сбоя на первичной линии связи. Таким образом, MonitorLink используется для мониторинга связей вверх по иерархии и обеспечения синхронизации между первичным и резервным соединением, улучшая работу механизма BackupLink.

- Знакомство с концепциями MonitorLink

Группа MonitorLink состоит из одного или нескольких портов восходящих и нисходящих линий. Статус порта нисходящей линии меняется в зависимости от изменения статуса порта восходящей линии.

Рисунок 29-3 – Схема группы MonitorLink

Как показано выше, три порта тестируемого устройства (G0/1, G0/2 и G0/3) образуют группу MonitorLink.

Порт восходящей линии связи (Uplink Port) – это отслеживаемый объект в группе MonitorLink, который выполняет групповую роль, указанную через командную строку.

Восходящий порт группы MonitorLink может быть портом Ethernet (электрическим или оптическим) или агрегированным интерфейсом. Как показано на рисунке 29-3, порт G0/1 тестируемого устройства является восходящим портом настроенной на устройстве группы MonitorLink. При выходе из строя восходящего порта группы MonitorLink группа находится в состоянии DOWN, и все нисходящие порты будут закрыты. Если порт восходящей линии связи группы MonitorLink не указан, считается, что порт восходящей линии вышел из строя и все порты нисходящей линии связи будут закрыты.

Порт нисходящей линии связи (Downlink Port) – это монитор в группе MonitorLink, который выполняет еще одну групповую роль, указанную при помощи командной строки. Нисходящим портом также может быть порт Ethernet или агрегированный интерфейс. Как показано на рисунке выше, два порта тестируемого устройства, G0/2 и G0/3, являются двумя нисходящими портами группы MonitorLink, настроенными на устройстве.

- Механизм работы MonitorLink

В сетевой среде, показанной ниже, группа BackupLink настроена на тестируемом устройстве (коммутатор A) для обеспечения надежного доступа к Интернету с хоста. Порт G0/1, находится в состоянии пересылки и является основным портом; G0/2 – это вторичный порт.

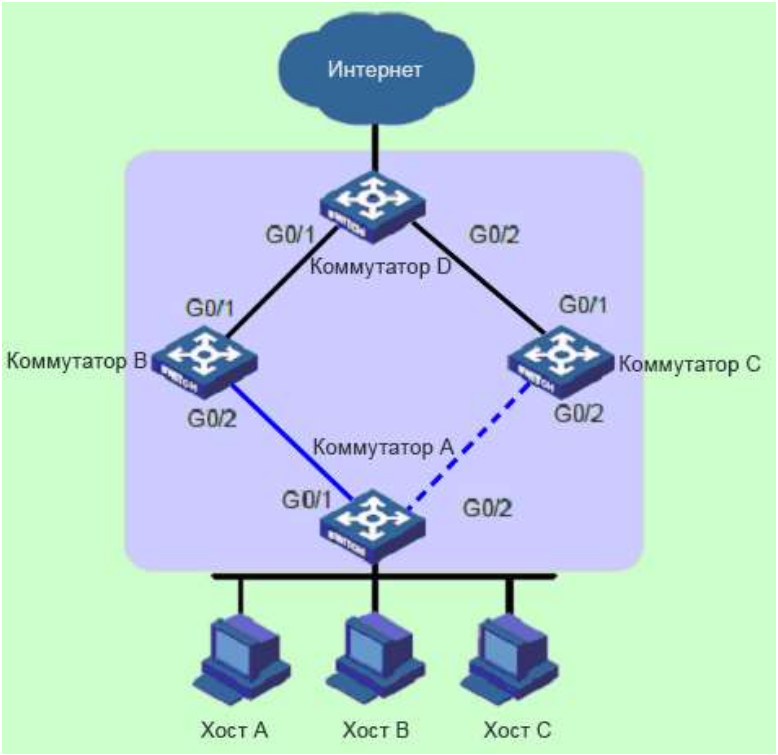

Рисунок 29-4 – Схема механизма работы MonitorLink

Чтобы предотвратить ситуацию, когда трафик тестируемого коммутатора A не может проходить из-за сбоя канала, на котором находится порт коммутатора B G0/1, на коммутаторе B настроена группа MonitorLink. Порт G0/1 указывается как порт восходящей линии связи, а G0/2 – как порт нисходящей линии.

При выходе из строя канала восходящей линии коммутатора B, G0/1, группа MonitorLink принудительно отключит порт нисходящей линии этой группы G0/2, вызывая переключение канала группы BackupLink на тестируемом устройстве.

Когда канал восходящей линии связи коммутатора B, G0/1, восстанавливается после сбоя, порт G0/2 нисходящей линии также будет включен; если группа BackupLink на коммутаторе A настроена в режиме приоритета ролей, в соответствии с ним будет выбран активный порт группы. В противном случае необходимо дождаться следующего переключения канала. Таким образом, сочетание технологии MonitorLink с технологией BackupLink обеспечивает эффективное и надежное резервирование каналов, а также быструю сходимость сетевой топологии.

29.4.4 Механизм обработки восстановления канала связи

Группа BackupLink поддерживает два режима: режим без перехода ролей и режим с переходом ролей. Механизм восстановления связи в разных режимах различен. О режиме без ролевого приоритета см. раздел 29.2.4; о режиме изменения ролей см. раздел 29.2.5.

29.5 Настройка резервного соединения

29.5.1 Рекомендации по настройке BackupLink

Перед настройкой протокола BackupLink прочтите следующие инструкции:

- основной порт (порт Ethernet или агрегированный порт) можно настроить с резервным портом BackupLink. Резервный порт и основной порт не могут быть одним и тем же портом;
- порт может принадлежать только одной группе BackupLink; резервный порт можно использовать только как резервный порт одного основного порта; основной порт определенной группы не может принадлежать другим группам BackupLink;
- ни один порт в группе BackupLink не может быть членом группы агрегации портов. Членами группы BackupLink могут стать агрегированный и физический порт, два физических или два агрегированных порта;
- основной и резервный порт BackupLink могут различаться по типу; это могут быть порты Fast Ethernet, гигабитные порты или агрегированные порты, но оба они должны иметь схожие функции. Таким образом, при выходе из строя основного порта, резервный порт сможет пересылать трафик данных аналогичным образом;
- функции балансировки нагрузки VLAN и переключения портов BackupLink нельзя использовать одновременно.

Задачи настройки BackupLink

- Настройка группы BackupLink
- Настройка приоритетного переключения портов
- Настройка балансировки нагрузки для VLAN
- Настройка функции MMU для группы BackupLink
- Настройка группы MonitorLink

29.5.2 Настройка группы BackupLink

Для настройки группы BackupLink, выполните следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации коммутатора
Switch_config# **backup-link-group** *id*	Настраивает группу BackupLink. *id*: номер экземпляра группы
Switch_config# **interface** *interface-type interface-number*	Вход в режим настройки интерфейса
Switch_config_g1/1# **backup-link-group** *id* **active** [**backup**]	Настраивает роль порта группы BackupLink. *id*: номер экземпляра группы
Switch_config_g1/1# **exit**	Выход из режима настройки интерфейса
Switch_config#	

- Используйте команду **no backup-link-group** *id*, чтобы удалить конфигурацию группы BackupLink и настройки портов группы.
- Если функция BackupLink настраивается непосредственно для порта, без предварительного создания группы в режиме глобальной конфигурации, система создаст группу BackupLink автоматически.

29.5.3 Настройка приоритетного переключения портов

Настройте функцию приоритетного переключения портов для группы BackupLink, выполнив следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **backup-link-group** *id* {**preemption-mode** [**forced** | **bandwidth**] {**delay** *value*}}	Настраивает функцию приоритетного переключения портов для группы BackupLink. *id*: номер экземпляра группы BackupLink; *value*: время задержки
Switch_config#	

Команду **backup-link-group** *id* {**preemption-mode** [**forced** | **bandwidth**] {**delay** *value*}} также можно использовать для непосредственного создания группы BackupLink.

29.5.4 Настройка балансировки нагрузки для VLAN

Настройте балансировку нагрузки для VLAN, выполнив следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **interface** *interface-type interface-number*	Вход в режим настройки интерфейса
Switch_config_g1/2# **share-load vlan** *vlanmap*	Настраивает балансировку нагрузки для VLAN
Switch_config_g1/2# **exit**	Выход из режима настройки интерфейса
Switch_config#	

Порт, настроенный как передающий, должен быть портом группы BackupLink, то есть сначала он должен быть настроен как «активный» или «резервный». В случае настройки порта в качестве принимающего нет необходимости в его специфической конфигурации для BackupLink.

29.5.5 Настройка группы MonitorLink

Настройте группу MonitorLink, выполнив следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации

Switch_config# **monitor-link-group** *id*	Настраивает группу MonitorLink. *id*: номер экземпляра группы MonitorLink
Switch_config# **interface** *interface-type interface-number*	Вход в режим настройки интерфейса
Switch_config_g1/1#**monitor-link-group** *id* **uplink** [**downlink**]	Настраивает роль порта группы MonitorLink. *id*: номер экземпляра группы MonitorLink
Switch_config_g1/1# **exit**	Выход из режима настройки интерфейса
Switch_config#	

- Используйте команду **no monitor-link-group id**, чтобы удалить конфигурацию группы MonitorLink и настройки портов группы.
- Если групповая роль MonitorLink настраивается непосредственно для порта, без предварительного создания группы в режиме глобальной конфигурации, система создаст группу MonitorLink автоматически.

30. Настройка EAPS

30.1 Обзор

Протокол EAPS (Ethernet Automatic Protection Switching) – это особый тип протокола канального уровня, специально разработанный для построения и защиты кольцевой топологии Ethernet. EAPS может отключить один канал в замкнутой кольцевой топологии, предотвращая образование широковещательного шторма из-за сетевой петли. Если кольцо разомкнуто, протокол немедленно возобновляет соединение, которое ранее было закрыто. Таким образом, узлы кольцевой сети могут взаимодействовать друг с другом.

Протоколы EAPS и STP используются для управления топологией на канальном уровне. STP подходит для всех видов сложных сетей, которые передают изменение своей топологии шаг за шагом. Протокол EAPS применяется для кольцевой топологии и использует механизм распространения оповещений для передачи изменений топологии сети. Таким образом, сходимость протокола EAPS в кольцевой сети лучше, чем STP. В хорошо построенной сети EAPS может возобновить сетевое соединение менее чем за 50 мс.

EAPS поддерживает настройку коммутатора в качестве узла нескольких физических колец для построения сложной топологии.

30.2 Основные понятия кольцевого резервирования Ethernet

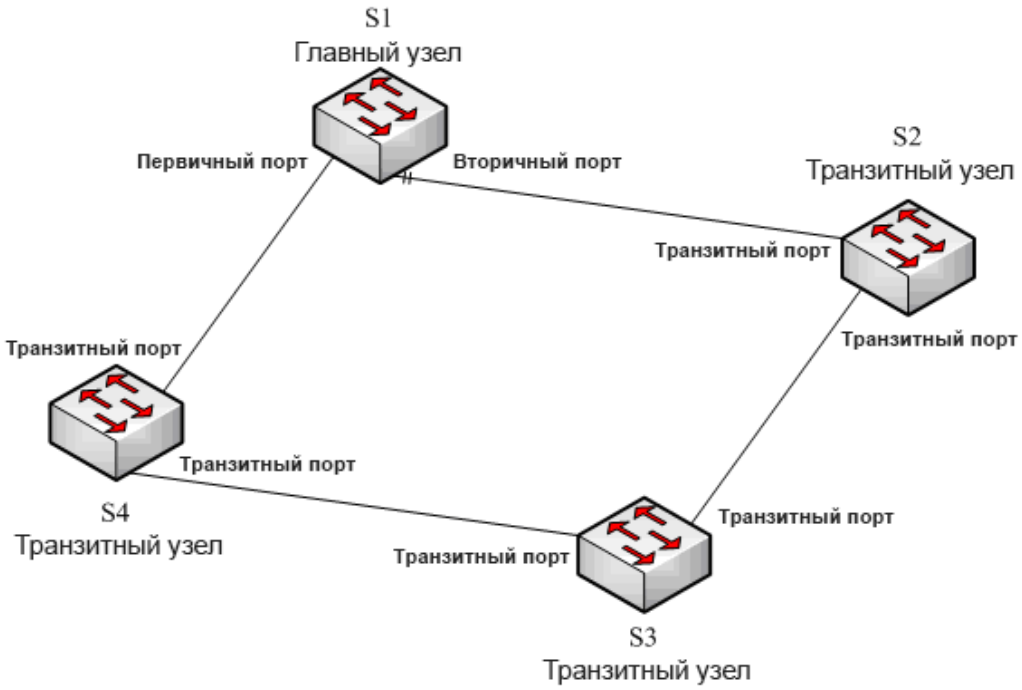

Рисунок 30-1 – Ethernet-кольцо EAPS

30.2.1 Роли кольцевых узлов

Каждый коммутатор в кольце Ethernet является узлом кольца. Кольцевые узлы подразделяются на главные и транзитные. Только один коммутатор в кольце Ethernet может служить просто главным узлом, а остальные коммутаторы работают как транзитные узлы.

- Главный (мастер) узел

Он точно знает, замкнута ли топология кольца, устраняет петлю, управляет другими коммутаторами для обновления информации о топологии.

- Транзитный узел

Он проверяет только состояние локального порта кольца и уведомляет главный узел о недействительном канале.

Роль каждого узла может быть указана пользователем посредством настройки. Дело в том, что каждому коммутатору в одном кольце можно назначить только один тип узла. На рисунке 30-1 коммутатор S1 является главным узлом кольцевой сети, а коммутаторы S2, S3 и S4 – транзитными узлами.

30.2.2 Роли кольцевых портов

EAPS требует, чтобы каждый коммутатор имел два порта для подключения к кольцевой сети. Каждый порт кольцевой сети также необходимо указать в конфигурации. Протокол поддерживает несколько ролей порта.

- Первичный (основной) порт

Основной порт можно настроить только на главном узле. Главный узел передает информацию о кольце (пакеты Ring detection) через основной порт.

- Вторичный порт

Вторичный порт можно настроить только на главном узле. Главный узел получает пакеты Ring detection от вторичного порта и оценивает целостность топологии кольцевой сети. В замкнутой топологии главный узел блокирует пакеты данных на вторичном порту и предотвращает возникновение петли; после прерывания соединения в кольцевой сети главный узел откроет вторичный порт для пересылки пакетов данных.

- Транзитный порт

Транзитный порт можно настроить только на транзитном узле. Оба порта, через которые транзитный узел подключается к кольцевой сети, являются транзитными.

Для каждого порта кольцевой сети можно настроить только одну роль после настройки роли узла коммутатора и управляющей VLAN. Как показано на рисунке 30-1, порт, через который главный узел S1 соединяется с транзитным узлом S4, является первичным, порт, через который S1 соединяется с S2, является вторичным, а порты, через которые другие коммутаторы подключаются к кольцевой сети, являются транзитными.

Чтобы настроить один и тот же коммутатор для работы с несколькими кольцами, необходимо подключать разные кольца через разные физические порты.

30.2.3 Управляющая VLAN и VLAN для передачи данных

Частная управляющая VLAN используется между главным и транзитным узлом для передачи пакетов протокола. Эта управляющая VLAN указывается пользователем в настройках. Также пользователь добавляет в нее кольцевые порты, что гарантирует нормальную пересылку пакетов протокола. Как правило, каждый порт кольцевой сети находится в управляющей VLAN в состоянии пересылки, а порты, не принадлежащие кольцевой сети, не могут пересылать пакеты управляющей VLAN.

Вы можете указать разные управляющие VLAN для каждого кольца на коммутаторе. Управляющая VLAN используется только для пересылки управляющих пакетов кольцевой сети, а не для связи L2/L3. Например, если установлен порт VLAN, соответствующий управляющей VLAN, IP-адрес порта VLAN не может быть проверен через другие устройства.

Все VLAN, за исключением управляющей, являются VLAN данных, которые используются для передачи пакетов обычных услуг или пакетов управления.

VLAN для передачи данных можно использовать для обычной связи L2/L3. Например, вы можете установить порт VLAN, соответствующий VLAN данных, и настроить протоколы динамической маршрутизации.

30.2.4 Устаревание таблицы MAC-адресов

Кольцевой протокол EAPS может передавать пакеты данных по правильному каналу, контролируя устаревание таблицы MAC-адресов коммутатора при изменении топологии. Обычно время старения MAC-адреса в таблице MAC-адресов составляет 300 секунд. Протокол EAPS может контролировать старение таблицы MAC-адресов за короткое время.

30.2.5 Символ замкнутой кольцевой сети

И главный, и транзитный узел могут показать, замкнута ли текущая кольцевая сеть, с помощью символа состояния «COMPLETE». На главном узле это происходит только тогда, когда все каналы кольцевой сети находятся в норме, первичный порт находится в состоянии пересылки, а вторичный – в состоянии блокировки. На транзитном узле – только тогда, когда его два транзитных порта находятся в состоянии пересылки.

Символ состояния кольцевой сети помогает пользователю оценивать исправность топологии.

30.3 Типы пакетов EAPS

Пакеты EAPS можно разделить на следующие типы, как показано в таблице 30-1:

Таблица 30-1 – Типы пакетов EAPS

Тип пакета	Описание
HEALTH	Обнаружение петель (здоровье системы). Пакет передается главным узлом, чтобы определить, замкнута ли топология кольцевой сети
LINK-DOWN	Указывает, что в кольце происходит прерывание соединения. Пакеты такого типа передаются транзитным узлом

RING-DOWN-FLUSH-FDB	Пакет передается главным узлом после обнаружения прерывания кольцевой сети и в нем отображается таблица устаревания MAC-адресов транзитного узла
RING-UP-FLUSH-FDB	Пакет передается главным узлом при восстановлении связи после прерывания кольцевой сети, и в нем отображается таблица устаревания MAC-адресов транзитного узла

30.4 Механизм работы кольца Ethernet

30.4.1 Ring detection и управление главным узлом

Главный узел передает пакеты HEALTH в управляющую VLAN через основной порт в течение настраиваемого периода. В случае нормальной связи пакеты HEALTH проходят через все остальные узлы кольцевой сети и, наконец, достигают вторичного порта главного узла.

В исходном состоянии вторичный порт блокирует все сети VLAN для передачи данных. При непрерывном получении пакетов HEALTH вторичный порт продолжает блокировать VLAN данных, предотвращая петлю. Если вторичный порт не получает пакеты HEALTH от основного порта в течение определенного времени (которое можно настроить), он будет считать, что кольцевая сеть вышла из строя. Затем главный узел снимает блокировку VLAN данных на вторичном порту, признает локальную таблицу MAC-адресов устаревшей и передает пакеты RING-DOWN-FLUSH-FDB для уведомления других узлов.

Если главный узел получает пакеты HEALTH на вторичном порту, открытом для VLAN данных, кольцевая сеть восстанавливается. В этом случае главный узел немедленно блокирует VLAN данных на вторичном порту, обновляет информацию о локальной топологии и сообщает другим узлам об устаревании таблицы MAC-адресов посредством пакетов RING-UP-FLUSH-FDB.

Вы можете настроить параметры «Hello-time» и «Fail-time» с целью изменения интервала передачи пакетов «HEALTH» через основной порт и временного ограничения, в течение которого вторичный порт ожидает получения пакетов «HEALTH».

30.4.2 Уведомление о нерабочем канале транзитного узла

После того, как транзитный порт транзитного узла выйдет из строя, пакет LINK-DOWN будет немедленно передан другим транзитным портом для уведомления остальных узлов. В обычной ситуации пакет проходит через другие транзитные узлы и, наконец, достигает порта главного узла.

После того как главный узел получает пакет LINK-DOWN, он считает, что кольцевая сеть неисправна. В этом случае главный узел снимает блокировку VLAN данных на своем вторичном порту, признает локальную таблицу MAC-адресов устаревшей, передает пакет RING-DOWN-FLUSH-FDB и уведомляет другие узлы.

30.4.3 Возобновление соединения транзитного узла

После возобновления работы транзитного порта он не сразу передает пакеты данных VLAN, а переходит в состояние, предшествующее началу пересылки (Pre-Forwarding). В этом состоянии транзитный порт передает и принимает только пакеты управления из управляющей VLAN.

Если в кольцевой сети имеется только один нерабочий транзитный порт, то, когда он переходит в состояние Pre-Forwarding, вторичный порт главного узла может снова получить пакет HEALTH от основного порта. В этом случае главный узел снова блокирует VLAN данных на вторичном порту и передает уведомление об устаревании таблицы адресов другим узлам. После того, как узел с транзитным портом в состоянии Pre-Forwarding получит уведомление об устаревании таблицы адресов, он сначала переведет порт в состояние обычной пересылки, а затем удалит устаревшую локальную таблицу MAC-адресов.

Если транзитный узел не получает уведомление об устаревании таблицы адресов от главного узла и считает, что связь с главным узлом потеряна, он автоматически переводит порт из состояния Pre-Forwarding в состояние обычной пересылки.

Вы можете настроить соответствующие параметры времени, предшествующего началу пересылки, чтобы изменить интервал, в течение которого транзитный порт продолжает работу в режиме Pre-Forwarding.

30.5 Конфигурация EAPS по умолчанию

Протокол EAPS не может быть настроен вместе с STP.

После отключения STP рекомендуется выполнить **spanning-tree bpdu-terminal**, чтобы запретить кольцевым узлам пересылку BPDU во избежание шторма.

Настройки по умолчанию для протокола кольцевого резервирования и STP следующие:

- протокол связующего дерева – **spanning-tree mode rstp**;
- протокол кольцевого резервирования Ethernet – не настроен.

30.6 Требования перед настройкой

Перед настройкой протокола кольцевого резервирования внимательно прочитайте следующие пункты:

- Одной из важных функций протокола является недопущение широковещательного шторма, поэтому перед повторным подключением кольцевого канала убедитесь, что все узлы кольца корректно настроены. Если кольцевая сеть подключена и настройка не завершена, может легко возникнуть широковещательный шторм.

- Хотя EAPS в настоящее время совместим с STP, порт, находящийся под контролем EAPS, не подчиняется STP.
- Протокол кольцевого резервирования позволяет коммутатору настраивать несколько кольцевых сетей.
- Настройка VLAN управления кольцом приведет к автоматическому созданию соответствующей системной VLAN.
- Порт каждого кольца может пересылать пакеты из управляющей VLAN, тогда как для других портов, даже настроенных в режиме trunk, эта VLAN недоступна.
- По умолчанию время сбоя (Fail-time) главного узла в три раза дольше, чем время приветствия (Hello-time), поэтому задержка пакетов не приводит к нарушению работы кольца. После изменения времени приветствия необходимо соответствующим образом изменить время сбоя.
- По умолчанию время Pre-Forwarding транзитного узла в три раза превышает время приветствия главного узла, чтобы гарантировать, что главный узел сможет обнаружить восстановление кольцевой сети до того, как транзитный порт войдет в режим пересылки. Если время приветствия, настроенное на главном узле, превышает время Pre-Forwarding транзитного узла, легко генерируется петля и запускается широковещательный шторм.
- Физический интерфейс (Fast-Ethernet, Gigabit-Ethernet) и логический интерфейс агрегации можно настроить в качестве кольцевого порта. Если на физическом интерфейсе уже настроены агрегация, 802.1X или безопасность портов, этот физический интерфейс больше нельзя настроить в качестве кольцевого.

30.7 Настройка протокола кольцевого резервирования

Задачи настройки

- Настройка главного узла
- Настройка транзитного узла
- Настройка кольцевого порта
- Просмотр состояния протокола

30.7.1 Настройка главного узла

Настройте коммутатор в качестве главного узла кольцевой сети, выполнив следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **ether-ring** *id*	Устанавливает узел и входит в режим настройки узла. *id*: идентификатор экземпляра
Switch_config_ring# **control-vlan** *vlan-id*	Настраивает управляющую VLAN. *vlan-id*: идентификатор управляющей VLAN
Switch_config_ring# **master-node**	Настраивает тип узла как главный узел
Switch_config_ring# **hello-time** *value*	Этот шаг не является обязательным. Настраивает интервал передачи главным узлом пакетов HEALTH. *value*: значение времени в диапазоне от 1 до 10 секунд, значение по умолчанию – 1 секунда
Switch_config_ring# **fail-time** *value*	Этот шаг не является обязательным. Настраивает время, в течение которого вторичный порт будет ожидать пакетов HEALTH. *value*: значение времени в диапазоне от 3 до 30 секунд, значение по умолчанию – 3 секунды
Switch_config_ring# **exit**	Сохранение текущих настроек и выход из режима настройки узла

Команда **no ether-ring id** используется для удаления настроек узла и кольцевого порта.

30.7.2 Настройка транзитного узла

Для настройки коммутатора в качестве транзитного узла кольцевой сети, выполните следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **ether-ring** *id*	Устанавливает узел и входит в режим настройки узла. *id*: идентификатор экземпляра
Switch_config_ring# **control-vlan** *vlan-id*	Настраивает управляющую VLAN. *vlan-id*: идентификатор управляющей VLAN

Switch_config_ring# **transit-node**	Настраивает тип узла как транзитный узел
Switch_config_ring# **pre-forward-time** *value*	Этот шаг не является обязательным. Настраивает время поддержания состояния Pre-Forwarding на транзитном порту. *value*: значение времени в диапазоне от 3 до 30 секунд, значение по умолчанию – 3 секунды
Switch_config_ring# **exit**	Сохранение текущих настроек и выход из режима настройки узла

30.7.3 Настройка кольцевого порта

Чтобы настроить порт коммутатора в качестве порта кольца Ethernet, выполните следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **interface** *intf-name*	Вход в режим настройки интерфейса. *intf-name*: обозначает имя интерфейса
Switch_config_intf# **ether-ring** *id* {**primary-port** | **secondary-port** | **transit-port**}	Настраивает тип кольцевого порта. *id*: идентификатор узла кольца Ethernet
Switch_config_intf# **exit**	Выход из режима настройки интерфейса

Команда **no ether-ring** *id* {**primary-port** | **secondary-port** | **transit-port**} может использоваться для отмены настроек кольцевого порта.

30.7.4 Просмотр состояния протокола

Выполните следующую команду, чтобы просмотреть состояние кольцевого протокола:

Команда	Описание
show ether-ring *id*	Отображает сводную информацию о кольцевом протоколе и портах кольца Ethernet. id: идентификатор кольца Ethernet
show ether-ring *id* **detail**	Отображает подробную информацию о кольцевом протоколе и портах кольца Ethernet
show ether-ring *id* **interface** *intf-name*	Отображает состояние кольцевого или общего порта

30.7.5 Пример настройки EAPS

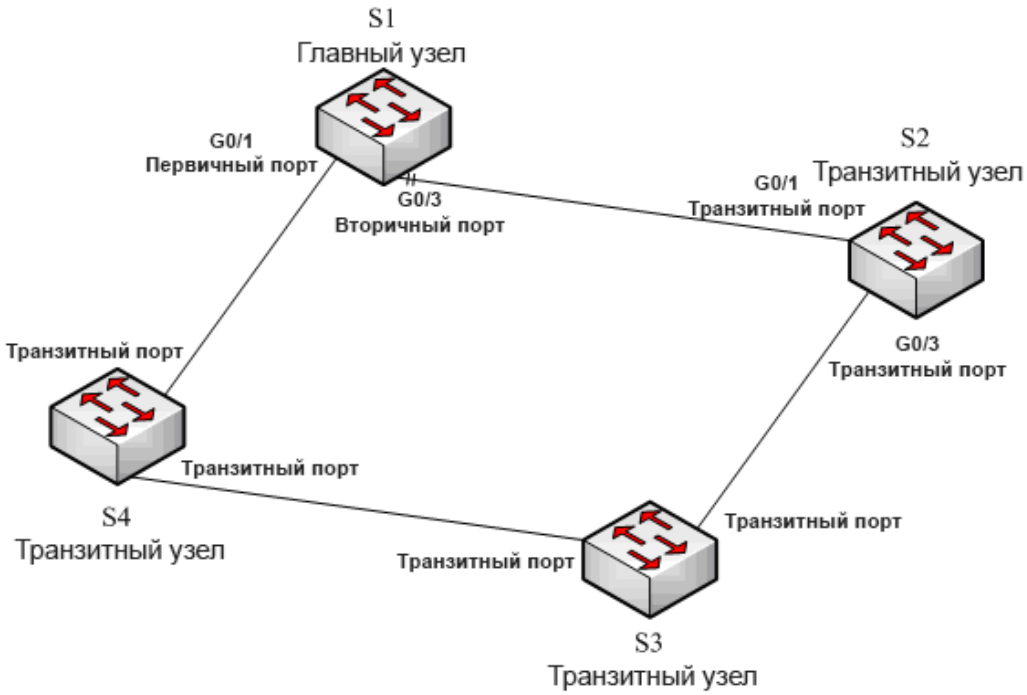

Рисунок 30-2 – Настройка EAPS

Как показано на рисунке 30-2, главный узел S1 и транзитный узел S2 настроены следующим образом. Что касается настроек остальных узлов, то они аналогичны настройкам S2.

- **Настройка коммутатора S1:**

Выключение STP и настройка узла кольцевой топологии:

```
S1_config# no spanning-tree
S1_config# ether-ring 1
S1_config_ring1# control-vlan 2
S1_config_ring1# master-node
```

Следующие команды используются для установки параметров, связанных со временем:

```
S1_config_ring1# hello-time 2
S1_config_ring1# fail-time 6
```

Выход из режима настройки узла:

```
S1_config_ring1# exit
```

Настройка первичного и вторичного портов:

S1_config# interface gigaEthernet 0/1

S1_config_g0/1# ether-ring 1 primary-port

S1_config_g0/1# exit

S1_config# interface gigaEthernet 0/3

S1_config_g0/3# ether-ring 1 secondary-port

S1_config_g0/3# exit

Настройка управляющей VLAN:

S1_config# vlan 2

S1_config_vlan2# exit

S1_config# interface range g0/1 , 3

S1_config_if_range# switchport mode trunk

S1_config_if_range# exit

- **Настройка коммутатора S2:**

S1_config# no spanning-tree

S1_config# ether-ring 1

S1_config_ring1# control-vlan 2

S1_config_ring1# transit-node

S1_config_ring1# pre-forward-time 8

S1_config_ring1# exit

S1_config# interface gigaEthernet 0/1

S1_config_g0/1# ether-ring 1 transit-port

S1_config_g0/1# exit

S1_config# interface gigaEthernet 0/3

S1_config_g0/3# ether-ring 1 transit-port

S1_config_g0/3# exit

S1_config# vlan 2

S1_config_vlan2# exit

S1_config# interface range gigaEthernet 0/1 , 3

S1_config_if_range# switchport mode trunk

S1_config_if_range# exit

31. Настройка MEAPS

31.1 Введение

EAPS – это протокол, специально применяемый на канальном уровне для кольцевой топологии Ethernet. Когда кольцо замкнуто, это предотвращает возникновение петли и широковещательного шторма. Но когда канал кольца Ethernet прерывается, протокол быстро включает резервный канал, чтобы возобновить связь между различными узлами в кольце. Роль коммутатора задается пользователем при помощи настроек.

MEAPS, расширение на основе EAPS, может поддерживать не только однокольцевую, но и многокольцевую структуру 2-го уровня. Эта структура состоит из уровня агрегации посередине, созданного оборудованием агрегации при помощи кольца Ethernet, и уровня доступа снаружи, представленного оборудованием доступа. Различные уровни колец соединяются посредством касания или пересечения. Пример топологии показан на рисунке 31-1:

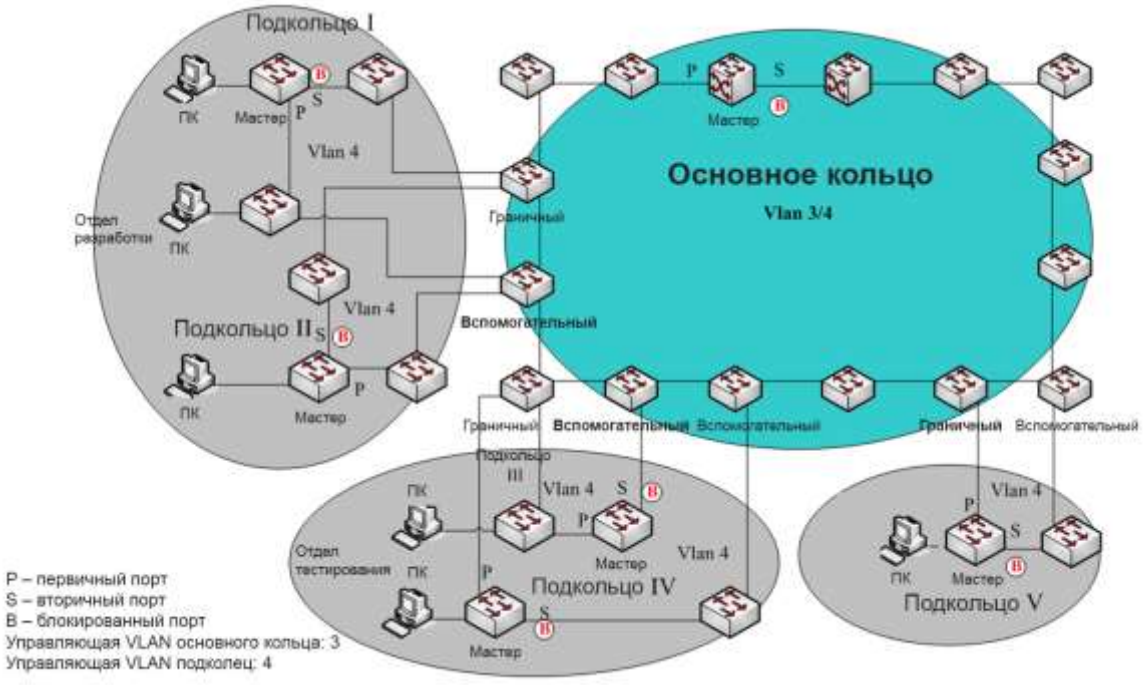

Рисунок 31-1 – Структура MEAPS

Протокол кольцевого резервирования и STP используются для управления топологией на канальном уровне. STP подходит для всех видов сложных сетей, которые передают

изменение топологии сети шаг за шагом. Протокол кольцевого резервирования применяется для кольцевой топологии и использует механизм распространения оповещений для передачи информации об изменениях сети. Таким образом, сходимость в кольцевой сети лучше, чем в STP. В хорошо настроенной сети протокол кольцевого резервирования может возобновить сетевое соединение менее чем за 50 мс.

31.2 Основные понятия MEAPS

31.2.1 Домен

Домен определяет диапазон защищаемого от петель сегмента Ethernet и помечается идентификатором, состоящим из целых чисел. Группа коммутаторов, поддерживающих одни и те же настройки защиты и имеющих одну и ту же управляющую VLAN, может образовывать домен после их соединения друг с другом. Один домен может включать только одно кольцо или несколько колец, пересекающихся друг с другом (см. рисунок 31-2).

Один домен MEAPS имеет следующие компоненты: кольцо MEAPS, управляющая VLAN, главный (мастер) узел, транзитный узел, граничный узел и вспомогательный граничный узел.

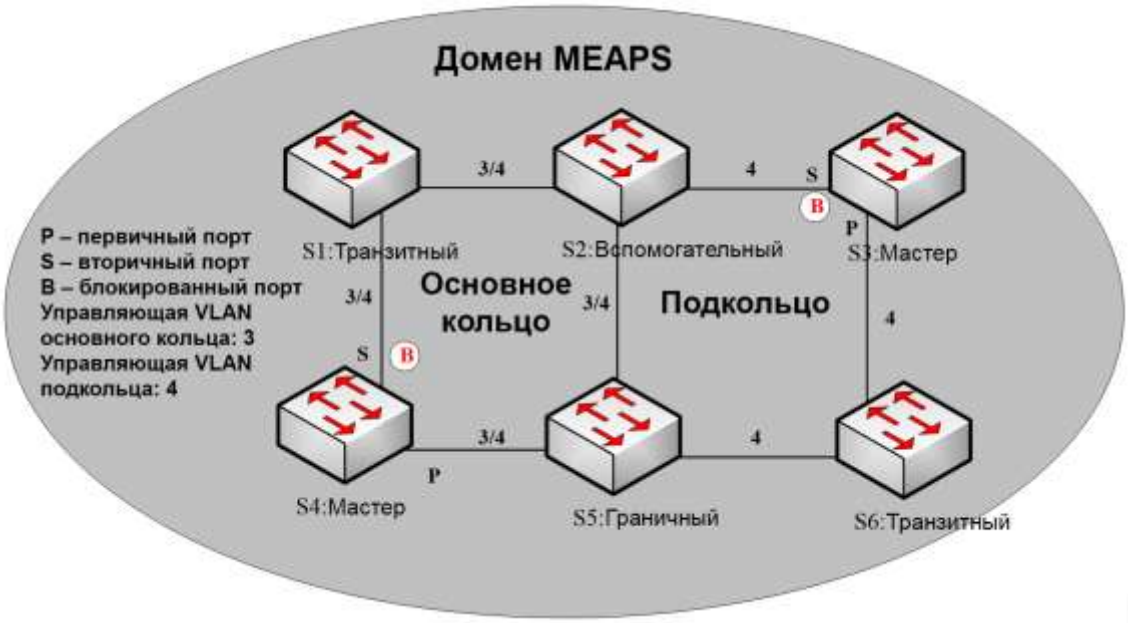

Рисунок 31-2 – Простая модель MEAPS

31.2.2 Кольцо

Одно кольцо физически соответствует кольцевой топологии Ethernet, которая представляет собой группу коммутаторов, соединенных друг с другом. Один домен MEAPS может включать только одно кольцо или несколько колец, пересекающихся друг с другом.

31.2.3 Основное кольцо

Если домен состоит из множества колец, включенные в него дополнительные кольца, за исключением основного, называются подкольцами. Первичные и вторичные порты каждого узла основного кольца должны быть добавлены в основную управляющую VLAN и дополнительную управляющую VLAN подколец одновременно, как показано на рисунке 31-2.

31.2.4 Дополнительное кольцо

Когда домен включает в себя множество колец, из них следует выбрать одно кольцо в качестве основного. Первичные и вторичные порты каждого узла в дополнительном кольце (подкольце) должны быть добавлены в дополнительную управляющую VLAN подкольца (см. рисунок 31-2).

31.2.5 VLAN управления

VLAN управления функционально отличается от VLAN данных. В MEAPS управляющая VLAN используется только для передачи пакетов протокола. Каждая сеть MEAPS имеет две управляющие VLAN: основную и дополнительную.

При настройке основного кольца или подкольца необходимо указать основную управляющую VLAN, а в качестве дополнительной выбрать VLAN, идентификатор которой на 1 больше, чем идентификатор основной. Основное кольцо будет добавлено к основной и дополнительной управляющей VLAN одновременно, а подкольцо будет добавлено только к дополнительной управляющей VLAN, как показано на рисунке 31-2.

Пакеты протокола основного кольца передаются в основной управляющей VLAN, а пакеты протокола подкольца – в дополнительной. Дополнительная VLAN управления на основном кольце является VLAN данных основного кольца. Порты коммутатора, имеющие доступ к кольцу Ethernet, принадлежат управляющей VLAN; в управляющую VLAN можно добавить только те порты, которые обращаются к кольцу Ethernet.

Порт MEAPS основного кольца должен принадлежать как основной управляющей VLAN, так и дополнительной; порт MEAPS подкольца принадлежит только дополнительной управляющей VLAN. Основное кольцо рассматривается как логический узел подкольца, и через него прозрачно передаются пакеты подкольца; пакеты главного кольца передаются только в главном кольце.

31.2.6 VLAN для передачи данных

В отличие от управляющей VLAN, передающей только специальные сообщения, касающиеся сетевой топологии, VLAN данных используется для передачи пакетов различной информации. VLAN данных может включать в себя порт MEAPS и порт, не имеющий отношения к MEAPS. Каждый домен защищает одну или несколько VLAN данных. Топология, рассчитанная кольцевым протоколом в домене, действительна только для VLAN данных в этом домене.

Создана ли, или нет VLAN данных, это не влияет на работу механизма кольца, где порт MEAPS управляется модулем MEAPS, а порт, не относящийся к MEAPS, контролируется модулем STP.

Могут использоваться методы обработки, аналогичные методам модуля MSTP, то есть статус порта в экземпляре STP по умолчанию определяется статусом соединения порта, независимо от того, какова конфигурация VLAN этого порта.

31.2.7 Главный узел

Главный узел, или мастер-узел, выполняет функции определения политики и управления кольцом. Каждое кольцо должно иметь только один главный узел. Главный узел активно проверяет, замкнута ли топология кольца, удаляет петлю, контролирует своевременное обновление информации о топологии на других коммутаторах. См. рисунок 31-2, где S3 – главный узел подкольца, а S4 – главный узел основного кольца.

31.2.8 Транзитный узел

Все коммутаторы Ethernet, за исключением мастера, можно называть транзитными узлами. Транзитный узел только проверяет состояние локального порта кольца и уведомляет главный узел о недействительном канале. См. рисунок 31-2, на котором S1, S2, S5 и S6 – транзитные узлы.

31.2.9 Граничный и вспомогательный узлы

Когда подкольцо и основное кольцо пересекаются, возникают две точки пересечения, два коммутатора, один из которых называют граничным узлом, а другой – вспомогательным. Оба узла являются узлами подкольца. Нет специальных требований относительно того, какой из коммутаторов будет выбран в качестве граничного, а какой в качестве вспомогательного узла, если их конфигурации позволяют им отличать друг друга. Однако один из них должен быть настроен как граничный узел, а другой – как вспомогательный. Роль узла определяет, какую функцию коммутатор выполняет в подкольце, но этот же

коммутатор может выполнять функции транзитного или главного узла, когда он находится в основной кольцевой сети.

31.2.10 Первичный и вторичный порты

Два порта, через которые главный узел получает доступ к кольцу Ethernet, называются первичным (основным) и вторичным портом. Роль двух портов определяется клиентами.

Когда первичный порт включен, он находится в состоянии пересылки. Его функция заключается в пересылке пакетов VLAN данных на главный узел, а также в приеме и передаче пакетов управления в управляющей VLAN. Главный узел будет передавать пакеты обнаружения петель из основного порта в управляющую VLAN. Если канал основного порта восстанавливается из нерабочего состояния, главный узел должен немедленно отправить уведомление об устаревании адресов в управляющую VLAN, а затем начать передавать пакеты обнаружения петель из основного порта.

Вторичный порт находится в состоянии пересылки или блокировки, когда он включен. Главный узел получает пакеты Ring detection от вторичного порта и оценивает, замкнута ли топология кольцевой сети. В замкнутой топологии главный узел блокирует пакеты данных на вторичном порту и предотвращает возникновение петли. В случае прерывания соединения в кольце главный узел откроет вторичный порт для пересылки пакетов данных.

Порт может быть настроен как основной или вторичный порт узла, но не может быть одновременно и основным, и вторичным.

31.2.11 Общий и граничный порты

Граничный узел и вспомогательный узел – это места пересечения подкольца и основного кольца. Что касается двух портов, имеющих доступ к Ethernet, то один из них является общим портом, доступным для подкольца и основного кольца; другой – это граничный порт в подкольце. Роли двух портов определяются пользователями посредством настроек.

Общий порт находится на интерфейсе основного кольца, поэтому его состояние определяется состоянием порта основного кольца. Сам общий порт не производит никаких операций или уведомлений. При изменении состояния канала, соединенного с общим портом, узел подкольца, где находится общий порт, не будет уведомлен. Наличие общего порта только гарантирует целостность кольца.

Граничный порт граничного узла находится в состоянии пересылки или Pre-Forwarding, когда он включен. Его основные характеристики соответствуют характеристикам транзитного порта, за исключением одной функции. Она заключается в том, что, когда граничный порт и соответствующий порт основного кольца включены, он будет передавать пакеты Edge-Hello из порта основного кольца для определения его целостности.

Граничный порт вспомогательного узла находится в состоянии пересылки, Pre-Forwarding или Edge Preforwarding, когда он включен. Помимо характеристик транзитного порта, он также имеет еще одно состояние – состояние Edge Preforwarding. Если граничный порт находится в состоянии пересылки, а порт основного кольца, которому соответствует граничный порт, не получил пакеты Edge-Hello, состояние пограничного порта изменяется на состояние Edge Preforwarding, и он получает и пересылает только пакеты управления, а также блокирует VLAN данных до тех пор, пока соответствующий порт основного кольца снова не получит пакеты Edge-hello.

Граничный порт граничного узла и вспомогательный узел помогают поддерживать целостность основного кольца. Для получения более подробной информации см. раздел «Механизм работы кольцевой сети».

Каждый порт можно настроить как единственный граничный порт узла, после чего эту настройку уже нельзя изменить. Общий порт может существовать только на порту основного кольца, эта настройка не может быть применена к другим портам в сети.

31.2.12 Устаревание таблицы MAC-адресов (FLUSH MAC FDB)

Протокол кольцевого резервирования может передавать пакеты данных по правильному каналу, контролируя устаревание таблицы MAC-адресов коммутатора при изменении топологии. Обычно время устаревания MAC-адреса в таблице составляет 300 секунд. Протокол может управлять этим процессом в более короткие сроки.

31.2.13 Символ замкнутой кольцевой сети

И главный узел, и транзитный могут показать, замкнута ли текущая кольцевая сеть, с помощью символа состояния «COMPLETE». На мастер-узле флаг «COMPLETE» отображается только в том случае, если все соединения кольцевой сети в нормальном состоянии, первичный порт находится в состоянии пересылки, а вторичный – в состоянии блокировки. На транзитном узле «COMPLETE» отобразится, если оба транзитных порта находятся в состоянии пересылки.

Символ «COMPLETE» помогает пользователю судить о состоянии топологии текущей сети.

31.3 Типы пакетов MEAPS

Пакеты MEAPS можно разделить на следующие типы, как показано в таблице 31-1:

Таблица 31-1 – Типы пакетов MEAPS

Тип пакета	Описание
Проверка кольца (HEALTH)	Проверка наличия петли (здоровье системы). Пакет передается главным узлом, чтобы определить, замкнута ли топология кольцевой сети
Прерывание связи (LINK-DOWN)	Указывает, что в кольце происходит прерывание соединения. Пакеты такого типа передаются транзитным узлом
Таблица устаревания MAC-адресов транзитного узла (RING-DOWN-FLUSH-FDB)	Пакет передается главным узлом после обнаружения прерывания кольцевой сети и в нем отображается таблица устаревания MAC-адресов транзитного узла
Таблица адресов восстановленного кольца (RING-UP-FLUSH-FDB)	Пакет передается главным узлом при восстановлении связи после прерывания кольцевой сети, и в нем отображается таблица устаревания MAC-адресов транзитного узла
Проверка целостности кольца (EDGE-HELLO)	Механизм, который зависит от граничного порта на граничном узле сети. Информация о состоянии кольца передается через основной порт, который соответствует граничному узлу, и служит для определения, находится ли основное кольцо в замкнутом состоянии

31.4 Механизм работы кольцевой сети

31.4.1 Механизм опроса

Первичный порт передает пакеты HEALTH в управляющую VLAN. В исправной сети пакеты HEALTH проходят через все остальные узлы кольца и, наконец, достигают вторичного порта главного узла.

В исходном состоянии вторичный порт блокирует все сети VLAN для передачи данных. При непрерывном получении пакетов HEALTH вторичный порт продолжает блокировать VLAN данных, не допуская образования петли. Если вторичный порт не получает пакеты HEALTH от основного порта в течение определенного времени (которое можно настроить), он будет считать, что кольцевая сеть не работает. Затем главный узел снимает блокировку VLAN данных на вторичном порту, удаляет устаревшую локальную таблицу MAC-адресов и передает пакеты RING-DOWN-FLUSH-FDB для уведомления других узлов.

Если главный узел получает пакеты HEALTH на вторичном порту, открытом для VLAN данных, кольцевая сеть восстанавливается. В этом случае главный узел немедленно блокирует VLAN данных на вторичном порту, обновляет информацию о локальной топологии и сообщает другим узлам об устаревании таблицы MAC-адресов посредством пакетов RING-UP-FLUSH-FDB.

Как показано на рисунке 31-3, главный узел S4 периодически передает пакеты HELLO. Если с сетью все в порядке, пакеты HELLO прибудут на вторичный порт главного узла, и главный

узел заблокирует пересылку пакетов VLAN данных, к которой принадлежит вторичный порт, предотвращая возникновение петли.

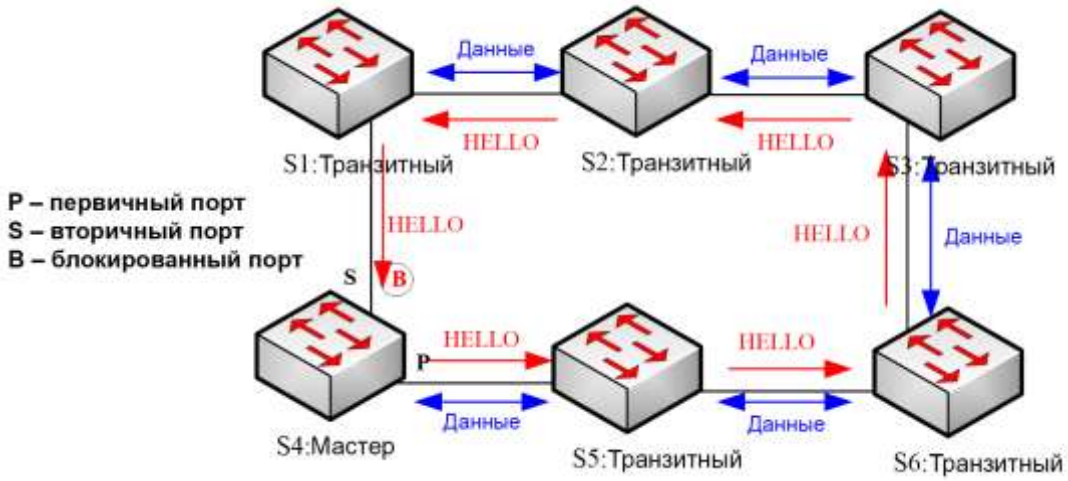

Рисунок 31-3 – Механизм опроса

Вы можете настроить параметры «Hello-time» и «Fail-time» с целью изменения интервала передачи пакетов HEALTH через основной порт и временного ограничения, в течение которого вторичный порт ожидает получения пакетов HEALTH.

31.4.2 Уведомление о неисправном канале транзитного узла

Механизм уведомления об изменении состояния канала обеспечивает более быструю обработку изменений топологии кольцевой сети, чем механизм опроса.

В случае выхода из строя транзитного порта транзитного узла, пакет LINK-DOWN будет немедленно передан другим транзитным портом для уведомления других узлов. В результате пакет проходит через другие транзитные узлы и, наконец, достигает порта главного узла.

После того как главный узел получает пакет LINK-DOWN, он считает, что кольцевая сеть неисправна. В этом случае главный узел снимает блокировку VLAN данных на своем вторичном порту, удаляет устаревшую локальную таблицу MAC-адресов, передает пакет RING-DOWN-FLUSH-FDB и уведомляет другие узлы. Как показано на рисунке 31-4, проблема возникла на канале между узлами S3 и S6. После того как узлы S3 и S6 обнаруживают проблему, они блокируют порты, которым соответствует данный канал, и передают пакеты LINK-DOWN соответственно из другого порта; когда главный узел получает пакеты LINK-DOWN, он считает, что проблема возникла из-за петли, и решает больше не ждать окончания времени Fail-time.

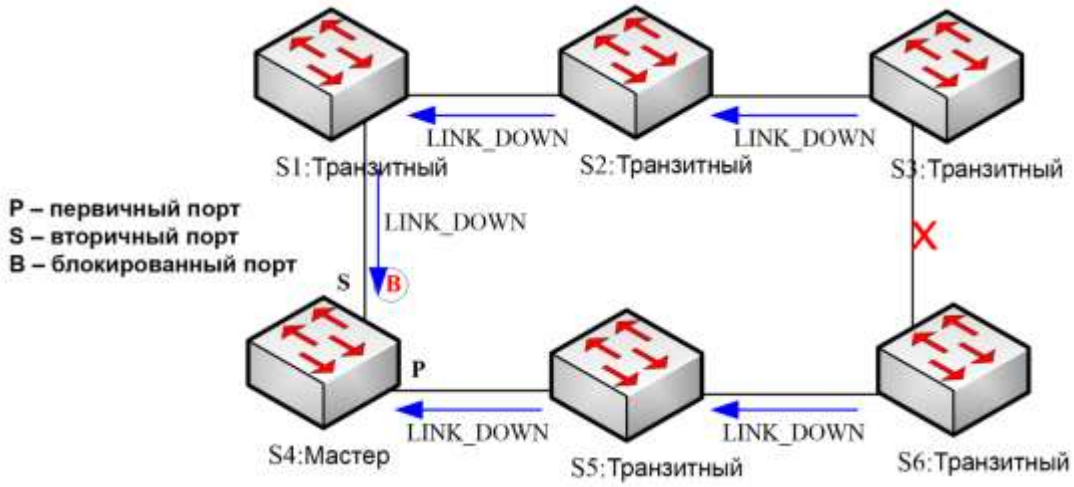

Рисунок 31-4 – Уведомление об изменении состояния связи

После возобновления работы транзитного порта он не сразу передает пакеты данных VLAN, а переходит в состояние, предваряющее начало пересылки (Pre-Forwarding). Транзитный порт в состоянии Pre-Forwarding передает и принимает только пакеты управления из управляющей VLAN.

Если в кольцевой сети имеется только один нерабочий транзитный порт, то, когда он переходит в состояние Pre-Forwarding, вторичный порт главного узла может снова получить пакет HEALTH от основного порта. В этом случае главный узел снова блокирует VLAN данных на вторичном порту и передает уведомление об устаревании таблицы адресов остальным узлам. После того, как узел с транзитным портом в состоянии Pre-Forwarding получит уведомление об устаревании таблицы адресов, он сначала изменит режим порта с Pre-Forwarding на обычную пересылку, а затем удалит устаревшую локальную таблицу MAC-адресов.

Если транзитный узел не получает уведомление об устаревании таблицы адресов от главного узла, он считает, что связь, соединяющая главный узел, более недействительна, и автоматически меняет режим передачи с Pre-Forwarding на обычную пересылку данных.

Пользователь может самостоятельно настроить время, в течение которого будет удерживаться режим Pre-Forwarding.

31.4.3 Механизм проверки состояния канала подкольца

Порты основного кольца одновременно добавляются как в управляющую VLAN основного кольца, так и в управляющую VLAN подкольца. Следовательно, пакеты протоколов

подкольца должны транслироваться между граничными портами граничного и вспомогательного узлов через канал, предоставляемый основным кольцом. В этом случае все основное кольцо как бы становится узлом подкольца (аналогично виртуальному транзитному узлу), как показано на следующем рисунке:

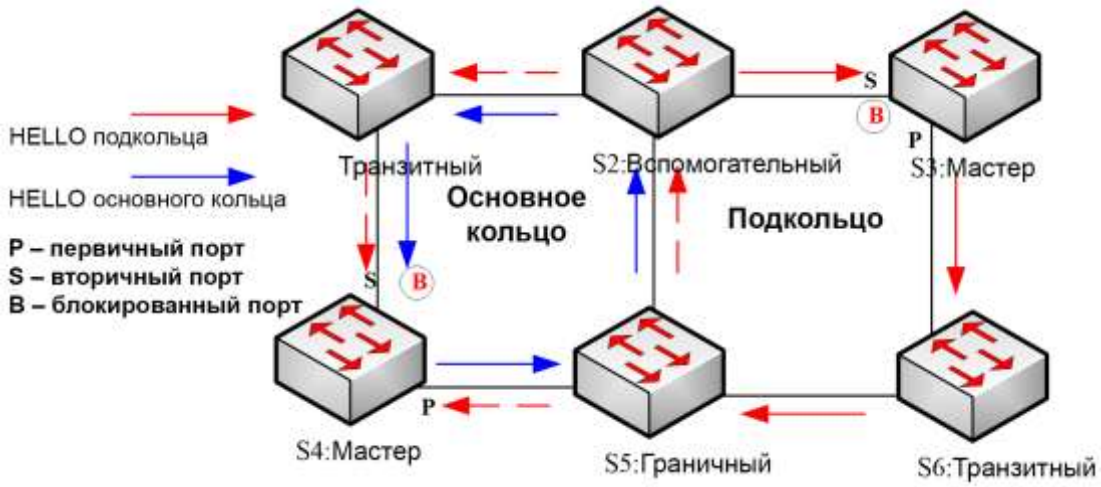

Рисунок 31-5 – Пересечение основного кольца и подкольца

При возникновении неисправности на канале главного кольца и когда канал, по которому идут пакеты протокола подкольца, между граничным и вспомогательным узлами прерывается, главный узел подкольца не может получить свои отправленные пакеты HELLO. В этом случае временной интервал Fail-time истекает, а главный узел подкольца переходит в состояние сбоя и открывает свой вторичный порт.

Вышеупомянутые процессы имеют эффективную защиту по сравнению с обычной сетью, гарантируя не только предотвращение петли, но и соответствующие функции резервного канала. Режим двойного подключения (dual homing) всегда используется в реальной сети, как показано на рисунке 31-6. Два подкольца в сети с двойной адресацией, подкольцо I и подкольцо II, соединяются между собой через граничный узел и вспомогательный узел и образуют большое кольцо. Когда в главном кольце возникают проблемы, вторичные порты главных узлов всех подколец открываются, и начинается широковещательная передача в большом кольце.

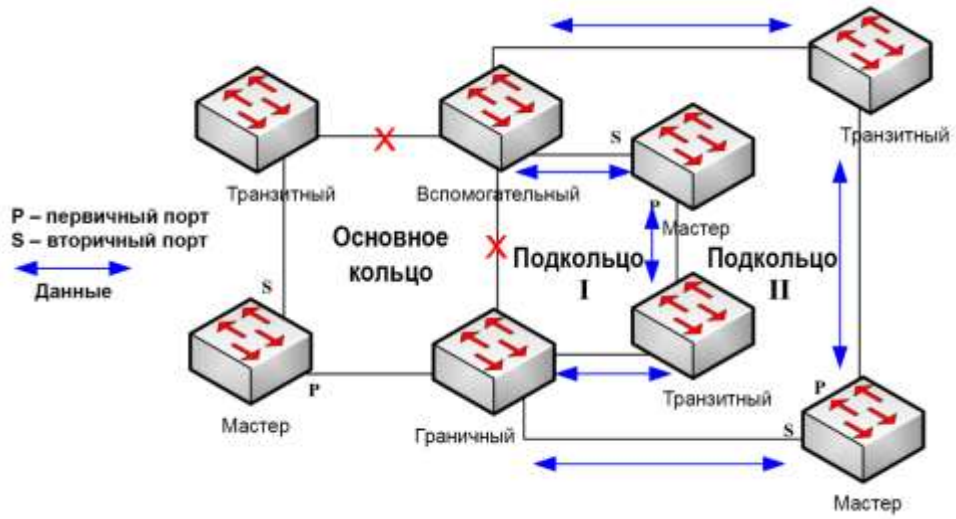

Рисунок 31-6 – Широковещательный шторм, вызванный режимом dual homing

Механизм проверки состояния канала протокола подкольца на основном кольце введен для решения проблемы кольца с двойным подключением. Этот механизм предназначен для мониторинга состояния канала связи на главном кольце между граничным и вспомогательным узлами, что требует их непосредственного участия. Целью этого механизма является предотвращение возникновения петли путем блокировки граничного порта граничного узла до того, как откроется вторичный порт главного узла на подкольце. Граничный узел является триггером механизма, а вспомогательный узел слушает и принимает решение относительно необходимого действия. Если уведомление от граничного узла не может быть получено, граничный узел мгновенно перейдет в состояние блокировки до тех пор, пока это уведомление не будет получено снова. Работа этого механизма, начавшаяся в результате неполадок на главном кольце, показана на следующем рисунке:

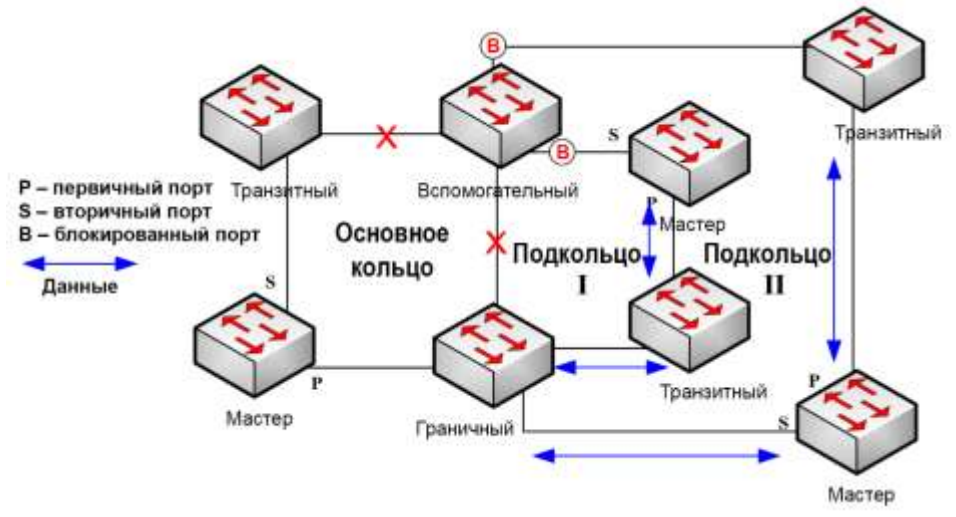

Рисунок 31-7 – Результаты работы механизма проверки состояния канала

Следует обратить особое внимание на важный момент: граничный порт вспомогательного узла должен быть заблокирован до того, как откроется вторичный порт главного узла на подкольце. В противном случае произойдет широковещательный шторм.

Вся процедура работы этого механизма описывается следующим образом:

1. Проверка состояние связи на основном кольце между граничным узлом и вспомогательным узлом

Граничный узел подкольца периодически передает пакеты Edge-Hello в основное кольцо через два порта главного кольца. Эти пакеты последовательно проходят через все узлы главного кольца и, наконец, достигают вспомогательного узла, как показано на рисунке 31-8. Если вспомогательный узел может получить пакет Edge-Hello в установленное время, это указывает на то, что связь нормальная; если нет, это означает, что канал прерван. Пакет Edge-Hello является пакетом управления подкольца, но он передается и принимается портами основного кольца и передается на подкольцо для обработки.

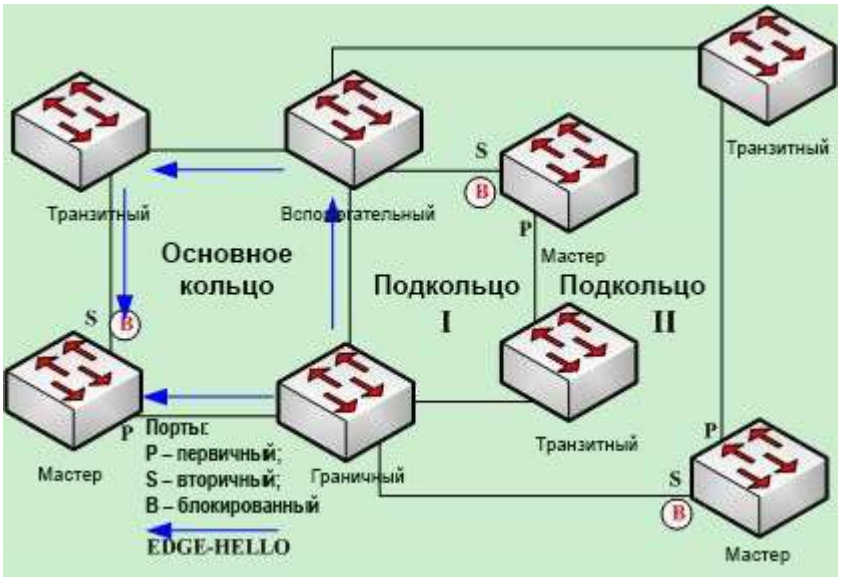

Рисунок 31-8 – Проверка состояния канала на основном кольце между граничным и вспомогательным узлами

2. Граничный узел блокирует граничный порт при прерывании канала

Если вспомогательный узел не может получить пакет Edge-Hello в течение времени Edge Fail Time, он считает, что канал, по которому пересылаются пакеты Edge-Hello, прерван и меняет статус своего граничного порта на статус Edge-Preforwarding, мгновенно блокируя пересылку пакетов данных (хотя по-прежнему получает и пересылает пакеты управления).

После этого он передает пакет LINK-DOWN главному узлу, чтобы главный узел открыл вторичный порт во избежание прерывания связи между всеми узлами кольца.

Чтобы гарантировать, что граничный порт сначала перейдет в состояние Edge-Preforwarding, а затем главный узел откроет вторичный порт, вы должны быть уверены, что цикл передачи пакета Edge-Hello граничного узла, короче, чем цикл передачи пакета Hello главного узла. То есть, значение Edge Hello-Time меньше значения Hello-Time. Аналогично, Edge Fail-Time вспомогательного узла должно быть меньше, чем Fail-Time. В то же время значение интервала Fail-Time обычно является тройным значением Hello-Time, а Edge Fail-Time – тройным значением Edge Hello-Time.

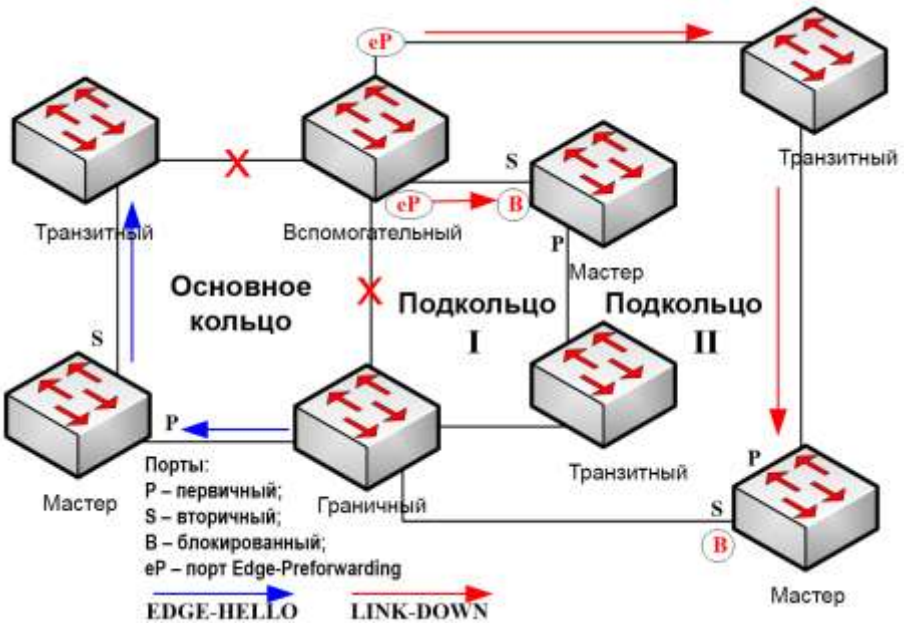

Рисунок 31-9 – Граничный порт блокируется граничным узлом при прерывании канала

3. Восстановление канала

Когда канал основного кольца и связь между граничным и вспомогательным узлами восстанавливаются, канал, по которому передаются пакеты протокола подкольца, возобновляет нормальную работу. В этом случае мастер-узел подкольца снова получает свой пакет Hello, переходит в статус COMPLETE, блокирует вторичный порт и передает по кольцу пакет RING-UP-FLUSH-FDB. В то же время статус граничного порта вспомогательного узла меняется с Pre-Forwarding на обычную пересылку, гарантируя бесперебойную связь между всеми узлами в кольце. На рисунке 31-10 показано, что канал восстанавливается, а затем возобновляется связь по кольцу.

Прежде чем граничный узел откроет заблокированный граничный порт, вторичный порт главного узла подкольца должен быть заблокирован, чтобы предотвратить широковещательный шторм.

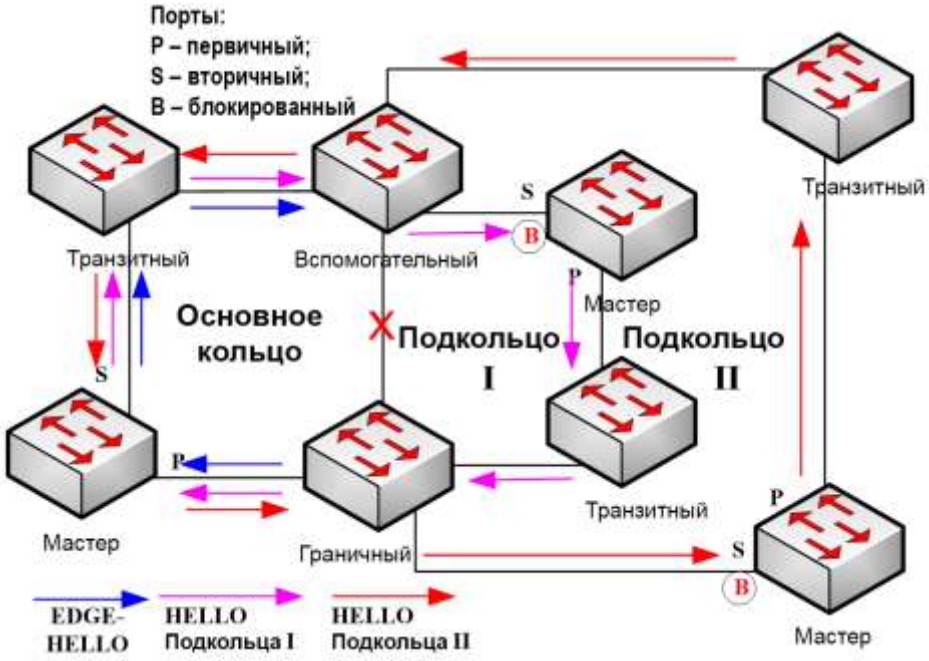

Рисунок 31-10 – Восстановление канала

31.5 Настройка протокола кольцевого резервирования

Задачи настройки MEAPS

- Настройка главного узла
- Настройка транзитного узла
- Настройка граничного и вспомогательного узлов
- Настройка кольцевого порта
- Просмотр состояния протокола

31.5.1 Требования перед настройкой

Перед настройкой MEAPS внимательно прочитайте следующие пункты:

- Одной из важных функций протокола кольцевого резервирования является предотвращение широковещательного шторма, поэтому перед переключением канала убедитесь, что все узлы кольца настроены. Например, при настройке EAPS после настройки главного узла и всех транзитных узлов подключите сетевой кабель и вторичный порт главного узла; при настройке ERPS оставьте хотя бы одно соединение отключенным, пока не будут настроены все кольцевые узлы.
- Включая протокол кольцевого резервирования, следите, чтобы он был совместим с STP коммутатора. Этого можно достичь с помощью соответствующих настроек. Пользователям разрешено устанавливать режим «без связующего дерева», SSTP, RSTP PVST или MSTP.
- После настройки экземпляра узла кольца пользователям запрещается изменять основную информацию узла (за исключением временных параметров), если только текущий узел кольца не будет удален и переустановлен.
- Если вы запустите команду **show** для просмотра настроенного узла и обнаружите, что его состояние – init, это показывает, что конфигурация узла не завершена и, следовательно, узел не может быть запущен. В этом случае вам потребуется изменить или добавить базовую информацию для завершения настройки узла.
- Протокол кольцевого резервирования поддерживает настройку нескольких кольцевых сетей.
- Настройка управляющей VLAN кольца автоматически создает соответствующую VLAN, не требуя участия пользователя.
- Порт каждого кольца может пересылать пакеты управляющей VLAN кольца, тогда как другие порты, даже в режиме Trunk, не могут пересылать пакеты управляющей VLAN.
- По умолчанию время сбоя (Fail-time) главного узла в три раза дольше, чем время приветствия (Hello-time), поэтому задержка пакетов не приводит к нарушению работы протокола. После изменения времени приветствия необходимо соответствующим образом изменить время сбоя.
- По умолчанию время Pre-Forwarding транзитного узла в три раза превышает время приветствия главного узла, чтобы гарантировать, что главный узел сможет обнаружить восстановление кольцевой сети до того, как транзитный порт войдет в режим пересылки. Если время приветствия, настроенное на главном узле, превышает время Pre-Forwarding транзитного узла, легко генерируется петля и запускается широковещательный шторм.
- Пользователи не могут устанавливать Edge Hello-time и Edge Fail-time. Их значения по умолчанию определяются значениями Hello-time и Fail-time соответственно и составляют 1/3 от этих значений.
- Физический интерфейс (Fast-Ethernet, Gigabit-Ethernet) и логический интерфейс агрегации можно настроить в качестве кольцевого порта. Если на физическом интерфейсе уже настроены агрегация, 802.1X или безопасность портов, этот физический интерфейс нельзя настроить в качестве кольцевого.

- Протокол MEAPS аналогичен исходному EAPS по функциям, но топология его кольца обладает большей расширяемостью и гибкостью. Следовательно, MEAPS и EAPS частично совместимы, и можно выполнить настройку с пересечением колец MEAPS и EAPS.

31.5.2 Настройка главного узла

Для настройки коммутатора в качестве главного узла кольцевой сети, выполните следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **mether-ring** *id1* **domain** *id2*	Устанавливает узел и входит в режим настройки узла. *id1*: идентификатор экземпляра узла; *id2*: идентификатор экземпляра домена (опускается, если он равен 0)
Switch_config_ring1# **master-node**	Обязательно. Настраивает тип узла как главный узел
Switch_config_ring1# **major-ring** [**sub-ring**]	Обязательно. Настраивает уровень узла в качестве одного из узлов основного кольца или подкольца
Switch_config_ring1# **control-vlan** *vlan-id*	Обязательно. Настраивает управляющую VLAN и создает VLAN ID и VLAN ID+1. *vlan-id*: идентификатор управляющей VLAN
Switch_config_ring1# **hello-time** *value*	Необязательно. Настраивает интервал передачи главным узлом пакетов HEALTH. *value*: это значение времени в диапазоне от 1 до 10 секунд, значение по умолчанию – 3 секунды
Switch_config_ring1# **fail-time** *value*	Необязательно. Настраивает время, в течение которого вторичный порт будет ожидать пакетов HEALTH. *value*: значение времени в диапазоне от 3 до 30 секунд, значение по умолчанию – 3 секунды
Switch_config_ring1# **exit**	Сохранение текущих настроек и выход из режима настройки узла
Switch_config#	

- Команда **no mether-ring** *id* **domain** *id2* используется для удаления настроек узла и настроек порта узла.
- Основное кольцо и подкольцо должны быть настроены с использованием одной и той же виртуальной локальной сети – VLAN управления основного

кольца. После настройки VLAN управления основного кольца и VLAN управления подкольца будут действовать на основном кольце одновременно.

31.5.3 Настройка транзитного узла

Для настройки коммутатора в качестве транзитного узла кольцевой сети, выполните следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **mether-ring** *id1* **domain** *id2*	Устанавливает узел и входит в режим настройки узла. *id1*: идентификатор экземпляра узла; *id2*: идентификатор экземпляра домена (опускается, если он равен 0)
Switch_config_ring1# **transit-node**	Обязательно. Настраивает тип узла как транзитный узел
Switch_config_ring1# **major-ring** [**sub-ring**]	Обязательно. Настраивает уровень узла в качестве одного из узлов основного кольца или подкольца
Switch_config_ring1# **control-vlan** *vlan-id*	Обязательно. Настраивает управляющую VLAN и создает VLAN ID и VLAN ID+1. *vlan-id*: идентификатор управляющей VLAN
Switch_config_ring1# **pre-forward-time** *value*	Необязательно. Настраивает время поддержания состояния Pre-Forwarding на транзитном порту. *value*: значение времени в диапазоне от 3 до 30 секунд, значение по умолчанию – 9 секунд
Switch_config_ring# **exit**	Сохранение текущих настроек и выход из режима настройки узла
Switch_config#	

31.5.4 Настройка граничного и вспомогательного узлов

Для настройки коммутатора в качестве граничного или вспомогательного узла, выполните следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **mether-ring** *id1* **domain** *id2*	Устанавливает узел и входит в режим настройки узла. *id1*: идентификатор экземпляра узла; *id2*: идентификатор экземпляра домена (опускается, если он равен 0)

Switch_config_ring1# **edge-node** [**assistant-node**]	Обязательно. Устанавливает тип узла как граничный/вспомогательный узел
Switch_config_ring1# **sub-ring**	Этот шаг можно пропустить. Граничный узел должен быть узлом подкольца
Switch_config_ring1# **control-vlan** *vlan-id*	Обязательно. Настраивает управляющую VLAN и создает VLAN ID и VLAN ID+1. *vlan-id*: идентификатор управляющей VLAN
Switch_config_ring1# **pre-forward-time** *value*	Необязательно. Настраивает время поддержания состояния Pre-Forwarding на граничном порту. *value*: значение времени в диапазоне от 3 до 30 секунд, значение по умолчанию – 9 секунд
Switch_config_ring1# **exit**	Сохранение текущих настроек и выход из режима настройки узла
Switch_config#	

31.5.5 Настройка режима подкольца

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **mether-ring** *id1* **domain** *id2*	Устанавливает узел и входит в режим настройки узла. *id1*: идентификатор экземпляра узла; *id2*: идентификатор экземпляра домена (опускается, если он равен 0)
Switch_config_ring1# **edge-node** [**assistant-node**]	Обязательно. Устанавливает тип узла как граничный/вспомогательный узел
Switch_config_ring1# **sub-ring**	Этот шаг можно пропустить. Граничный узел должен быть узлом подкольца
Switch_config_ring1# **control-vlan** *vlan-id*	Обязательно. Настраивает управляющую VLAN и создает VLAN ID и VLAN ID+1. *vlan-id*: идентификатор управляющей VLAN
Switch _config_ring2# **single-subring-mode**	Обязательно. Настройку кольца можно завершить без использования этой команды, но тогда подкольцо будет недоступно. В режиме подкольца механизм проверки канала протокола подкольца не может работать в главном кольце, и в этом режиме нельзя использовать сетевую конфигурацию с двойным подключением (dual homing). Эта команда применима только для граничного и вспомогательного узлов

Switch_config_ring1# **pre-forward-time** *value*	Необязательно. Настраивает время поддержания состояния Pre-Forwarding на граничном порту. *value*: значение времени в диапазоне от 3 до 30 секунд, значение по умолчанию – 9 секунд
Switch_config_ring1#**exit**	Сохранение текущих настроек и выход из режима настройки узла
Switch_config#	

31.5.6 Настройка кольцевого порта

Чтобы настроить порт коммутатора в качестве порта кольца Ethernet, выполните следующие действия:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **interface** *intf-name*	Вход в режим настройки интерфейса. *intf-name*: обозначает имя интерфейса
Switch_config_intf# **mether-ring** *id1* **domain** *id2* **primary-port** [**secondary-port** | **transit-port** | **common-port** | **edge-port**]	Настраивает тип кольцевого порта. *id1*: идентификатор экземпляра узла; *id2*: идентификатор экземпляра домена (опускается, если он равен 0)
Switch_config_intf# **exit**	Сохранение текущих настроек и выход из режима настройки узла

Форма **no** команды **mether-ring** используется для удаления соответствующих настроек кольцевого порта.

31.5.7 Просмотр состояния протокола

Выполните следующую команду, чтобы просмотреть состояние кольцевого протокола:

Команда	Описание
show mether-ring	Отображает сводную информацию о протоколе и портах кольца
show mether-ring *id1* **domain** *id2*	Отображает сводную информацию о протоколе выбранного кольца и портах кольца. *id1*: идентификатор экземпляра узла *id2*: идентификатор экземпляра домена (опускается, если он равен 0)

show mether-ring *id1* **domain** *id2* **detail**	Отображает детальную информацию о протоколе выбранного кольца и портах кольца
show mether-ring *id1* **domain** *id2* **interface** *intf-name*	Отображает состояние кольцевого или общего порта

31.6 Порядок работы MEAPS

MEAPS использует три механизма защиты для поддержки структуры с одним кольцом или структуры с несколькими кольцами 2-го уровня. В следующих разделах показаны детали работы MEAPS и изменения топологии MEAPS на типичных примерах, от замкнутого состояния до состояния отключения связи, затем до восстановления и, наконец, снова до замкнутого состояния.

31.6.1 Целостная кольцевая топология

Замкнутое состояние кольца контролируется и поддерживается механизмом опроса. В замкнутом кольце все каналы находятся в состоянии UP, и контролируются главным узлом. Чтобы предотвратить широковещательный шторм, главный узел блокирует свой вторичный порт для данных. В то же время главный узел будет периодически передавать пакеты Hello со своего основного порта. Эти пакеты последовательно пройдут через транзитный узел и, наконец, вернутся к главному узлу через его вторичный порт. Целостная кольцевая топология показана на рисунке 31-11. Основное кольцо и два подкольца находятся в замкнутом состоянии. Пакет Hello основного кольца транслируется только в основном кольце, в то время как пакет Hello подкольца может быть прозрачно передан через главное кольцо, затем вернуться в подкольцо и, наконец, достичь вторичного порта главного узла подкольца.

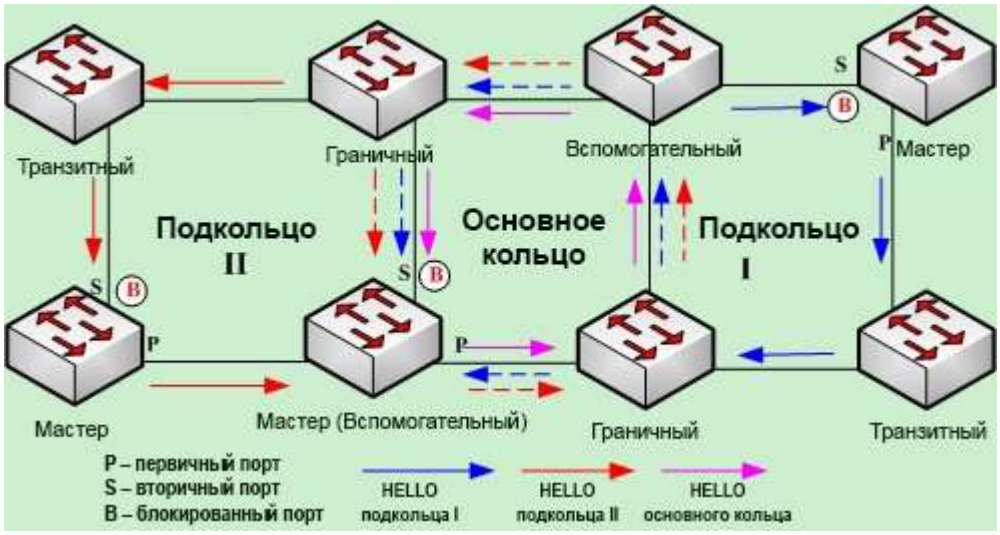

Рисунок 31-11 – Целостная кольцевая топология

31.6.2 Разрыв связи

Разрыв связи в кольце определяется механизмом опроса, уведомлением об изменении состояния канала и механизмом проверки состояния канала пакетов протокола подкольца. Когда какой-либо канал в кольце прерывается, кольцо переходит из замкнутого состояния в разомкнутое, то есть в состояние отсутствия связи (link-down).

Если на канале происходит разрыв соединения, будут работать как механизм опроса, так и механизм уведомления об изменении статуса канала. Транзитный узел, на котором прекратилось соединение, передаст пакет уведомления Link-down главному узлу через рабочий порт на другой своей стороне; в то же время механизм опроса будет отслеживать и оперативно изменять состояние кольца через интервал Fail-time. При возникновении неисправности в канале протокола подкольца она будет обрабатываться механизмом проверки состояния канала на основном кольце. Как показано на рисунке 31-12, сообщение уведомления о неисправности на канале основного кольца и на общем канале передается только на основном кольце и, наконец, приходит на главный узел; сообщение о проблеме на связи в подкольце 2 будет передано главному узлу этого подкольца и может быть прозрачно передано через основное кольцо без изменений.

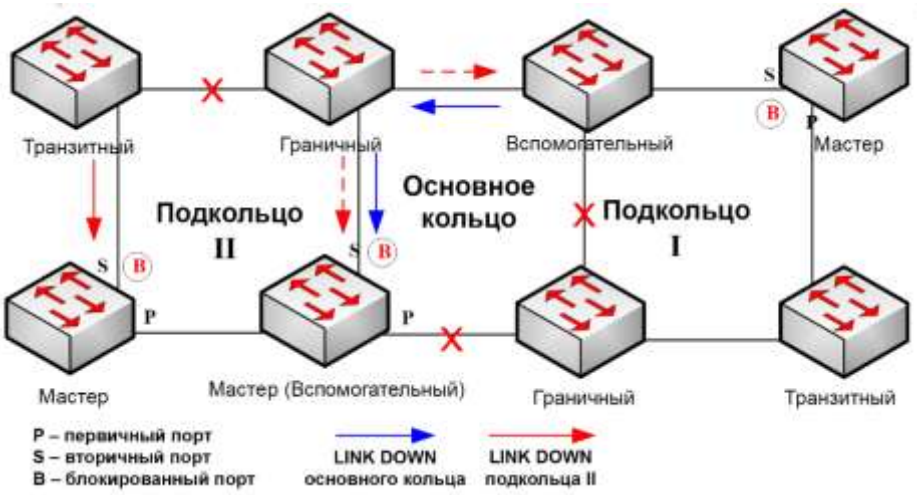

Рисунок 31-12 – Уведомление главного узла о неисправности

После того, как главный узел получит пакет Link-down, он перейдет в состояние сбоя и откроет вторичный порт. Таблица FDB будет обновлена, а пакеты RING-DOWN-FLUSH-FDB будут передаваться с двух портов для уведомления всех узлов. Как показано на рисунке 31-13, главный узел основного кольца уведомляет транзитный узел основного кольца об обновлении FDB. На канале подкольца 1 возникли проблемы, поэтому граничный порт вспомогательного узла будет заблокирован. Главный узел подкольца 2 уведомляет транзитные узлы подкольца о необходимости обновления FDB, после чего прозрачная передача будет осуществляться по основному кольцу.

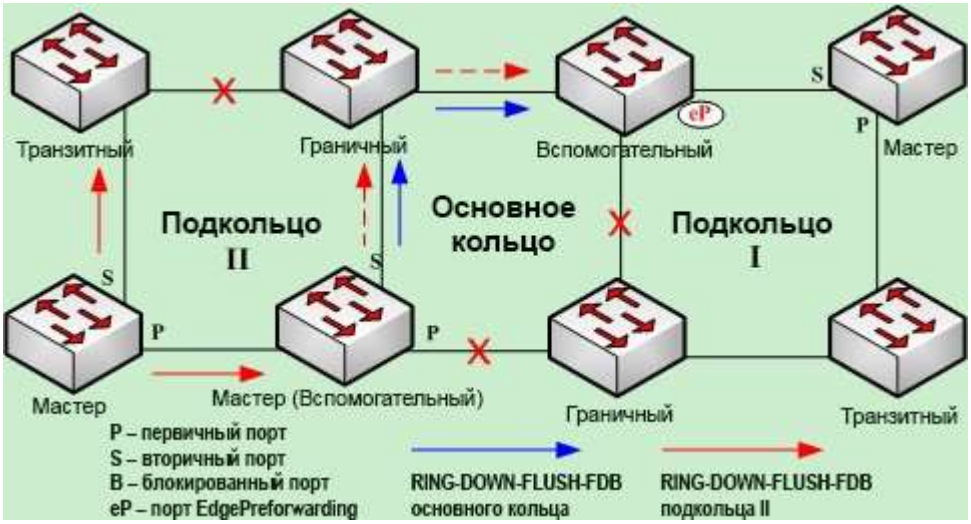

Рисунок 31-13 – Уведомление о неисправности и обновление FDB

31.6.3 Восстановление

Когда порт на транзитном узле будет восстановлен, транзитный узел перейдет в состояние Pre-Forwarding. Процедура обработки при восстановлении порта транзитного узла показана на рисунке 31-14. Канал основного кольца восстановится, транзитный узел, соединяющий канал основного кольца, перейдет в состояние Pre-Forwarding, блокирует пакеты данных, но будет пропускать пакеты управления Hello; аналогично, транзитный узел на подкольце 2 также переходит в состояние Pre-Forwarding; когда пакет Hello на подкольце 1 достигает граничного узла, из-за того, что возобновленный транзитный узел пропускает только управляющий пакет основного кольца и что пакет Hello подкольца 1 аналогичен пакету данных основного кольца, этот пакет Hello не может быть перенаправлен.

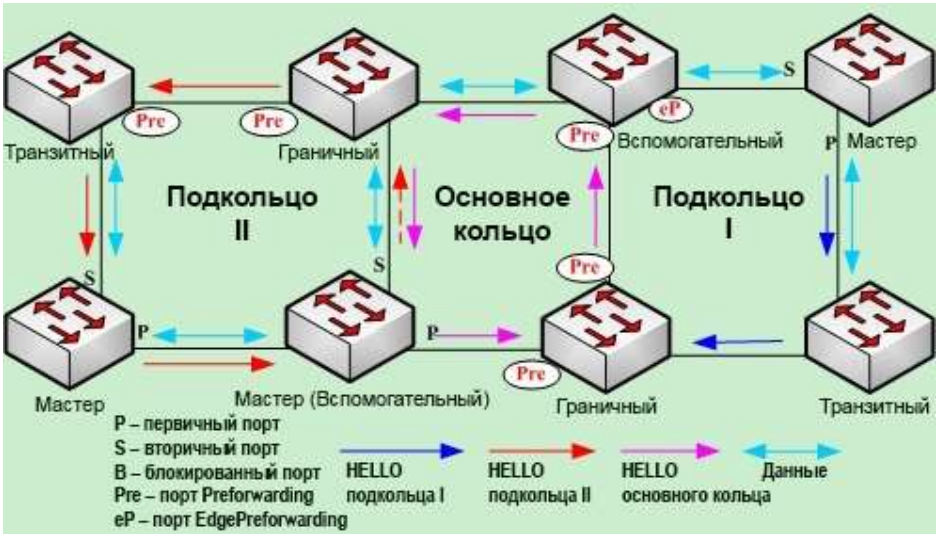

Рисунок 31-14 – Восстановление канала кольца и перевод транзитного узла режим Pre-Forwarding

Транзитный порт может передавать пакет управления в состоянии Pre-Forwarding, поэтому вторичный порт главного узла получает пакет Hello от первичного порта. Следовательно, главный узел меняет свое состояние на COMPLETE, блокирует вторичный порт и передает пакет RING-UP-FLUSH-FDB из первичного порта. После того, как транзитный узел получит пакет RING-UP-FLUSH-FDB, транзитный узел вернется в состояние Link-Up, откроет заблокированный порт и обновит таблицу FDB. Процедура восстановления кольца показана на рисунке 31-15. Главный узел на основном кольце переходит в состояние COMPLETE, блокирует вторичный порт, передает пакет RING-UP-FLUSH-FDB всем транзитным узлам на главном кольце, что вынуждает их вернуться в состояние Link-Up, открыть заблокированные порты и обновить таблицы FDB. Аналогично, транзитный узел и главный узел на подкольце 2 также проводят соответствующие изменения. Из-за восстановления канала протокола подкольца, на подкольце 1 вторичный порт главного узла может получить пакет Hello от первичного порта, и главный узел переводит свое состояние обратно состояние COMPLETE, блокирует вторичный порт, передает пакет RING-UP-FLUSH-FDB, благодаря чему вспомогательный узел открывает граничный порт. Таким образом подкольцо 1 возвращается к целостному состоянию.

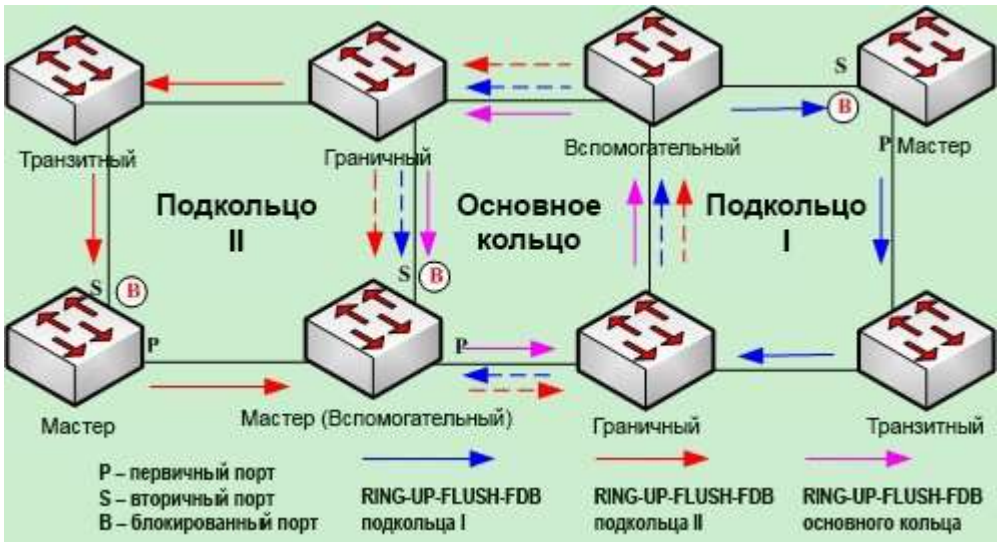

Рисунок 31-15 – Восстановление кольца

Если транзитный узел в состоянии Pre-Forwarding не получает пакет RING-UP-FLUSH-FDB и интервал Fail-time превышается, он откроет заблокированный транзитный порт и возобновит передачу данных.

31.7 Примеры настройки MEAPS

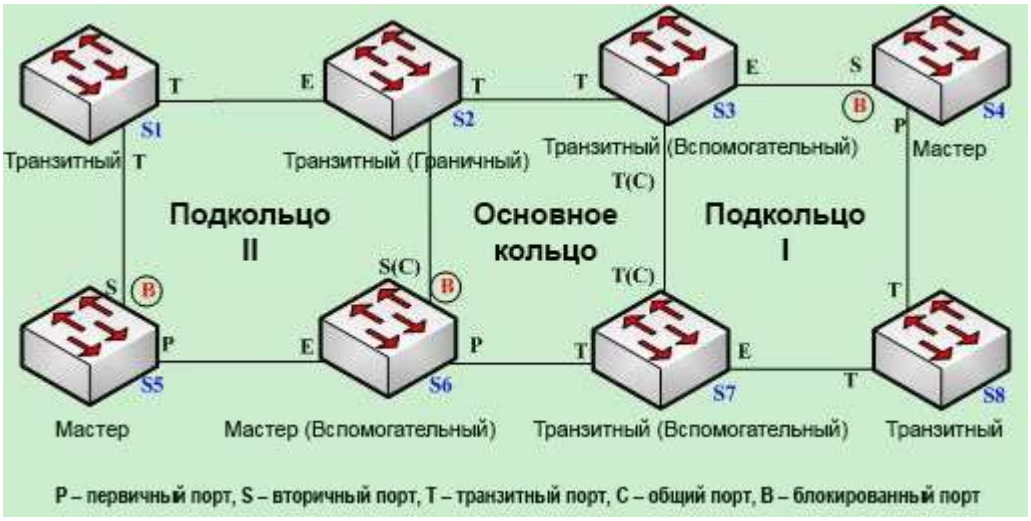

Рисунок 31-16 – Топология MEAPS

Главный узел S1 и транзитный узел S2 на рисунке 31-16 настроены как описано ниже. Что касается настроек остальных узлов, то они аналогичны настройкам S2.

Настройка коммутатора S1

Следующие команды используются для настройки транзитного узла подкольца, узла 2:

Switch_config# mether-ring 2 domain 1

Switch_config_ring2# transit-node

Switch_config_ring2# sub-ring

Switch_config_ring2# control-vlan 2

Для установки параметра времени используются следующая команда:

Switch_config_ring2# pre-forward-time 12

Выход из режима настройки узла:

Switch_config_ring2#quit

Для настройки транзитного порта узла 2 используются следующие команды:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# mether-ring 2 domain 1 transit-port

Switch_config_g0/1# switchport mode trunk

Switch_config_g0/1# quit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 2 domain 1 transit-port

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# quit

Настройка коммутатора S2

Следующие команды используются для настройки транзитного узла основного кольца, узла 1:

Switch_config# mether-ring 1 domain 1

Switch_config_ring1# transit-node

Switch_config_ring1# major-ring

Switch_config_ring1# control-vlan 2

Для установки параметра времени используются следующая команда:

Switch_config_ring1# pre-forward-time 12

Выход из режима настройки узла:

Switch_config_ring1# quit

Для настройки транзитного порта узла 1 используются следующие команды:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# mether-ring 1 domain 1 transit-port

Switch_config_g0/1# switchport mode trunk

Switch_config_g0/1# quit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 1 domain 1 transit-port

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# quit

Следующие команды используются для настройки граничного узла подкольца, узла 2:

Switch_config# mether-ring 2 domain 1

Switch_config_ring2# edge-node

Switch_config_ring2# sub-ring *(этот шаг можно пропустить)*

Switch_config_ring2# control-vlan 2

Для установки параметра времени используются следующая команда:

Switch_config_ring2# pre-forward-time 12

Выход из режима настройки узла:

Switch_config_ring2# quit

Следующие команды используются для настройки общего порта и граничного порта узла 2:

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 2 domain 1 common-port

Switch_config_g0/2#quit

Switch_config# interface gigaEthernet 0/3

Switch_config_g0/3# mether-ring 2 domain 1 edge-port

Switch_config_g0/3# switchport mode trunk

Switch_config_g0/3# quit

Настройка коммутатора S3

Следующие команды используются для настройки транзитного узла основного кольца, узла 1:

Switch_config# mether-ring 1 domain 1

Switch_config_ring1# transit-node

Switch_config_ring1# major-ring

Switch_config_ring1# control-vlan 2

Для установки параметра времени используются следующая команда:

Switch_config_ring1# pre-forward-time 12

Выход из режима настройки узла:

Switch_config_ring1# quit

Для настройки транзитного порта узла 1 используются следующие команды:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# mether-ring 1 domain 1 transit-port

Switch_config_g0/1# switchport mode trunk

Switch_config_g0/1# quit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 1 domain 1 transit-port

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# quit

Следующие команды используются для настройки вспомогательного узла подкольца, узла 4:

Switch_config# mether-ring 4 domain 1

Switch_config_ring4# assistant-node

Switch_config_ring4# sub-ring (*этот шаг можно пропустить*)

Switch_config_ring4# control-vlan 2

Для установки параметра времени используются следующая команда:

Switch_config_ring4# pre-forward-time 12

Выход из режима настройки узла:

Switch_config_ring4# quit

Следующие команды используются для настройки общего порта и граничного порта узла 2:

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 4 domain 1 common-port

Switch_config_g0/2# quit

Switch_config# interface gigaEthernet 0/3

Switch_config_g0/3# mether-ring 4 domain 1 edge-port

Switch_config_g0/3# switchport mode trunk

Switch_config_g0/3# quit

Настройка коммутатора S4

Следующие команды используются для настройки главного узла подкольца, узла 4:

Switch_config# mether-ring 4 domain 1

Switch_config_ring4# master-node

Switch_config_ring4# sub-ring

Switch_config_ring4# control-vlan 2

Следующие команды используются для установки временных параметров:

Switch_config_ring4# hello-time 4
Switch_config_ring4# fail-time 12

Выход из режима настройки узла:

Switch_config_ring4# quit

Следующие команды используются для настройки первичного и вторичного портов узла 4:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# mether-ring 4 domain 1 primary-port

Switch_config_g0/1# switchport mode trunk

Switch_config_g0/1# quit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 4 domain 1 secondary-port

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# quit

Настройка коммутатора S5

Следующие команды используются для настройки главного узла подкольца, узла 2:

Switch_config# mether-ring 2 domain 1

Switch_config_ring2# master-node

Switch_config_ring2# sub-ring

Switch_config_ring2# control-vlan 2

Следующие команды используются для установки временных параметров:

Switch_config_ring2# hello-time 4

Switch_config_ring2# fail-time 12

Выход из режима настройки узла:

Switch_config_ring2# quit

Следующие команды используются для установки первичного и вторичного портов узла 2:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# mether-ring 2 domain 1 primary-port

Switch_config_g0/1# switchport mode trunk

Switch_config_g0/1# quit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 2 domain 1 secondary-port

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# quit

Настройка коммутатора S6

Следующие команды используются для настройки главного узла основного кольца, узла 1:

Switch_config# mether-ring 1 domain 1

Switch_config_ring1# master-node

Switch_config_ring1# major-ring

Switch_config_ring1# control-vlan 2

Следующие команды используются для установки временных параметров:

Switch_config_ring1# hello-time 4

Switch_config_ring1# fail-time 12

Выход из режима настройки узла:

Switch_config_ring1# quit

Для настройки транзитного порта узла 1 используются следующие команды:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# mether-ring 1 domain 1 primary-port

Switch_config_g0/1# switchport mode trunk

Switch_config_g0/1# quit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 1 domain 1 secondary-port

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# quit

Следующие команды используются для настройки вспомогательного узла подкольца, узла 2:

Switch_config# mether-ring 2 domain 1

Switch_config_ring2# assistant-node

Switch_config_ring2# sub-ring (*этот шаг можно пропустить*)

Switch_config_ring2# control-vlan 2

Для установки параметра времени используются следующая команда:

Switch_config_ring2# pre-forward-time 12

Выход из режима настройки узла:

Switch_config_ring2# quit

Следующие команды используются для настройки общего порта и граничного порта узла 2:

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 2 domain 1 common-port

Switch_config_g0/2# quit

Switch_config# interface gigaEthernet 0/3

Switch_config_g0/3# mether-ring 2 domain 1 edge-port

Switch_config_g0/3# switchport mode trunk

Switch_config_g0/3# quit

Настройка коммутатора S7

Следующие команды используются для настройки транзитного узла основного кольца, узла 1:

Switch_config# mether-ring 1 domain 1

Switch_config_ring1# transit-node

Switch_config_ring1# major-ring

Switch_config_ring1# control-vlan 2

Для установки параметра времени используются следующая команда:

Switch_config_ring1# pre-forward-time 12

Выход из режима настройки узла:

Switch_config_ring1# quit

Для настройки транзитного порта узла 1 используются следующие команды:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# mether-ring 1 domain 1 transit-port

Switch_config_g0/1# switchport mode trunk

Switch_config_g0/1# quit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 1 domain 1 transit-port

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# quit

Следующие команды используются для настройки вторичного порта узла 4:

Switch_config# mether-ring 4 domain 1

Switch_config_ring4# edge-node

Switch_config_ring4# sub-ring (*этот шаг можно пропустить*)

Switch_config_ring4# control-vlan 2

Для установки параметра времени используются следующая команда:

Switch_config_ring4# pre-forward-time 12

Выход из режима настройки узла:

Switch_config_ring4# quit

Следующие команды используются для настройки общего порта и граничного порта узла 2:

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# mether-ring 4 domain 1 common-port

Switch_config_g0/2# quit

Switch_config# interface gigaEthernet 0/3

Switch_config_g0/3# mether-ring 4 domain 1 edge-port

Switch_config_g0/3# switchport mode trunk

Switch_config_g0/3# quit

Настройка коммутатора S8

Следующие команды используются для настройки транзитного узла подкольца, узла 4:

Switch_config# mether-ring 4 domain 1

Switch_config_ring4# transit -node

Switch_config_ring4# sub-ring

Switch_config_ring4# control-vlan 2

Для установки параметра времени используются следующая команда:

Switch_config_ring4# pre-forward-time 12

Выход из режима настройки узла:

Switch_config_ring4# quit

Для настройки транзитного порта узла 4 используются следующие команды:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# mether-ring 4 domain 1 transit-port

Switch_config_g0/1# switchport mode trunk

Switch_config_g0/1# quit

```
Switch_config# interface gigaEthernet 0/2
Switch_config_g0/2# mether-ring 4 domain 1 transit -port
Switch_config_g0/2# switchport mode trunk
Switch_config_g0/2# quit
```

31.8 Незавершенные настройки

Незавершенная настройка базовой информации: не настроена одна из ролей кольца, уровень кольца и управляющая VLAN. Одним из исключительных случаев является то, что, когда роль узла настроена как граничный или вспомогательный узел, уровень кольца по умолчанию будет подкольцом.

Противоречие базовой информации: когда роль узла – граничный или вспомогательный узел, уровень кольца по умолчанию – подкольцо; если уровень кольца установлен как основное кольцо, появится информационное сообщение.

Подкольцо, не имеющее соответствующего узла основного кольца: если роль узла – граничный или вспомогательный, этот узел переносится на узел основного кольца; если нет соответствующего узла основного кольца для принудительного создания граничного или вспомогательного узла подкольца, появится информационное сообщение. В этом случае можно использовать команду **show** для просмотра состояния MEAPS; если вы обнаружите, что базовая информация заполнена, но состояние – init, это указывает на то, что настройка узла кольца не завершена.

Конфликты, возникающие во время настройки управляющей VLAN: если управляющая VLAN, настроенная узлом, конфликтует с другими настроенными узлами, появится информационное сообщение. В этом случае можно использовать команду **show** для просмотра состояния MEAPS; если вы обнаружите, что базовая информация заполнена, но состояние – init, это указывает на то, что настройка узла кольца не завершена.

При настройке узла подкольца на основе настроек узла основного кольца, идентификатор узла подкольца должен быть больше, чем идентификатор узла основного кольца. В противном случае появится информационное сообщение с подсказкой.

32. UDLD

32.1 Обзор

UDLD (Unidirectional Link Detection) – это протокол 2-го уровня, который отслеживает физическое состояние кабеля через устройства, подключенные по оптическому кабелю или витой паре, и определяет, существует ли однонаправленное соединение. Для работы протокола необходима его поддержка подключенными устройствами. Целью использования UDLD является предотвращение проблем, связанных с однонаправленными связями, такими как петли в STP. Следовательно, при обнаружении однонаправленного канала UDLD отключит затронутый интерфейс и уведомит пользователей.

UDLD работает с механизмом протокола физического уровня для оценки состояния канала. На физическом уровне автоматически согласовываются и обрабатываются физические сигналы и ошибки обнаружения, в то время как UDLD отвечает за обнаружение идентификаторов соседних устройств и отключение неправильных сетевых соединений. При включении автоматической настройки и применении UDLD можно предотвратить проблемы, связанные с физическими и логическими соединениями, а также с другими протоколами.

32.1.1 Режим UDLD

Протокол UDLD имеет два режима: нормальный (по умолчанию) и агрессивный. В нормальном режиме он обнаруживает однонаправленные связи на основе характеристик соединения. В агрессивном режиме, кроме обнаружения однонаправленных связей, он также способен обнаружить прерывание соединения, которое не может быть выявлено протоколами 1-го уровня.

В нормальном режиме, если UDLD определяет, что соединение пропало, он меняет состояние порта на неопределенное (undetermined), а не отключенное (down). В агрессивном режиме, если UDLD определяет, что канал пропал и его невозможно повторно подключить, это рассматривается как серьезная проблема с сетью, и UDLD поменяет состояние протокола на linkdown, а порт перейдет в состояние отключения из-за ошибки (errdisable). Независимо от режима, если UDLD определяет, что соединение является двунаправленным, порт будет настроен на двунаправленный режим (bidirectional).

В агрессивном режиме UDLD может обнаружить следующие случаи однонаправленного соединения:

- по оптоволоконному кабелю или витой паре интерфейс не может принимать или передавать информацию;
- в оптоволокне или витой паре интерфейс одного терминала выключен, а другого – включен;
- одна линия оптического кабеля повреждена, в связи с чем данные могут только передаваться или только приниматься.

В этих случаях UDLD отключает затронутый интерфейс.

32.1.2 Механизм работы

UDLD – это протокол L2, работающий на уровне LLC, который использует 01-00-0c-cc-cc-cc в качестве MAC-адреса назначения. SNAP HDLC аналогичен 0x0111. Когда он работает с FEFI 1-го уровня и автоматическим согласованием, целостность канала может быть проверена на физическом и логическом уровне.

UDLD предоставляет некоторые функции, которые не могут выполнять FEFI и автоматическое согласование, такие как проверка и кэширование информации о соседях, отключение любого неправильно настроенного порта, а также проверка неисправностей и аннулирование логических портов, за исключением логических портов «точка-точка».

UDLD использует два основных механизма: изучение информации о соседях и сохранение ее в локальном кэше. Когда обнаруживается новый сосед или сосед снова подает заявку на синхронизацию кэша, будет передана серия зондирующих эхо-пакетов UDLD (Hello).

UDLD передает зондирующие пакеты на все порты, и когда на портах принимается эхо-информация UDLD, запускается фаза обнаружения и процесс аутентификации. Если все действующие условия соблюдены (порт подключен в двух направлениях и кабель подключен правильно), этот порт будет включен. В противном случае порт будет недоступен.

Как только соединение будет установлено и помечено как двунаправленное, UDLD будет передавать эхо-сообщение Hello каждые 15 секунд.

32.1.3 Состояние порта

Интерфейс UDLD может находиться в одном из следующих состояний:

Состояние порта	Описание
Обнаружение (detection)	Означает, что интерфейс находится в состоянии обнаружения
Неизвестное (unknown)	Означает, что интерфейс находится в неизвестном состоянии, то есть, либо он может находиться в состоянии обнаружения, либо не проводил обнаружение
Однонаправленное (unidirectional)	Означает, что обнаружено однонаправленное соединение
Двунаправленное (bidirectional)	Означает, что обнаружено двунаправленное соединение

32.1.4 Поддержание кэша соседнего устройства

UDLD регулярно передает эхо-пакеты на каждом активном интерфейсе, чтобы поддерживать полноту кэша соседнего устройства. После получения сообщения Hello оно будет временно сохранено в памяти, а также будет сохранен интервал, определяемый временем удержания (hold-time). Если время удержания истекает, соответствующий кэш полностью очищается. Если во время удержания будет получено новое сообщение Hello, новое сообщение Hello заменит старое, и таймер будет сброшен на ноль.

После отключения интерфейса, на котором работает UDLD, или перезапуска устройства на интерфейсе все кэши интерфейса будут удалены. UDLD передает по крайней мере одно сообщение, чтобы уведомить соседа об удалении соответствующих элементов кэша.

32.1.5 Обнаружение при помощи эха

Механизм эха является основой алгоритма обнаружения. Как только устройство UDLD узнает о существовании нового соседа или получает запрос синхронизации от асинхронного соседа, оно запускает или перезапускает окно обнаружения локального терминала и передает эхо-сообщение для согласования данных. Поскольку всем соседним устройствам требуется соответствующее действие, отправитель эхо-сообщения ожидает отклика. Если окно проверки закрылось до того, как было получено правильное эхо, эта связь считается однонаправленной. В этом случае будет запущено переподключение канала или процесс отключения связи на порту.

32.2 Настройка UDLD

Задачи настройки

- Глобальное включение или отключение UDLD
- Включение или отключение интерфейса UDLD
- Настройка интервала сообщений в агрессивном режиме
- Перезапуск отключенного с помощью UDLD интерфейса
- Отображение состояния UDLD

32.2.1 Глобальное включение или отключение UDLD

В режиме глобальной конфигурации выполните следующую команду, чтобы включить функцию UDLD для всех интерфейсов:

Команда	Описание
udld [**enable** | **aggressive**]	Включает модули UDLD всех интерфейсов в определенном режиме

В режиме глобальной конфигурации выполните следующую команду, чтобы отключить функцию UDLD всех интерфейсов:

Команда	Описание
no udld [**enable** | **aggressive**]	Выключает модули UDLD всех интерфейсов

- Если вы включите или отключите функцию UDLD в глобальной конфигурации, команда будет выполняться на всех интерфейсах.
- Агрессивный режим UDLD может предоставлять дополнительные преимущества. Когда UDLD находится в агрессивном режиме и порт прекращает передачу UDLD-пакетов, протокол снова попытается установить соединение с соседним устройством. Если количество попыток превышает определенное число, состояние порта меняется на Error-Disable, и связь на порту прекращается.
- При включенном UDLD порты на обоих терминалах должны работать в одном и том же режиме, иначе ожидаемый результат не будет достигнут.

32.2.2 Включение или отключение интерфейса UDLD

В режиме настройки интерфейса выполните следующую команду, чтобы включить функцию UDLD на интерфейсе:

Команда	Описание
udld port [**aggressive**]	Включает модуль UDLD интерфейса в определенном режиме. Если параметр **aggressive** не введен, функция UDLD интерфейса включается в нормальном режиме; если введен параметр **aggressive**, функция UDLD интерфейса включается в агрессивном режиме

В режиме настройки интерфейса выполните следующую команду, чтобы отключить функцию UDLD на интерфейсе:

Команда	Описание
no udld port [**aggressive**]	Отключает модуль UDLD интерфейса путем ввода соответствующей команды в определенном режиме

32.2.3 Настройка интервала сообщений в агрессивном режиме

В режиме глобальной конфигурации выполните следующую команду, чтобы установить интервал сообщений агрессивного режима:

Команда	Описание
udld message *time*	Устанавливает временной интервал сообщений агрессивного режима

32.2.4 Перезапуск отключенного с помощью UDLD интерфейса

В режиме EXEC выполните следующую команду, чтобы перезапустить интерфейс, отключенный модулем UDLD:

Команда	Описание
udld reset	Перезапускает интерфейс, отключенный модулем UDLD

32.2.5 Отображение состояния UDLD

Запустите следующую команду, чтобы отобразить состояния модулей UDLD всех текущих интерфейсов:

Команда	Описание
show udld	Отображает состояния модулей UDLD всех текущих интерфейсов

Выполните следующую команду, чтобы отобразить состояние модуля UDLD указанного интерфейса:

Команда	Описание
show udld *interface*	Отображает состояние модуля UDLD указанного интерфейса

Команда отображения UDLD используется для просмотра состояния и режима UDLD, текущего состояния обнаружения, а также состояния канала и некоторой информации о соседних устройствах.

- Эта команда используется для отображения рабочих состояний модулей UDLD текущих интерфейсов:

```
Switch# show udld


Interface FastEthernet0/1

---
```

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Bidirectional

Current operational state: Advertisement

Message interval: 15

Time out interval: 5

Entry 1

Expiration time: 42

Cache Device index: 1

Device ID: CAT0611Z0L9

Port ID: FastEthernet0/1

Neighbor echo 1 device: S35000202

Neighbor echo 1 port: FastEthernet0/1

Message interval: 15

Time out interval: 5

UDLD Device name: Switch

Interface FastEthernet0/2

Port enable administrative configuration setting: Disabled

Port enable operational state: Disabled

Current bidirectional state: Unknown

Interface FastEthernet0/3

Port enable administrative configuration setting: Disabled

Port enable operational state: Disabled

Current bidirectional state: Unknown

……

- Эта команда используется для отображения рабочего состояния модуля UDLD текущего интерфейса:

```
Switch# show udld interface f0/1

Interface FastEthernet0/1

---

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Bidirectional

Current operational state: Advertisement

Message interval: 15

Time out interval: 5

    Entry 1

    ---

    Expiration time: 42

    Cache Device index: 1

    Device ID: CAT0611Z0L9

    Port ID: FastEthernet0/1

    Neighbor echo 1 device: S35000202

    Neighbor echo 1 port: FastEthernet0/1


    Message interval: 15

    Time out interval: 5

    UDLD Device name: Switch
```

32.3 Пример настройки

32.3.1 Требования к сетевой среде

Настройте протокол UDLD на портах, соединяющих коммутаторы A и B.

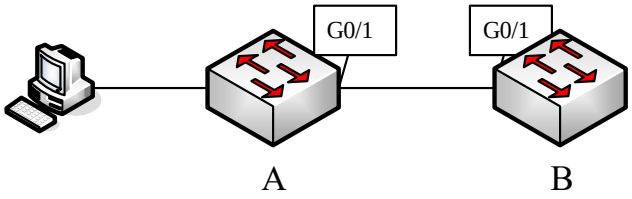

Рисунок 32-1 – Сетевая топология

32.3.2 Процедура настройки

Настройка коммутатора A

Switch_config# udld enable

Switch_config# interface g0/1

Switch_config_g0/1# udld port

Switch_config_g0/1# quit

Настройка коммутатора B

Switch_config# udld enable

Switch_config# interface g0/1

Switch_config_g0/1# udld port

Switch_config_g0/1# quit

Ввод команды **show** на коммутаторе A:

Switch_config# show udld interface g0/1

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Detection

Message interval: 15

Time out interval: 1

Entry 1

Expiration time: 44

Cache Device index: 1

Device ID: S35043000

Port ID: GigaEthernet0/1

Neighbor echo 1 device: S32030079

Neighbor echo 1 port: GigaEthernet0/1

Message interval: 15

Time out interval: 1

UDLD Device name: SwitchB

Switch_config#

Switch_config# show udld interface g0/1

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Advertisement

Message interval: 15

Time out interval: 7

Entry 1

Expiration time: 43

Cache Device index: 1

Device ID: S35043000

Port ID: GigaEthernet0/1

Neighbor echo 1 device: S32030079

Neighbor echo 1 port: GigaEthernet0/1

Message interval: 15

Time out interval: 7

UDLD Device name: SwitchB

Switch_config#

Switch_config# show udld interface g0/1

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Bidirectional

Current operational state: Advertisement

Message interval: 15

Time out interval: 15

Entry 1

Expiration time: 36

Cache Device index: 1

Device ID: S35043000

Port ID: GigaEthernet0/1

Neighbor echo 1 device: S32030079

Neighbor echo 1 port: GigaEthernet0/1

Message interval: 15

Time out interval: 15

UDLD Device name: SwitchB

Switch_config#

Из приведенной выше информации можно определить три фазы состояния связи, которые обнаруживает UDLD:

1. Фаза обнаружения. На этом этапе пакеты UDLD передаются каждую секунду.
2. Фаза неизвестности. На этой фазе пакеты UDLD передаются каждые восемь секунд.
3. Фаза известного двунаправленного/однонаправленного соединения: как только соединение установлено и помечено как двунаправленное, UDLD будет передавать эхо-сообщение каждые 16 секунд.

33. IGMP-Snooping

Задача IGMP-snooping – поддерживать связи между VLAN и групповым адресом и обновлять их одновременно с изменениями многоадресной рассылки, позволяя коммутаторам пересылать данные в соответствии со структурой топологии многоадресной группы.

Основные функции IGMP-snooping следующие:

- прослушивание сообщений IGMP;
- ведение таблицы соответствия между VLAN и групповыми адресами;
- синхронизация состояния между IGMP-сущностями хоста и маршрутизатора для предотвращения избыточного широковещательного трафика.

IGMP-snooping выполняет вышеуказанные функции, прослушивая запросы и сообщения об отчетах, отправляемые через протокол IGMP. Этот механизм может функционировать корректно только при условии, что он подключен к мультикастовому маршрутизатору. Другими словами, коммутатор должен периодически получать информацию о запросах IGMP от маршрутизатора. Для правильной работы IGMP-snooping необходимо установить таймер истечения срока действия данных маршрутизатора (router age timer) на значение, большее, чем период отправки запросов групп маршрутизатором, с которым связан IGMP-snooping. Вы можете проверить информацию о многоадресном маршрутизаторе в каждой виртуальной локальной сети, запустив команду **show ip igmp-snooping**.

33.1 Настройка IGMP-Snooping

Задачи настройки

- Включение/отключение IGMP-Snooping для VLAN
- Добавление/удаление статического мультикастового адреса VLAN
- Настройка немедленного выхода VLAN из группы
- Настройка немедленного выхода порта из группы

- Настройка интерфейса статической маршрутизации VLAN
- Настройка IPACL для создания таблицы многоадресной рассылки
- Настройка фильтрации многоадресных сообщений без зарегистрированного адреса назначения.
- Настройка таймера срока действия данных маршрутизатора IGMP-Snooping
- Настройка таймера ответов IGMP-Snooping
- Настройка генератора IGMP-запросов
- Настройка таймера запросов IGMP-Snooping
- Настройка функции forward-l3-to-mrouter
- Настройка чувствительного режима для IGMP-Snooping
- Настройка функции v3-leave-check
- Настройка функции forward-wrongiif-within-vlan
- Настройка функции IPACL на порту
- Настройка IGMP-фильтрации в VLAN
- Настройка максимального количества мультикастовых адресов на порту IGMP-Snooping
- Настройка функции подавления отчетов
- Настройка функции proxy-leave IGMP-Snooping
- Мониторинг и поддержка IGMP-Snooping
- Пример настройки IGMP-Snooping

33.1.1 Включение/отключение IGMP-Snooping для VLAN

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-snooping [**vlan** *vlan_id*]	Включает IGMP-Snooping для VLAN
no ip igmp-snooping [**vlan** *vlan_id*]	Восстанавливает настройки по умолчанию

Если VLAN не указана, все виртуальные сети в системе, включая созданные позже, можно включить или отключить.

В конфигурации по умолчанию включено отслеживание IGMP всех VLAN, так, как это делается при помощи команды **ip igmp-snooping**.

IGMP-Snooping может работать в 16 VLAN.

Чтобы включить IGMP-Snooping в VLAN3, необходимо сначала отключить эту функцию для всех VLAN при помощи команды **no ip igmp-snooping**, а затем запустить команду **ip igmp-snooping vlan 3** и сохранить конфигурацию.

33.1.2 Добавление/удаление статического мультикастового адреса VLAN

Хосты, не поддерживающие IGMP, могут получать соответствующие сообщения многоадресной рассылки, настроив статический мультикастовый адрес. Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Добавляет статический мультикастовый адрес VLAN
no ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Удаляет статический мультикастовый адрес VLAN

33.1.3 Настройка немедленного выхода VLAN из группы

Если настроена функция немедленного выхода, коммутатор может удалить VLAN из списка многоадресной группы после того, как получит сообщение о выходе. Таким образом, коммутатору не требуется включать таймер для ожидания подключения других хостов к многоадресной рассылке. Если другие хосты указанной VLAN принадлежат к той же группе и их пользователи не хотят покидать группу, это может повлиять на многоадресную связь этих пользователей. В этом случае функцию немедленного выхода включать не следует. Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-snooping vlan *vlan_id* **immediate-leave**	Настраивает функцию немедленного выхода VLAN из группы
no ip igmp-snooping vlan *vlan_id* **immediate-leave**	Устанавливает значение по умолчанию для функции немедленного выхода VLAN из группы

По умолчанию данная функция отключена.

33.1.4 Настройка немедленного выхода порта из группы

Если для порта настроена функция немедленного выхода, коммутатор может удалить порт из списка портов группы многоадресной рассылки после того, как получит сообщение о выходе. Таким образом, коммутатору не требуется включать таймер для ожидания подключения других хостов к многоадресной рассылке. Если другие хосты на том же порту принадлежат к той же группе и их пользователи не хотят покидать группу, это может повлиять на многоадресную связь этих пользователей. В этом случае функцию немедленного выхода включать не следует.

Включение функции немедленного выхода порта запускает также и функцию немедленного выхода VLAN.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-snooping immediate-leave	Настраивает функцию немедленного выхода порта из группы
no ip igmp-snooping immediate-leave	Возвращает настройки по умолчанию для функции немедленного выхода порта из группы

По умолчанию данная функция отключена.

33.1.5 Настройка интерфейса статической маршрутизации VLAN

Настройте интерфейс статической маршрутизации и отправьте на него многоадресный пакет. Коммутатор отправит пакеты отчетов многоадресной рассылки на все порты маршрутизации в виртуальной локальной сети.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	Добавляет порт статической маршрутизации VLAN
no ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	Удаляет порта статической маршрутизации VLAN.

33.1.6 Настройка IPACL для создания таблицы многоадресной рассылки

Выполните следующие команды в режиме глобальной конфигурации, чтобы настроить список контроля доступа IPACL. Таким образом, могут быть установлены правила и

ограничения создания таблицы многоадресной рассылки после получения пакетов отчета IGMP.

Команда	Описание
ip igmp-snooping policy *word*	Добавляет IPACL при создании таблицы многоадресной рассылки
no ip igmp-snooping policy	Удаляет IPACL при создании таблицы многоадресной рассылки

33.1.7 Настройка фильтрации многоадресных сообщений без зарегистрированного адреса назначения

Если цель многоадресного сообщения не найдена (DLF – адрес назначения не зарегистрирован в микросхеме коммутатора посредством IGMP-Snooping), методом обработки по умолчанию является отправка сообщения на все порты VLAN. Путем настройки вы можете изменить метод обработки, и все многоадресные сообщения, адреса назначения которых не зарегистрированы ни на одном порту, будут удалены.

Команда	Описание
ip igmp-snooping dlf-drop	Отбрасывает многоадресное сообщение, пункт назначения которого не найден
no ip igmp-snooping dlf-drop	Возобновляет конфигурацию по умолчанию (многоадресную рассылку)

- Атрибут настраивается для всех VLAN.
- Методом по умолчанию для коммутатора обработки сообщений этого типа является пересылка (сообщение этого типа будет транслироваться внутри VLAN).

33.1.8 Настройка таймера срока действия данных маршрутизатора IGMP-Snooping

Таймер срока действия данных маршрутизатора используется для отслеживания существования запроса IGMP. Запрашивающие устройства IGMP поддерживают адреса многоадресной рассылки, отправляя сообщение запроса. Отслеживание работает посредством связи между запросчиком IGMP и хостом.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-snooping timer router-age *timer_value*	Настраивает значение таймера
no ip igmp-snooping timer router-age	Восстанавливает значение по умолчанию

Сведения об установке таймера запрашивающего устройства см. в разделе «Настройка таймера запросов IGMP-Snooping». Таймер срока действия данных маршрутизатора не может быть установлен на время, меньшее, чем время периода запроса. Рекомендуется установить значение таймера на время, в три раза превышающее период запроса.

Значение по умолчанию для таймера срока действия данных маршрутизатора – 260 секунд.

33.1.9 Настройка таймера ответов IGMP-Snooping

Таймер времени ответа – это верхний предел времени, в течение которого хост сообщает о многоадресной рассылке после того, как запрашивающая сторона IGMP отправит свое сообщение. Если сообщение отчета не получено по истечении времени таймера, коммутатор удалит адрес многоадресной рассылки.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-snooping timer response-time timer_value	Настраивает значение времени ответа IGMP-Snooping
no ip igmp-snooping timer response-time	Возвращает значение по умолчанию для времени ответа IGMP-Snooping

Значение таймера не может быть слишком маленьким. В противном случае многоадресная связь будет нестабильной.

По умолчанию значение времени ответа IGMP-Snooping составляет 15 секунд.

33.1.10 Настройка генератора запросов IGMP-Snooping

Если маршрутизатор многоадресной рассылки не существует в VLAN, где активировано отслеживание IGMP, можно использовать функцию запроса IGMP-Snooping, чтобы имитировать маршрутизатор многоадресной рассылки для регулярной отправки

запрашивающих сообщений IGMP. Функция является глобальной, то есть ее можно включить или отключить в VLAN, где глобально включено отслеживание IGMP.

Если маршрутизатор многоадресной рассылки не существует в VLAN и поток многоадресной рассылки не требует маршрутизации, функция автоматического запроса на коммутаторе может быть активирована посредством IGMP-Snooping, что обеспечит корректную работу отслеживания.

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
[**no**] **ip igmp-snooping querier [address** [*ip_addr*]	Настраивает генератор запросов IGMP-Snooping. Необязательный параметр **address** – это IP-адрес источника сообщений запросов

Изначально функция **ip igmp-snooping querier** выключена. Исходный IP-адрес фиктивного сообщения запроса IGMP-Snooping по умолчанию – 10.0.0.200.

Если функция запроса включена, она отключается, если многоадресный маршрутизатор появляется в VLAN; функция может автоматически активироваться по истечении времени ожидания многоадресного маршрутизатора.

33.1.11 Настройка таймера запросов IGMP-Snooping

Таймер времени запроса – это временной интервал, по истечении которого коммутатор в качестве локального генератора IGMP-запросов отправляет сообщения. При помощи этого таймера коммутатор периодически отправляет запросы в пределах VLAN после удаления устаревших записей.

Для настройки таймера выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-snooping querier querier-timer *timer_value*	Настройка значения таймера запросов IGMP-Snooping
no ip igmp-snooping querier querier-timer	Восстановление настройки по умолчанию

По умолчанию генератор запросов IGMP-Snooping отключен. Временной интервал передачи сообщений запроса по умолчанию составляет 200 секунд.

Когда активирована функция генерации запросов, интервал отправки сообщений не должен быть слишком долгим. Если в подсети есть другие коммутаторы с активированной аналогичной функцией, большое значение таймера запросов (больше, чем значение срока действия данных маршрутизатора, настроенное на других коммутаторах) приведет к нестабильности выбора запрашивающего узла в подсети.

33.1.12 Настройка функции forward-l3-to-mrouter

Если функция многоадресной рассылки L3 активирована и IGMP-Snooping не присоединяет сообщения к нисходящему порту, по маршруту многоадресной рассылки можно узнать только нисходящий порт VLAN. Если активирована функция **forward-l3-to-mrouter**, все нисходящие порты маршрутизатора могут быть изучены. Сообщения с данными могут быть отправлены на многоадресный порт маршрутизатора, зарегистрированный сообщением PIM-SM, без широковещательной передачи сообщений на все нисходящие физические порты. Команда в основном используется при следующих условиях:

- Когда несколько коммутаторов включают функцию многоадресной рассылки на уровне маршрутизации и создают цепочку, верхнее устройство в иерархии может узнать только о портах VLAN, которые находятся ниже по уровню, с использованием многоадресного протокола маршрутизатора. Поскольку верхние и нижние устройства не обмениваются интерактивными сообщениями IGMP, то верхние устройства не могут узнать о конкретных физических портах, подключенных к нижним устройствам.
- Когда верхние устройства направляют многоадресные потоки данных, они отправляют их на все физические порты в данной VLAN. Если активируется указанная функция, сообщения могут быть перенаправлены только на физические порты, подключенные к нижним устройствам, и не будут широковещательно транслироваться в данной VLAN, то есть не будут отправлены на все порты в этой VLAN.

Для настройки функции выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
[**no**] **ip igmp-snooping forward-l3-to-mrouter**	Настраивает отправку IGMP-сообщений на многоадресный порт маршрутизатора

По умолчанию функция выключена.

Эта команда позволяет перенаправлять данные на многоадресный порт маршрутизатора, но при этом сетевой чип имеет ограничивающую функцию на порту источника данных. В результате сообщения не будут перенаправляться на

порт источника данных, а только на порт мультимедийного роутера, который был зарегистрирован с использованием протокола PIM-SM.

33.1.13 Настройка чувствительного режима для IGMP-Snooping

При активированной функции, когда порт, находящийся в режиме trunk, выключается, время устаревания данных маршрутизатора (router-age time) устанавливается на значение, заданное в настройках чувствительного режима. Это заставляет систему быстро отправлять сообщения запроса.

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
[**no**] **ip igmp-snooping sensitive** [value [3-30]]	При настройке чувствительного режима IGMP-отслеживания значением может являться время устаревания данных активного в настоящий момент многоадресного маршрутизатора

По умолчанию чувствительный режим IGMP-Snooping выключен.

Когда установлен чувствительный режим, заданное при его настройке значение используется для обновления времени жизни маршрута до текущего значения за один период времени. В следующий раз время жизни маршрута восстанавливается до настроенного значения времени router-age.

33.1.14 Настройка функции v3-leave-check

Если функция v3-leave-check включена в IGMP Snooping, то после получения сообщения о выходе из мультимедийной группы в формате IGMP v3, будет отправлен специальный запрос. В противном случае, если эта функция отключена, никакие дополнительные действия не выполняются.

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
[**no**] **ip igmp-snooping v3-leave-check**	Настраивает функцию v3-leave-check

33.1.15 Настройка функции forward-wrongiif-within-vlan

Если функция «forward-wrongiif-within-vlan» включена в IGMP-Snooping, то мультимедийные данные, полученные из неправильного VLAN-интерфейса (например, из

интерфейса, который не соответствует исходной VLAN), будут на канальном уровне пересылаться внутри исходной VLAN на соответствующие порты, принадлежащие членам группы внутри этой VLAN. Если функция отключена, то такие сообщения будут отбрасываться.

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
[**no**] **ip igmp-snooping forward-wrongiif-within-vlan**	Настраивает пересылку сообщений из некорректного интерфейса внутри VLAN

Команда **ip igmp-snooping forward-wrongiif-within-vlan** имеет смысл только в том случае, если включена многоадресная рассылка L3.

33.1.16 Настройка функции IPACL на порту

Выполните следующие команды в режиме глобальной конфигурации, чтобы настроить список контроля доступа IPACL. Таким образом, можно будет обрабатывать или игнорировать многоадресные сообщения, поступившие с определенных IP-адресов.

Команда	Описание
ip igmp-snooping policy *word*	Добавляет список контроля доступа на порту
no ip igmp-snooping policy	Удаляет список контроля доступа на порту

33.1.17 Настройка IGMP-фильтрации в VLAN

Когда фильтрация мультимедийных сообщений включена в данной VLAN с использованием IGMP Snooping, только запросы на присоединение к группам, указанным в списке фильтрации, будут разрешены и добавлены к соответствующей группе в данной VLAN. В противном случае такие запросы будут проигнорированы, и новая группа не будет создана.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-snooping vlan *value* **filter** *vlanid-list*	Настраивает фильтрацию многоадресной рассылки IGMP-Snooping в VLAN. Параметр *vlanid-list* представляет собой список идентификаторов VLAN,

	соединенных символами «,» и «-». Обратите внимание, что после «,» и «-» должен идти хотя бы один пробел
no ip igmp-snooping vlan *value* **filter** *vlanid-list*	Удаляет фильтрацию многоадресной рассылки в VLAN

33.1.18 Настройка максимального количества мультикастовых адресов на порту IGMP-Snooping

Настройка максимального количества IP-адресов для мультикастовой передачи на порту IGMP-Snooping позволяет контролировать количество групп, на которые этот порт может подписываться. Если количество групп превышает установленное ограничение, запись для этого порта не будет создана.

В режиме настройки интерфейса выполните следующую команду:

Команда	Описание
[**no**] **ip igmp-snooping limit** [value [1-2048]]	Настройка максимального количества IP-адресов для мультикастовой передачи на порту IGMP-Snooping

По умолчанию максимальное количество адресов составляет 2048.

33.1.19 Настройка функции подавления отчетов IGMP-Snooping

Если эта функция настроена в той же VLAN, то, независимо от того, инициирован ли изначально запрос клиентом, или же клиент отвечает на запрос, коммутатор пересылает ограниченное количество сообщений на порт многоадресной рассылки. Это количество определяется параметром после ключевого слова **max-number** и находится в диапазоне от 1 до 5. Если ключевое слово **max-number** опущено, количество переадресаций по умолчанию равно 1.

При нормальной работе функции IGMP-Snooping эта конфигурация позволяет снизить затраты на обработку в локальном коммутаторе и коммутаторе верхнего уровня, а также экономить пропускную способность для пересылки отчетов.

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
[**no**] **ip igmp-snooping report-suppression** [**max-number** value [1-5]]	Настраивает функцию подавления отчетов IGMP-Snooping и максимальное количество пересылок

По умолчанию функция подавления отчетов IGMP-отслеживания отключена.

Если **ip igmp-snooping report-suppression** настроено без ключевого слова **max-number**, количество пересылок отчетов по умолчанию равно 1.

33.1.20 Настройка функции proxy-leave IGMP-Snooping

Функция proxy-leave в IGMP-Snooping позволяет коммутатору выступать в роли прокси-сервера для обработки сообщений о выходе из мультимедийных групп. Когда устройство хочет покинуть определенную мультимедийную группу, оно отправляет соответствующее IGMP-сообщение о выходе из группы. Вместо того чтобы отправлять это сообщение всем устройствам в сети, коммутатор с включенной функцией proxy-leave может перехватить это сообщение и обработать его самостоятельно. Таким образом, коммутатор отправляет сообщение о выходе из группы вышестоящему устройству только после того, как все члены группы многоадресной рассылки действительно покинули группу.

Преимущество использования функции состоит в том, что она может уменьшить нагрузку на сеть, так как сообщение о выходе из группы не будет передаваться по всей сети, а будет обработано только коммутатором. Это позволяет снизить излишний мультимедийный трафик и повысить эффективность сети, особенно в ситуациях с большим количеством клиентов и групп многоадресной рассылки.

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
[**no**] **ip igmp-snooping proxy-leave**	Включает/выключает функцию proxy-leave

По умолчанию функция proxy-leave выключена.

33.1.21 Мониторинг и поддержка IGMP-Snooping

В режиме управления выполните следующие операции:

Команда	Описание
show ip igmp-snooping	Отображает информацию о конфигурации IGMP-Snooping
show ip igmp-snooping timer	Отображает информацию о времени IGMP-Snooping
show ip igmp-snooping group	Отображает информацию о многоадресной группе IGMP-Snooping
show ip igmp-snooping group interface	Отображает информацию о многоадресной группе IGMP-Snooping на порту

show ip igmp-snooping statistics [**message** | **packet** | **hardware** | **vlan** *vlanid*]	Отображает статистическую информацию IGMP-Snooping
show ip igmp-snooping vlan	Отображает информацию о VLAN IGMP-Snooping
[**no**] **debug ip igmp-snooping** [**packet** | **timer** | **event** | **error**]	Включает и отключает отладочные сообщения, связанные с протоколом IGMP-Snooping. С помощью указания параметров можно выбирать, какие конкретные аспекты необходимо отслеживать с помощью отладочных сообщений. Команда [**no**] **debug ip igmp-snooping** позволяет включать или выключать отладочный режим для этих аспектов протокола в зависимости от потребности пользователя.

Отображение информации VLAN о работе IGMP-Snooping:

```
switch# show ip igmp-snooping
Global IGMP snooping configuration:
------------------------------------
Globally enable      : Enabled
VLAN nodes           : 1,50,100,200,400,500
Dlf-frames filtering : Disabled
Sensitive            : Disabled
Querier              : Enabled
Querier address      : 10.0.0.200
Querier interval     : 140 s
Router age           : 260 s
Response time        : 15 s

 vlan_id   Immediate-leave   Ports   Router Ports
-------------------------------------------------------------
    1        Disabled        5-10     SWITCH(querier);
   50        Disabled        1-4      SWITCH(querier);
  100        Disabled        NULL     SWITCH(querier);G0/1(static);
  200        Disabled        NULL     SWITCH(querier);
  400        Disabled        NULL     SWITCH(querier);
  500        Disabled        NULL     SWITCH(querier);
```

Отображение информации о мультимедийной группе IGMP-Snooping:

```
switch# show ip igmp-snooping group
      The total number of groups       2
```

```
 Vlan Group       Type Port(s)
---- --------------- ---- -----------------------------------------------------
1 226.1.1.1       IGMP G0/1                 G0/3
 1 225.1.1.16      IGMP G0/1                   G0/3
```

Отображение информации о группе многоадресной рассылки IGMP-Snooping, добавленной на порт:

```
switch# show ip igmp-snooping group interface g0/4

Number of joined groups: 1

Vlan Group           Mode    Source Num
---- --------------- ------- ----------
   2 230.1.1.1       Exclude   0
```

Отображение таймера IGMP-Snooping:

```
switch# show ip igmp-snooping timers
vlan 1 router age : 251 Отображение таймера устаревания.
vlan 1 multicast address 0100.5e00.0809 response time: 1  Указание периода с момента получения последнего
 сообщения запроса группы многоадресной рассылки до текущего времени; если ни один хост на порту не
 ответит по истечении времени таймера, порт будет удален.
```

Отображение статистики IGMP-Snooping:

```
    switch_config#show ip igmp-s statistics

    IGMP Snooping Message Statistics
    ------------------------------------
    L2 main messages sent OK     : 75
    L2 main messages sent failed   : 0
    L2 packets received            : 72
    L2 packets sent               : 72
    L2 packets sent failed          : 0
    L2 link-status messages         : 3
    IGMP Snooping messages received: 79
    IGMP packet messages received  : 72

    IGMP Snooping Packet Statistics
    ---------------------------------------
    Received packets                 : 72
    IGMP packets                    : 29
    M-routing protocol packets          : 0
    Other packets                   : 43
    Received IGMP general queries      : 0
    Received IGMPv2 specific queries    : 0
    Received IGMPv3 g specific queries  : 0
    Received IGMPv3 gs specific queries: 0
```

```
Received IGMPv1 reports           : 0
Received IGMPv2 reports           : 0
Received IGMP leaves              : 0
Received IGMPv3 reports           : 29
Flooded queries                   : 0
Forwarded and proxy-sent reports  : 0
Forwarded and proxy-sent leaves   : 0

IGMP Snooping Hardware Operation Statistics
-------------------------------------------
Total               : 0   Общее количество аппаратных операций
Succeeded           : 0   Количество успешных аппаратных операций
Failed              : 0   Количество неудачных аппаратных операций
Report/leave processing: 0    Количество аппаратных операций по обработке отчетов и выходов
Response timer expiring: 0    Количество аппаратных операций в ответ на истечение таймера
Group creating/updating: 0  Количество аппаратных операций в результате создания и обновления групп
  Group deleting        : 0   Количество аппаратных операций, вызванных удалением группы
```

Отображение информации VLAN IGMP-Snooping:

```
switch_config# show ip igmp-snooping vlan
 vlan_id    Immediate-leave   Ports   Router Ports
-----------------------------------------------------------------
    1        Disabled        7-30
    2        Disabled        NULL
```

Отладка сообщений IGMP-Snooping:

```
switch# debug ip igmp-snooping packet
Jan  1 02:22:28 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:28 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:29 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:29 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:38 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:38 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:39 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:39 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:23:11 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:23:11 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:23:12 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:23:12 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
```

Отладка таймера IGMP-Snooping:

```
switch#debug ip igmp-snooping timer
Jan  1 02:30:36 IGMP-snooping: Vlan 1 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 100 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 200 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 400 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 500 router on interface (null) expiry. Inquerying the response timer expiry
```

33.1.22 Пример настройки IGMP-Snooping

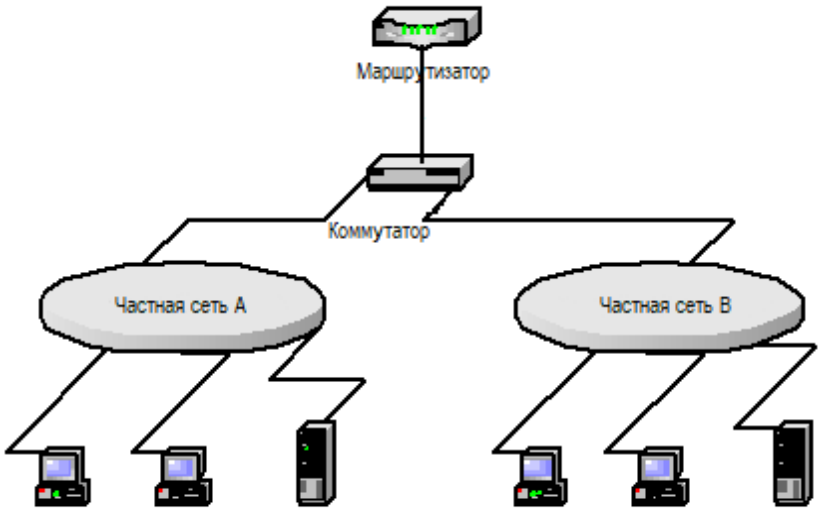

Рисунок 33-1 – Пример настройки IGMP-Snooping

Настройка коммутатора

1. Включите IGMP-Snooping для VLAN 1, соединяющей частную сеть A.

   Switch_config# ip igmp-snooping vlan 1

2. Включите IGMP-Snooping для VLAN 2, соединяющей частную сеть B.

   Switch_config# ip igmp-snooping vlan 2

33.2 IGMP-прокси

IGMP-прокси позволяет VLAN, в которой находится пользователь, получать данные многоадресной рассылки из других VLAN. Функция работает на уровне 2 независимо от других протоколов многоадресной маршрутизации. IGMP-прокси работает путем пересылки IGMP-пакетов из одной VLAN в другую и обновления таблицы пересылки в сетевом оборудовании для мультимедийных пользователей в на основе информации, полученной из этих IGMP-пакетов.

IGMP-прокси разделяет VLAN на два типа: проксируемые и проксирующие. Нисходящие группы могут быть настроены как проксируемые VLAN, а восходящие – как проксирующие.

IGMP-прокси основан на IGMP-Snooping и работает только при включенном отслеживании. Тогда как на саму функцию IGMP-Snooping включение или отключение IGMP-прокси никак не влияет.

IGMP-прокси нельзя использовать, если не выполнены следующие условия:

1. Поддержка коммутатором протоколов L3;

2. Недопущение включения многоадресной IP-маршрутизации одновременно с IGMP-прокси;

3. Недопущение использования виртуальной локальной сети в качестве нисходящей и восходящей одновременно.

Задачи настройки

- Включение/отключение IGMP-прокси
- Добавление/удаление связи агента VLAN
- Добавление/удаление статических записей источника многоадресной рассылки
- Мониторинг и поддержка IGMP-прокси
- Пример настройки IGMP-прокси

33.2.1 Включение/отключение IGMP-прокси

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-proxy enable	Включает IGMP-прокси
no ip igmp-proxy enable	Восстанавливает настройки по умолчанию

IGMP-прокси нельзя включить после включения многоадресной IP-маршрутизации. Если она включена, ранее включенный прокси-сервер IGMP автоматически отключается. Отключение многоадресной IP-маршрутизации не приведет к автоматическому включению IGMP-прокси.

33.2.2 Добавление/удаление связи агента VLAN

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** c*vlan_map*	Добавляет VLAN агента (avlan_map) для управления клиентской VLAN (cvlan_map)

no ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** c*vlan_map*	Удаляет связи клиента и агента

- Клиентская VLAN не может быть настроена до того, как при помощи **avlan_map** будет назначена агентская VLAN; кроме того, VLAN агента нельзя настроить до того, как при помощи **cvlan_map** будет назначена клиентская VLAN.
- В обеих VLAN должна быть включена поддержка IGMP-Snooping.

33.2.3 Мониторинг и поддержка IGMP-прокси

Выполните следующие команды в режиме управления:

Команда	Описание
show ip igmp-proxy	Отображает информацию об IGMP-прокси
[**no**] **debug ip igmp-proxy** [*error* | *event* | *packet*]	Включает или отключает информацию отладки IGMP-прокси

33.2.4 Пример настройки IGMP-прокси

Топология сети показана на рисунке 33-2.

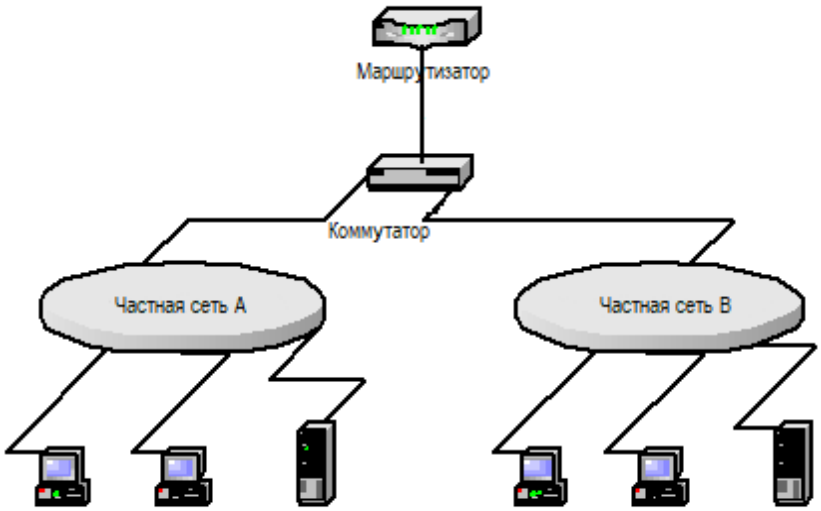

Рисунок 33-2 – Пример настройки IGMP-прокси

Настройка коммутатора

1. Включите IGMP-Snooping и IGMP-прокси.

    Switch_config# ip igmp-snooping

    Switch_config# ip igmp-proxy enable

2. Укажите VLAN 2 (в частной сети A) в качестве агентской VLAN клиентской VLAN 3 (в частной сети B).

    Switch_config# ip igmp-proxy agent-vlan 2 client-vlan map 3

34. MLD-Snooping

34.1 Введение

MLD-Snooping (Multicast Listener Discovery Snooping) – это технология, аналогичная IGMP-Snooping, но используемая для IPv6-сетей. Она применяется для эффективного управления трафиком многоадресной коммуникации в сетях, работающих с протоколом IPv6.

Основные концепции MLD-Snooping включают:

MLD (Multicast Listener Discovery): MLD – это протокол, используемый в сетях IPv6 для управления групповой (многоадресной) коммуникацией. Аналогом IGMP в IPv4 является MLD в IPv6. Устройства, подключенные к сети IPv6, используют MLD, чтобы сообщать маршрутизаторам о своей заинтересованности в присоединении к многоадресным группам.

MLD Snooping: MLD-Snooping – это технология, которая позволяет коммутаторам в сети отслеживать MLD-сообщения, отправляемые устройствами IPv6. Она позволяет коммутаторам узнавать, какие устройства в определенных сегментах сети интересуются многоадресным трафиком и на какие многоадресные группы они подписаны.

Управление трафиком: MLD-Snooping позволяет коммутаторам более эффективно управлять многоадресным трафиком. Он может решать, на какие порты отправлять многоадресные пакеты, основываясь на информации, полученной через MLD-сообщения устройств.

Уменьшение нагрузки на сеть: путем отправки многоадресных пакетов только на порты, где есть устройства, заинтересованные в этом трафике, MLD-Snooping помогает снизить нагрузку на сеть и повысить ее эффективность. Если устройство L2 не выполняет отслеживание MLD, многоадресные данные будут транслироваться на втором уровне; когда устройство L2 запускает отслеживание MLD, многоадресные данные известной группы многоадресной рассылки не будут транслироваться широковещательно, а будут отправлены назначенному получателю. Неизвестные данные многоадресной рассылки будут отброшены.

В общем, MLD-Snooping играет аналогичную роль для IPv6, как IGMP-Snooping для IPv4, и помогает оптимизировать работу сетей, использующих IPv6 для многоадресной коммуникации.

Поскольку отслеживание MLD решает вышеупомянутые проблемы путем мониторинга пакетов запросов или отчетов MLD-Snooping, оно может работать нормально только при наличии многоадресного маршрутизатора, что означает, что коммутатор должен периодически получать сообщение запроса MLD-Snooping от маршрутизатора. Таким образом, в конфигурации MLD-Snooping значение таймера устаревания данных маршрутизатора должно быть больше, чем период, через который маршрутизатор отправляет запросы. Информацию о многоадресном маршрутизаторе в каждой виртуальной локальной сети можно посмотреть, используя команду **show ipv6 mld-snooping**.

34.2 Настройка MLD-Snooping

Задачи настройки

- Включение/отключение MLD-Snooping
- Включение/отключение запроса аппаратным устройствам о многоадресной рассылке
- Добавление/удаление статического мультикастового адреса VLAN
- Установка таймера устаревания данных маршрутизатора для MLD-Snooping
- Настройка таймера времени отклика MLD-Snooping
- Настройка генератора запросов в MLD-Snooping
- Настройка порта статического многоадресного маршрутизатора
- Настройка функции немедленного выхода из группы
- Мониторинг и поддержка MLD-Snooping

34.2.1 Включение/отключение MLD-Snooping

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ipv6 mld-snooping	Включает многоадресную рассылку с отслеживанием MLD
no ipv6 mld-snooping	Отключает отслеживание MLD

После того, как MLD-Snooping включен, пакеты многоадресной рассылки, адреса назначения которых не зарегистрированы, отбрасываются.

34.2.2 Включение/отключение запроса аппаратным устройствам о многоадресной рассылке

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ipv6 mld-snooping solicitation	Включает функцию запроса аппаратным устройствам о многоадресной рассылке группы
no ipv6 mld-snooping solicitation	Выключает функцию запроса аппаратным устройствам о многоадресной рассылке группы

34.2.3 Добавление/удаление статического мультикастового адреса VLAN

Настройка статического мультикастового адреса позволяет определенным хостам, которые не поддерживают протокол MLD-Snooping, получать соответствующие групповые пакеты.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*	Добавляет статический мультикастовый адрес VLAN
no ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*	Удаляет статический мультикастовый адрес VLAN

34.2.4 Установка таймера устаревания данных маршрутизатора для MLD-Snooping

Таймер устаревания данных маршрутизатора используется для проверки существования запрашивающей стороны MLD-Snooping. Запрашивающая сторона MLD-Snooping поддерживает адрес рассылки, отправляя пакеты запросов. Процесс переадресации мультимедийного трафика опирается на связь между запрашивающей стороной MLD-Snooping и хостом.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ipv6 mld-snooping timer router-age *timer_value*	Устанавливает время устаревания данных MLD-Snooping маршрутизатора
no ipv6 mld-snooping timer router-age	Восстанавливает для данных MLD-Snooping маршрутизатора время устаревания по умолчанию

Настройки этого таймера должны коррелировать с настройками периода запроса MLD-Snooping и быть больше периода запроса. Рекомендуется установить таймер устаревания данных маршрутизатора в три раза больше периода запроса.

Значение по умолчанию составляет 260 секунд.

34.2.5 Установка таймера времени отклика MLD-Snooping

Таймер времени ответа – это время, в течение которого хост должен сообщить о своей потребности в многоадресной рассылке после того, как запрашивающая сторона MLD-Snooping отправит пакет запроса. Если не было получено ни одного пакета отчета, после истечения срока действия таймера коммутатор удалит данный адрес из списка многоадресной рассылки.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ipv6 mld-snooping timer response-time *timer_value*	Устанавливает время ответа MLD-Snooping
no ipv6 mld-snooping timer response-time	Восстанавливает для времени ответа MLD-Snooping значение по умолчанию

Значение таймера не должно быть слишком маленьким, иначе многоадресная связь может стать нестабильной.

Значение по умолчанию составляет 10 секунд.

34.2.6 Настройка генератора запросов в MLD-Snooping

Если в VLAN с отслеживанием MLD нет специального маршрутизатора многоадресной рассылки, то для регулярной пересылки пакетов группового запроса IGMP можно включить функцию запросов модуля MLD-Snooping, который действует как виртуальный маршрутизатор многоадресной рассылки. Функция может быть включена или отключена только в том случае, если все VLAN поддерживают отслеживание MLD.

Если в локальной сети нет маршрутизатора многоадресной рассылки и поток многоадресной рассылки не нуждается в маршрутизации, запустите команду **mld-snooping querier**, чтобы активировать функцию генерации запросов модулем MLD-Snooping коммутатора.

Запустите следующую команду в режиме глобальной конфигурации:

Команда	Описание
[**no**] **ipv6 mld-snooping querier** [**address** [*ip_addr*]]	Устанавливает функцию генерации запросов модулем MLD-Snooping. Выбирает значение дополнительного параметра **address** в качестве IP-адреса источника пакета запроса

По умолчанию запросы IGMP-Snooping отключены. Исходный IP-адрес фиктивного пакета запроса – FE80::3FF:FEFE:FD00:1.

При включении функции генерации запросов, если в VLAN есть многоадресный маршрутизатор, функция автоматически становится недействительной; если физический маршрутизатор перестает работать, функция вступает в силу автоматически.

34.2.7 Настройка порта статического многоадресного маршрутизатора

Как только порт настроен в качестве порта статической многоадресной маршрутизации, все полученные отчеты и сообщения о завершении MLD-Snooping перенаправляются на этот порт.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ipv6 mld-snooping vlan *WORD* **mrouter** interface *intf_name*	Назначает порт в качестве порта статического многоадресного маршрутизатора для VLAN *WORD*

no ipv6 mld-snooping vlan *WORD* **mrouter** interface *intf_name*	Удаляет порт статического многоадресного маршрутизатора для VLAN *WORD*

34.2.8 Настройка функции немедленного выхода из группы

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ipv6 mld-snooping vlan *WORD* **immediate-leave**	Включает функцию немедленного выхода
no ipv6 mld-snooping vlan *WORD* **immediate-leave**	Восстанавливает настройки по умолчанию

34.2.9 Мониторинг и поддержка MLD-Snooping

Выполните следующие команды в режиме управления:

Команда	Описание
show ipv6 mld-snooping	Отображает конфигурацию MLD-Snooping
show ipv6 mld-snooping timer	Отображает настройки параметров времени MLD-Snooping
show ipv6 mld-snooping groups	Отображает группы многоадресной рассылки MLD-Snooping
show ipv6 mld-snooping statistics	Отображает статистическую информацию MLD-Snooping
show ipv6 mld-snooping vlan	Отображает конфигурацию MLD-Snooping в VLAN
show ipv6 mld-snooping mac	Отображает MAC-адреса многоадресной рассылки, записанные при отслеживании MLD

Информация о конфигурации MLD-Snooping:

```
#show ipv6 mld-snooping

Global MLD snooping configuration:
------------------------------------
Globally enable      : Enabled
Querier              : Enabled
Querier address      : FE80::3FF:FEFE:FD00:1
Router age           : 260 s
Response time        : 10 s
```

```
Handle Solicitation  : Disabled

Vlan 1:
----------
   Running
   Routers: SWITCH(querier);
```

Информация о группах многоадресной рассылки MLD-Snooping:

```
#show ipv6 mld--snooping groups

Vlan Group          Type Port(s)
---- --------------- ---- -------------------------------------
  1 FF02::1:FF32:1B9B MLD  G2/23
  1 FF02::1:FF00:2  MLD  G2/23
  1 FF02::1:FF00:12 MLD  G2/23
  1 FF02::1:FF13:647D MLD  G2/23
  2 FF02::1:FF00:2  MLD  G2/22
  2 FF02::1:FF61:9901 MLD  G2/22
```

Информация о таймере MLD-Snooping:

```
Switch#show ipv6 mld-snooping timer

vlan 1 Querier on port 0 : 251
#
```

Querier on port 0: 251 означает, что время устаревания вышло.

vlan 2 multicast address 3333.0000.0005 response time: Здесь показан временной период от получения пакета многоадресного запроса до настоящего времени; если нет хоста, который мог бы ответить по истечении времени таймера, рассылка для порта будет прекращена.

Статистическая информация MLD-Snooping:

```
#show ipv6 mld-snooping statistics
 vlan 1
------------
   v1_packets:0       Количество пакетов v1
   v2_packets:6       Количество пакетов v2
   v3_packets:0       Количество пакетов v3
   general_query_packets:5    Количество пакетов общих запросов
   special_query_packets:0    Количество пакетов специальных запросов
   listener_packets:6      Количество пакетов Report
      done_packets:0    Количество пакетов Leave
      err_packets:0     Количество пакетов Error
```

Информация о MAC-адресах MLD-Snooping:

```
#show ipv6 mld-snooping mac
Vlan Mac            Ref Flags
```

```
---- --------------- ---- ------
  1 3333:0000:0001    1   2
  2 3333:ff61:9901    1   0
      FF02::1:FF61:9901
  1 3333:0000:0002    1   2
  1 3333:ff00:0002    1   0
      FF02::1:FF00:2
  1 3333:ff00:0012    1   0
      FF02::1:FF00:12
  1 3333:ff13:647d    1   0
      FF02::1:FF13:647D
  1 3333:ff32:1b9b    1   0
      FF02::1:FF32:1B9B
  2 3333:ff00:0002    1   0
      FF02::1:FF00:2
  1 3333:ff00:0001    1   2
  1 3333:ff8e:7000    1   2
```

35. EFM OAM

35.1 Обзор

EFM OAM (Ethernet in the First Mile Operations, Administration, and Maintenance) это набор протоколов и функций, разработанных в рамках стандарта IEEE 802.3ah. Этот стандарт определяет спецификации для использования Ethernet в местных сетях доступа, таких как сети передачи данных на последнем участке между абонентом и провайдером.

EFM OAM является частью этого стандарта и представляет собой набор механизмов и протоколов для управления, администрирования и обслуживания Ethernet-соединений в местных сетях доступа. Он обеспечивает проверку и обнаружение неисправностей двухточечного соединения в отдельной линии связи. Однако EFM OAM не может быть применен к виртуальному соединению EVC, и поэтому нельзя реализовать мониторинг Ethernet между терминалами. Пакеты данных для операций, администрирования и обслуживания (OAM PDU) не могут быть перенаправлены на другие интерфейсы. Ethernet OAM, регулируемый стандартом IEEE 802.3ah, является относительно медленным протоколом. Максимальная скорость передачи составляет 10 кадров в секунду, а минимальная – 1 кадр в секунду.

35.1.1 Атрибуты протокола OAM

- Поддержка устройств Ethernet OAM и атрибутов OAM

  Процесс подключения Ethernet OAM называется этапом обнаружения, когда объект OAM находит объект OAM удаленного устройства и устанавливается стабильный сеанс. На этом этапе подключенные объекты Ethernet OAM сообщают друг другу о своем режиме OAM, информацию о конфигурации Ethernet OAM и поддерживаемых локальным узлом возможностях Ethernet OAM, взаимодействуя друг с другом посредством информационных PDU OAM. Если конфигурация обратной связи,

конфигурация обнаружения однонаправленного канала и конфигурация событий канала были переданы в Ethernet OAM двух терминалов, протокол Ethernet OAM начнет работать на канальном уровне.

- Мониторинг связи

  Ethernet OAM осуществляет мониторинг канала посредством уведомлений PDU OAM о событиях. Если возникают проблемы на сетевой линии, и локальный узел обнаруживает эти проблемы, то он передает сообщение Event Notification OAM PDU (PDU для уведомления о событиях) партнеру Ethernet OAM, чтобы сообщить о нормальных или аномальных событиях на линии. Это позволяет администратору динамически отслеживать состояние сети через мониторинг линии связи. Определения нормальных событий связи показаны в таблице 35-1.

Таблица 35-1 – Определения нормальных событий связи

Нормальное событие связи	Определение
Периодическое событие ошибки сигнала	Указывает на номер сигнала N как период. Когда на приемной стороне получают N сигналов, и количество ошибочных сигналов превышает установленный порог (определенный величиной N), это считается событием ошибки
Событие кадра ошибки	Количество ошибочных кадров превышает установленный порог в течение определенного времени
Периодическое событие кадра ошибки	Указывает на то, что определенное количество кадров N является периодом для мониторинга ошибок в сети. Если количество ошибочных кадров превышает установленный порог в течение каждых N принятых кадров, то это считается событием ошибки
Второй кадр ошибки	Второй кадр, который идет после первого ошибочного, будет считаться проблемным, если количество ошибок в нем превышает определенный порог за определенное время (временное окно M секунд)

- Удаленная индикация неисправности

  Проверка проблем в Ethernet может быть сложной задачей, особенно когда производительность сети замедляется, но физическое сетевое взаимодействие продолжается. Для решения этой проблемы существует OAM PDU, который определяет область флагов, позволяющую Ethernet OAM-сущности передавать информацию о проблемах своему партнеру. Эти флаги могут представлять следующие чрезвычайные события связи:

- Link Fault (ошибка связи): физический уровень обнаруживает, что приемное направление локального DTE (Data Terminal Equipment) не функционирует. Если возникают проблемы, некоторые устройства на физическом уровне поддерживают однонаправленную передачу данных и позволяют уведомлять о проблемах от удаленного OAM.
- Dying Gasp (последний вздох): если происходит неисправимая локальная ошибка, такая как выключение OAM, интерфейс входит в состояние с ошибкой и затем выключается.
- Critical Event (критическое событие): возникают неопределенные критические события (производитель указывает, какие именно события считать критическими).

Информация OAM PDU непрерывно передается во время соединения Ethernet OAM. Локальный объект OAM может сообщать о локальных критических событиях связи удаленному объекту OAM через информационный PDU OAM. Таким образом, администратор может динамически узнавать о состояние связи и вовремя устранять возникающие ошибки

- Удаленная обратная связь

  OAM предоставляет опциональный режим обратной связи на канальном уровне и выполняет поиск ошибок и тестирование производительности соединения с использованием обратной связи без OAM PDU. После создания соединения OAM, активная сущность OAM инициирует команду удаленной обратной связи, и соседняя сущность на нее отвечает. Когда удаленный терминал находится в режиме обратной связи, все пакеты, кроме пакетов OAM PDU и пакетов Pause, отправляются обратно по предыдущим маршрутам. Это позволяет проводить локализацию ошибок и оценку производительности соединения. Когда удаленное оборудование находится в режиме обратной связи, можно произвольно запрашивать и сравнивать статистические данные, будь то локальные или удаленные. Запрос данных можно выполнять до, во время или после отправки кадра обратной связи на удаленное оборудование. Обычная проверка обратной связи помогает быстро обнаруживать ошибки в сети. Сегментарная проверка помогает выявлять конкретные ошибки в сети и затем устранять их.

- Круговой запрос любых MIB-переменных, описанных в главе 30 стандарта 802.3.

35.1.2 Режим OAM

Устройство может осуществлять соединение OAM в двух режимах: активном и пассивном. Возможности устройства в различных режимах сравнивается в таблице 35-2. Только объект OAM в активном режиме может инициировать процесс подключения, тогда как объект OAM в пассивном режиме должен ждать запроса на соединение от однорангового объекта OAM. После завершения процесса обнаружения удаленного OAM локальный объект в активном режиме может передать любой пакет OAM PDU, если удаленный объект находится в активном режиме, тогда как работа локального объекта в активном режиме будет ограничена, если удаленный объект находится в пассивном режиме. Это связано с тем, что устройство в активном режиме не реагирует на команды удаленной обратной связи и запросы переменных, передаваемые пассивным удаленным объектом.

Таблица 35-2 – Сравнение возможностей устройства в активном и пассивном режимах

Возможности	Активный режим	Пассивный режим
Инициализация процесса обнаружения Ethernet OAM	Да	Нет
Ответ на инициализацию процесса обнаружения OAM	Да	Да
Передача информационного пакета OAM PDU	Да	Да
Разрешение на передачу пакета OAM PDU с уведомлением о событии	Да	Да
Разрешение передачи пакета OAM PDU с запросом переменных	Да	Нет
Разрешение передачи пакета OAM PDU с ответом на запрос переменных	Да	Да
Разрешение передачи пакета OAM PDU проверки обратной связи	Да	Нет
Ответ на OAM PDU проверки обратной связи	Да, но одноранговый терминал должен находиться в активном режиме.	Да
Разрешение передачи указанного OAM PDU	Да	Да

После того как соединение Ethernet OAM установлено, объекты OAM на двух терминалах поддерживают соединение, передавая информационные пакеты PDU OAM. Если пакет OAM PDU от однорангового объекта OAM не получен в течение пяти секунд, время соединения истекает, после чего необходимо установить новое соединение OAM.

35.1.3 Компоненты пакета OAM

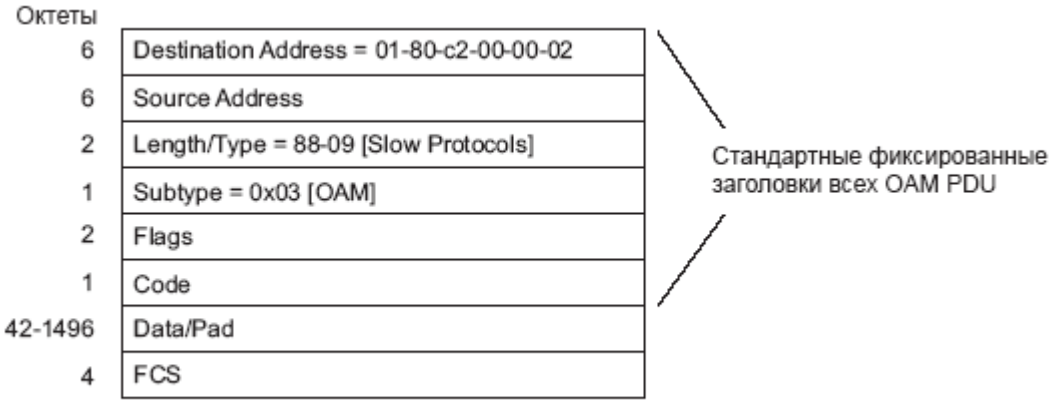

Рисунок 35-1 – Структура кадра OAM PDU

Ниже приведены описания полей пакета OAM:

- Destination address (адрес назначения): означает MAC-адрес назначения пакета Ethernet OAM.
- Source address (адрес источника): означает MAC-адрес источника пакета Ethernet OAM. Это MAC-адрес порта терминала передатчика, а также юникастовый MAC-адрес.
- Length/Type (длина/тип): всегда принимает кодировку типа. Тип протокола пакета Ethernet OAM – 0x8809.
- Subtype (подтип): подтип протокола для пакетов Ethernet OAM – 0x03.
- Flags (флаги): поле, в котором отображается состояние объекта Ethernet OAM.
- Code (код): поле, в котором отображается тип пакета OAM PDU.
- Data/Pad (дата/заполнение): поле, включающее в себя как собственно данные OAMPDU, так и возможное заполнение (дополнительные биты или значения), которые могут использоваться для выравнивания пакета.
- FCS: (контрольная сумма кадра): поле, представляющее собой значение, которое используется для проверки целостности данных в передаваемом пакете.

Таблица 35-3 – Типы пакетов OAM PDU

Код	Тип сообщения
00	Информационное
01	Уведомление о событии
02	Запрос переменных
03	Ответ на запрос переменных

04	Управление обратной связью
05-FD	Зарезервированное значение
FE	Содержимое определяется организацией
FF	Зарезервированное значение

Информационный OAM PDU используется для передачи информации о состоянии объекта OAM удаленному объекту OAM для поддержания соединения OAM.

Пакет уведомления о событии используется для мониторинга канала связи и сообщения о проблемах, возникших на канале между локальными и удаленными объектами OAM.

Пакет обратной связи OAM PDU применяется в основном для управления удаленной обратной связью, включая состояние обратной связи OAM с удаленного устройства. Пакет содержит информацию, позволяющую включать или выключать функцию обратной связи. С его помощью можно устанавливать или завершать удаленную обратную связь в соответствии с содержащейся информацией.

35.2 Настройка OAM

Задачи настройки

- Включение OAM на интерфейсе
- Включение удаленной обратной связи OAM
- Настройка мониторинга связи OAM
- Настройка уведомления о неисправностях от удаленного объекта OAM
- Отображение информации о протоколе OAM

35.2.1 Включение OAM на интерфейсе

Выполните следующие команды, чтобы включить OAM:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface *intf-type intf-id*	Вход в режим настройки интерфейса
ethernet oam	Включает Ethernet OAM на интерфейсе
ethernet oam [**max-rate** *oampdus* | **min-rate** *seconds* | **mode** {**active** | **passive**} | **timeout** *seconds*]	Настраивает дополнительные параметры OAM: Параметр **max-rate** используется для настройки максимального количества OAM PDU, передаваемых в секунду. Он находится в диапазоне от 1 до 10, значение по умолчанию – 10.

	Параметр **min-rate** используется для настройки минимальной скорости передачи OAMPDU. Его единица измерения – секунда. Он находится в диапазоне от 1 до 10, значение по умолчанию – 1. Параметр **mode {active | passive}** используется для установки режима OAM. Соединение OAM может быть установлено между двумя интерфейсами только тогда, когда хотя бы один интерфейс находится в активном режиме. Параметр **timeout** используется для установки времени ожидания соединения OAM. Оно находится в диапазоне от 1 до 30 секунд, значение по умолчанию – 1 секунда

Вы можете запустить команду **no ethernet oam**, чтобы отключить функцию OAM.

Удаленную обратную связь OAM нельзя включить на физическом интерфейсе, принадлежащем группе агрегации.

35.2.2 Настройка мониторинга связи OAM

Процедура настройки мониторинга канала OAM на интерфейсе показана в следующей таблице:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface *intf-type intf-id*	Вход в режим настройки интерфейса
ethernet oam link-monitor negotiation-supported	Включает мониторинг связи на интерфейсе. Мониторинг связи поддерживается по умолчанию
ethernet oam link-monitor symbol-period {**threshold** {**high** {*symbols* | **none**} | **low** {*symbols*}} | **window** *symbols*}	Устанавливает верхний и нижний порог для периодического события сигнала ошибки, которое запускает событие ошибки связи. Параметр **threshold high** используется для настройки верхнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 1 до 65535, а его значение по умолчанию – **none** (отсутствует). Параметр **threshold low** используется для настройки нижнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 0 до 65535, а его значение по умолчанию – 1. Параметр **window** используется для настройки размера окна периода кругового запроса.

	Единицей измерения размера окна является количество сигналов 100M. Размер окна может варьироваться в зависимости от интерфейса Ethernet: на интерфейсе 1000M Ethernet диапазон размера окна составляет от 10 до 600, а его значение по умолчанию – 10, в то время как на интерфейсе 100M Ethernet диапазон размера окна составляет от 1 до 60, и его значение по умолчанию – 1. Этот параметр позволяет настраивать частоту и размер периодических запросов для мониторинга связи в сетях Ethernet
ethernet oam link-monitor frame {**threshold** {**high** {*symbols* | **none**} | **low** {*symbols*}} | **window** *symbols*}	Устанавливает верхнее и нижнее пороговые значения события кадра ошибки, которое запускает соответствующее событие связи. Параметр **threshold high** используется для настройки верхнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 1 до 65535, а его значение по умолчанию – **none** (отсутствует). Параметр **threshold low** используется для настройки нижнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 0 до 65535, а его значение по умолчанию – 1. Параметр **window** используется для настройки размера временного окна периода кругового запроса. Единицей измерения являются секунды. Диапазон значений находится между 1 и 60, а значение по умолчанию – 1
ethernet oam link-monitor frame-period {**threshold** {**high** {*symbols* | **none**} | **low** {*symbols*}} | **window** *symbols*}	Устанавливает верхнее и нижнее пороговые значения периодического события кадра ошибки, которое запускает соответствующее событие связи. Параметр **threshold high** используется для настройки верхнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 1 до 65535, а его значение по умолчанию – **none** (отсутствует). Параметр **threshold low** используется для настройки нижнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 0 до 65535, а его значение по умолчанию – 1. Параметр **window** используется для настройки размера окна периода кругового запроса.

	Единицей измерения для размера окна является 14881 кадр. Размер окна находится в диапазоне от 100 до 6000 на интерфейсе 1000M Ethernet и в этом случае его значение по умолчанию составляет 100, в то время как на интерфейсе 100M Ethernet диапазон размера окна составляет от 1 до 600 и его значение по умолчанию – 10
ethernet oam link-monitor frame-seconds {**threshold** {**high** {*symbols* | **none**} | **low** {*symbols*}} | **window** *symbols*}	Устанавливает верхнее и нижнее пороговые значения второго события кадра ошибки, которое запускает соответствующее событие. Параметр **threshold high** используется для настройки верхнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 1 до 900, а его значение по умолчанию – **none** (отсутствует). Параметр **threshold low** используется для настройки нижнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 0 до 900, а его значение по умолчанию – 1. Параметр **window** используется для настройки размера окна периода кругового запроса. Его единица измерения – секунда. Находится в диапазоне от 10 до 900, а значение по умолчанию – 60
ethernet oam link-monitor receive-crc {**threshold** {**high** {*symbols* | **none**} | **low** {*symbols*}} | **window** *symbols*}	Устанавливает верхнее и нижнее пороговые значения события ошибки кадра CRC, которое запускает событие ошибки контрольной суммы. Параметр **threshold high** используется для настройки верхнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 1 до 65535, а его значение по умолчанию – **none** (отсутствует). Параметр **threshold low** используется для настройки нижнего порога. Его единица измерения – количество сигналов. Оно находится в диапазоне от 0 до 65535, а его значение по умолчанию – 1. Параметр **window** используется для настройки размера окна периода кругового запроса. Его единица измерения – секунда. Находится в диапазоне от 10 до 180, а значение по умолчанию – 10

35.2.3 Настройка уведомления о неисправностях от удаленного объекта OAM

Вы можете настроить действие по отключению из-за ошибки на интерфейсе. Локальный интерфейс перейдет в отключенное из-за ошибки состояние (errdisabled) в следующих случаях:

1. Превышен верхний порог нормального события соединения на локальном интерфейсе.

2. Удаленный интерфейс, соединенный с локальным интерфейсом, переходит в отключенное из-за ошибки состояние.

3. Функция OAM на удаленном интерфейсе, подключенном к локальному интерфейсу, отключена администратором.

Процедура настройки удаленной индикации неисправностей OAM на интерфейсе показана в следующей таблице:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface *intf-type intf-id*	Вход в режим настройки интерфейса
ethernet oam remote-failure {**critical-event** | **dying-gasp** | **link-fault**} **action error-disable-interface**	Настраивает события, которые инициируют отключение локального интерфейса при возникновении проблем с OAM на удалённом интерфейсе. Параметр **critical-event** используется для активации состояния errdisabled на интерфейсе, когда возникает неопределенное критическое событие. То есть, если на удалённом интерфейсе происходит какое-то событие, которое считается критическим, это может привести к отключению локального интерфейса и переводу его в состояние errdisabled. Параметр **dying-gasp** используется для активации состояния errdisabled на локальном интерфейсе в случае превышения верхнего порога события нормальной связи на локальном интерфейсе или если удалённый интерфейс, подключенный к локальному, переходит в состояние errdisabled, или если администратор отключает функцию OAM на удалённом интерфейсе, который подключен к локальному интерфейсу. Все эти условия могут вызвать перевод локального интерфейса в состояние errdisabled. Параметр **link-fault** используется для активации состояния errdisabled на интерфейсе в случае

	обнаружения потери сигнала приемником. То есть, если приемник обнаруживает потерю сигнала на интерфейсе, это может привести к переводу интерфейса в состояние errdisabled.

Данный коммутатор не может генерировать пакеты LINK FAULT и CRITICAL EVENT. Однако эти пакеты будут обработаны, если они получены от удаленного терминала. Коммутатор может передавать и получать пакеты DYING GASP. Когда локальный порт переходит в состояние errdisabled или закрывается администратором, или функция OAM локального порта закрывается пользователем, пакет DYING GASP будет передан на удаленный терминал, к которому подключается локальный порт.

35.2.4 Отображение информации о протоколе OAM

Для отображения информации о протоколе OAM выполните следующие команды:

Команда	Описание
show ethernet oam discovery interface [*intf-type intf-id*]	Отображает информацию об обнаружении OAM на всех интерфейсах или назначенном интерфейсе
show ethernet oam statistics {**pdu** | **link-monitor** | **remote-failure**} **interface** [*intf-type* intf-id]	Отображает статистическую информацию OAM на всех интерфейсах или назначенном интерфейсе. Параметр **pdu** используется для классификации и подсчета пакетов OAM в соответствии со значением поля «Code» пакета OAM. Параметр **link-monitor** используется для отображения подробной статистической информации о нормальных событиях связи. Параметр **remote-failure** предназначен для отображения подробной статистической информации об удаленной неисправности
show ethernet oam configuration interface [*intf-type intf-id*]	Отображает информацию о конфигурации OAM на всех интерфейсах или назначенном интерфейсе.
show ethernet oam runtime interface [*intf-type intf-id*]	Отображает информацию о работе OAM на всех интерфейсах или назначенном интерфейсе.

35.3 Пример настройки

Необходимо настроить мониторинг OAM на интерфейсе, который соединяет два сетевых коммутатора. Этот мониторинг будет следить за передачей данных между коммутаторами и регистрировать любые ошибочные кадры, которые могут возникнуть на стороне пользовательского доступа.

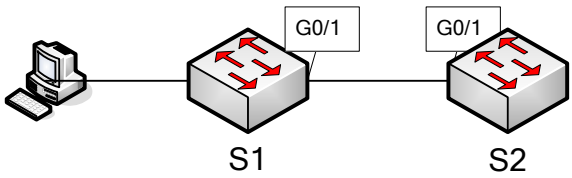

Рисунок 35-2 – Топология сети

Настройка коммутатора S1:

Switch_config_g0/1#ethernet oam

Switch_config_g0/1#ethernet oam mode passive

Switch_config_g0/1#ethernet oam link-monitor frame threshold low 10

Switch_config_g0/1#ethernet oam link-monitor frame window 30

Switch_config_g0/1#show ethernet oam configuration int g0/1

GigaEthernet0/1

General

Admin state : enabled

Mode : passive

PDU max rate : 10 packets/second

PDU min rate : 1 seconds/packet

Link timeout : 1 seconds

High threshold action: no action

Remote Failure

Link fault action : no action

Dying gasp action : no action

Critical event action: no action

Remote Loopback

Is supported : not supported

Loopback timeout : 2

Link Monitoring

Negotiation : supported

Status : on

Errored Symbol Period Event

Window : 10 * 100M symbols

Low threshold : 1 error symbol(s)

High threshold : none

Errored Frame Event

Window : 30 seconds

Low threshold : 10 error frame(s)

High threshold : none

Errored Frame Period Event

Window : 100 * 14881 frames

Low threshold : 1 error frame(s)

High threshold : none

Errored Frame Seconds Summary Event

Window : 60 seconds

Low threshold : 1 error second(s)

High threshold : none

Errored CRC Frames Event

Window : 1 seconds

Low threshold : 10 error frame(s)

High threshold : none

Настройка коммутатора S2:

Switch_config_g0/1#ethernet oam

Switch_config_g0/1#show ethernet oam statistics link-monitor int g0/1

GigaEthernet0/1

Local Link Events:

Errored Symbol Period Event:

No errored symbol period event happened yet.

Errored Frame Event:

No errored frame event happened yet.

Errored Frame Period Event:

No errored frame period event happened yet.

Errored Frame Seconds Summary Event:

No errored frame seconds summary event happened yet.

Errored CRC Frames Event:

No errored CRC frame event happened yet.

Remote Link Events:

Errored Symbol Period Event:

No errored symbol period event happened yet.

Errored Frame Event:

No errored frame event happened yet.

Errored Frame Period Event:

No errored frame period event happened yet.

Errored Frame Seconds Summary Event:

No errored frame seconds summary event happened yet.

Errored CRC Frames Event:

No errored CRC frame event happened yet.

36. CFM

36.1 Введение

CFM (Connectivity Fault Management), представляет собой протокол и механизм, используемый в сетях для мониторинга и управления сетевой связью. Он входит в состав стандарта Ethernet и был разработан для обнаружения и устранения проблем сетевой связи, таких как сбои, петли, потеря сигнала и другие аномалии.

Вот некоторые ключевые аспекты CFM:

Обнаружение и диагностика ошибок: CFM позволяет обнаруживать ошибки и сбои в сети, такие как потеря кадров, дублирование, задержки и другие аномалии. Это помогает операторам сети быстро выявлять и локализовать проблемы для более быстрого их устранения.

Мониторинг канала связи: протокол CFM может отслеживать сетевое подключение между устройствами и предоставлять информацию о состоянии связи между ними.

Управление петлями: CFM может помочь предотвращению возникновения в сети петель, которые приводят к нежелательным циклическим пересылкам данных и сбоям.

Системы оповещения: CFM может генерировать оповещения и сообщения о событиях и проблемах в сети, что упрощает оперативное реагирование на проблемы.

36.2 Настройка CFM

Задачи настройки

- Добавление домена обслуживания
- Добавление ассоциации обслуживания
- Добавление MIP
- Добавление MEP
- Запуск CFM
- Использование функции обратной связи
- Использование функции трассировки соединения

36.2.1 Добавление домена обслуживания

Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
ethernet cfm md mdnf {*string*} <*char_string*> [**level** <0-7> | **creation** <*MHF_creation_type*> | **sit** <*sender_id_type*> | **ip** <*IP_address*>]	Добавляет домен обслуживания с именем char_string

После добавления домена обслуживания система переходит в режим настройки домена.

36.2.2 Добавление ассоциации обслуживания

Выполните следующую команду в режиме настройки домена обслуживания:

Команда	Описание
ma manf {*string*} <*char_string*> **ci** {100ms | 1s | 10s | 1min | 10min} **meps** <*mepids*> [**vlan** <1-4094> | **creation** <*MHF_creation_type*> | **sit** <*sender_id_type*> | **ip** <*IP_address*>]	Добавляет ассоциацию обслуживания с именем char_string

36.2.3 Добавление MIP

Для добавления промежуточной точки домена обслуживания (MIP) выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
ethernet cfm mip add level <0-7> [**vlan** <1-4094>]	Добавляет назначенную VLAN и иерархическую MIP к указанному физическому интерфейсу

36.2.4 Добавление MEP

Для добавления конечной точки ассоциации обслуживания (MEP) выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
ethernet cfm mep add mdnf {*string*} <*char_string*> **manf** {*string*} <*char_string*> **mepid** <1-8191> **rmepid** <1-8191> [**direction** {**up** | **down**} **| ip** <*ip_address*> **| lap** {**all** | **mac** | **rccm** | **eccm** | **xcon** | **none**}]	Добавляет назначенный домен обслуживания и MEP к указанному физическому интерфейсу

36.2.5 Использование функции обратной связи

Выполните следующую команду в режиме управления:

Команда	Описание
ethernet cfm loopback mdnf {*string*} <*char_string*> **manf** {*string*} <*char_string*> **mepid** <1-8191> **mac** <*AA:BB:CC:DD:EE:FF*> **number** <1-64>	Используется для настройки и выполнения циклического самопроверочного тестирования с использованием определенной MEP

36.2.6 Использование функции трассировки соединения

Выполните следующую команду в режиме управления:

Команда	Описание
ethernet cfm linktrace mdnf {*string*} <*char_string*> **manf** {*string*} <*char_string*> **mepid** <1-8191> **mac** <*AA:BB:CC:DD:EE:FF*> [**ttl** {1-255} | **fdb-only** {yes}]	Позволяет определить, какие устройства и сегменты сети находятся между двумя конечными точками Ethernet-соединения

36.3 Пример настройки

Добавьте домен обслуживания с именем customer и иерархией 5, установите ассоциацию обслуживания customer1 для VLAN1. Интервал передачи CCM ассоциации обслуживания составляет 1 с (MEP1, MEP2, MEP2009). Далее добавьте к физическому порту 1 MEP с MEPID 2009, удаленная MEP которой – 2008:

```
Switch_config#ethernet cfm md mdnf string customer level 5
Switch_config_cfm#ma manf string customer1 vlan 1 ci 1s meps 1-2,2009
Switch_config_cfm#interface g0/1
Switch_config_g0/1#ethernet cfm mep add mdnf string customer manf string
customer1 mepid 2009 rmep 2008 direction down lap all
Switch_config_g0/1#exit
Switch_config#ethernet cfm enable
```

37. DHCP-Snooping

37.1 Введение

DHCP-Snooping предназначен для предотвращения действий поддельных DHCP-серверов, которые могут предоставлять DHCP-сервис, путем анализа DHCP-пакетов и поддержания связи между MAC-адресами и IP-адресами. Это механизм, который следит за DHCP-пакетами в сети. Он определяет, какие устройства в сети могут предоставлять DHCP-сервис, а также сохраняет соответствие между MAC-адресами и IP-адресами. Кроме того, на основе этой связи между MAC-адресами и IP-адресами, коммутаторы на уровне L2 могут выполнять функции Dynamic ARP Inspection (DAI) и IP Source Guard для повышения безопасности сети. Если пакеты не соответствуют этой связи между MAC и IP, то они фильтруются, что помогает предотвратить сетевые атаки со стороны несанкционированных пользователей.

37.2 Настройка DHCP-Snooping

Задачи настройки

- Включение/выключение функции DHCP-Snooping
- Включение DHCP-Snooping в VLAN
- Настройка интерфейса в качестве доверенного порта DHCP
- Включение DAI в VLAN
- Настройка интерфейса в качестве доверенного порта ARP

- Включение мониторинга исходного IP-адреса в VLAN
- Настройка интерфейса, доверенного для мониторинга исходного IP-адреса
- Привязка DHCP-Snooping к резервному TFTP-серверу
- Настройка имени файла для резервного копирования привязки DHCP-Snooping
- Настройка интервала резервного копирования привязки DHCP-Snooping
- Настройка или добавление привязки вручную
- Мониторинг и поддержка DHCP-Snooping
- Пример DHCP-Snooping

37.2.1 Включение/выключение функции DHCP-Snooping

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip dhcp-relay snooping	Включает DHCP-Snooping
no ip dhcp-relay snooping	Восстанавливает настройки по умолчанию

Эта команда используется для включения отслеживания DHCP в режиме глобальной конфигурации. После выполнения этой команды коммутатор должен отслеживать все пакеты DHCP и формировать соответствующие отношения привязки.

Если клиент получает адрес коммутатора до выполнения этой команды, коммутатор не сможет добавить соответствующее отношение привязки.

37.2.2 Включение DHCP-Snooping в VLAN

Если в VLAN включено отслеживание DHCP, пакеты DHCP, полученные от всех недоверенных физических портов в VLAN, будут проверяться. Пакеты ответа DHCP, полученные от недоверенных физических портов в VLAN, будут затем отброшены, что не позволит поддельному или неправильно настроенному DHCP-серверу предоставлять услуги распределения адресов. Что касается пакета запроса DHCP от недоверенных портов, если поле аппаратного адреса в пакете запроса DHCP не соответствует MAC-адресу этого пакета, пакет запроса DHCP считается поддельным и используемым в качестве пакета для атаки DHCP DOS. Коммутатор отбросит такой пакет.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание

ip dhcp-relay snooping vlan *vlan_id*	Включает DHCP-Snooping в VLAN
no ip dhcp-relay snooping vlan *vlan_id*	Отключает DHCP-Snooping в VLAN

37.2.3 Включение защиты DHCP от атак в VLAN

Чтобы включить предотвращение атак в VLAN, необходимо настроить допустимое максимальное количество DHCP-клиентов в конкретной VLAN и реализовать принцип «первым пришел – первым обслужен». Когда количество пользователей в конкретной VLAN достигает максимального значения, обслуживание новых клиентов прекращается.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*	Включает предотвращение атак в VLAN
no ip dhcp-relay snooping vlan *vlan_id* **max-client**	Отключает предотвращение атак в VLAN

37.2.4 Настройка интерфейса в качестве доверенного порта DHCP

Если интерфейс настроен в качестве доверенного порта DHCP, пакеты DHCP, полученные от этого интерфейса, не будут проверяться.

Выполните следующие команды в режиме настройки интерфейса:

Команда	Описание
dhcp snooping trust	Настройка интерфейса в качестве доверенного порта DHCP
no dhcp snooping trust	Восстановление режима недоверенного порта DHCP на интерфейсе

По умолчанию интерфейс является недоверенным.

37.2.5 Включение/отключение функции быстрого обновления таблицы привязок

По умолчанию эта функция отключена. Когда эта функция отключена и порт привязан к клиенту A, запрос DHCP того же MAC-адреса на других портах будет рассматриваться как ложная MAC-атака, даже если клиент A находится в автономном режиме.

Когда эта функция включена, вышеупомянутая ситуация не произойдет.

Рекомендуется использовать эту функцию в случае, если клиент часто меняет свой порт и аренду адреса, выдаваемого DHCP-сервером, невозможно изменить в течение короткого периода времени.

Команда	Описание
ip dhcp-relay snooping rapid-refresh-bind	Включает функцию быстрого обновления таблицы привязок
no ip dhcp-relay snooping rapid-refresh-bind	Отключает функцию быстрого обновления таблицы привязок

37.2.6 Включение DAI в VLAN

Когда динамический мониторинг ARP (DAI) проводится на всех физических портах VLAN, полученный пакет ARP будет отклонен, если исходный MAC-адрес и исходный IP-адрес этого пакета не совпадают с настроенным соотношением привязки MAC-IP. Отношения привязки на интерфейсе могут быть динамически связаны с помощью DHCP или настроены вручную. Если ни один MAC-адрес не привязан к IP-адресу на физическом интерфейсе, коммутатор отклоняет пересылку всех пакетов ARP.

Команда	Описание
ip arp inspection vlan *vlanid*	Включает динамический мониторинг ARP на всех недоверенных портах в VLAN
no ip arp inspection vlan *vlanid*	Отключает динамический мониторинг ARP на всех недоверенных портах в VLAN

37.2.7 Настройка интерфейса в качестве доверенного порта ARP

Функция DAI не работает на доверенных интерфейсах. По умолчанию интерфейсы являются недоверенными.

Выполните следующие команды в режиме настройки интерфейса:

Команда	Описание
arp inspection trust	Настройка интерфейса в качестве доверенного порта ARP
no arp inspection trust	Восстановление настройки по умолчанию

37.2.8 Включение мониторинга исходного IP-адреса в VLAN

После включения мониторинга IP-адреса источника в VLAN IP-пакеты, полученные от всех физических портов в VLAN, будут отклонены, если их MAC-адреса источника и IP-адреса источника не совпадают с настроенным соотношением привязки MAC-IP. Отношения MAC-IP на интерфейсе могут быть динамически связаны с помощью DHCP или настроены вручную. Если ни один MAC-адрес не привязан к IP-адресу на физическом интерфейсе, коммутатор отклоняет пересылку всех IP-пакетов, полученных от физического интерфейса.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip verify source vlan *vlanid*	Включает проверку IP-адреса источника на всех недоверенных интерфейсах в VLAN
no ip verify source vlan *vlanid*	Отключает проверку IP-адреса источника на всех интерфейсах VLAN

Если пакет DHCP (также IP-пакет) получен, он будет перенаправлен, поскольку настроено глобальное отслеживание.

37.2.9 Настройка интерфейса, доверенного для мониторинга исходного IP-адреса

Функция определения исходного адреса не будет включена для доверенного интерфейса IP-адреса источника.

Выполните следующие команды в режиме настройки интерфейса:

Команда	Описание
ip-source trust	Настройка интерфейса, которому доверяет мониторинг IP-адреса источника
no ip-source trust	Восстановление настройки по умолчанию

37.2.10 Настройка DHCP-Snooping Option 82

DHCP-Snooping Option 82 добавляет информацию о DHCP-клиенте и устройстве, на котором был получен DHCP-запрос, к DHCP-пакету, который пересылается между DHCP-клиентом и DHCP-сервером, тем самым помогая серверу распределять адреса клиентам.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip dhcp-relay snooping information option	Устанавливает режим, при котором Option 82, имеющая формат по умолчанию, передается, когда DHCP-Snooping пересылает пакеты DHCP
no ip dhcp-relay snooping information option	Устанавливает режим, при котором Option 82 не передается, когда DHCP-Snooping пересылает пакеты DHCP

Чтобы указать формат Option 82, выполните следующие настройки в режиме глобальной конфигурации:

Команда	Описание
ip dhcp-relay snooping information option format {**snmp-ifindex** | **manual** | **hn-type** | **cm-type** [**host**] | **hw-type**}	Устанавливает формат Option 82, который передается в пакетах DHCP при пересылке с помощью DHCP-Snooping
no ip dhcp-relay snooping information option format {**snmp-ifindex** | **manual** | **hn-type** | **cm-type** [**host**] | **hw-type**}	Устанавливает режим, при котором Option 82 не передается, когда DHCP-Snooping пересылает пакеты DHCP

Если для Option 82 установлен формат ручного режима ввода, выполните следующие команды в режиме интерфейса, чтобы настроить идентификатор Circuit-ID:

Команда	Описание
dhcp snooping information circuit-id string [*string*]	Если для Option 82 задан ручной формат, вам необходимо настроить DHCP-Snooping для пересылки пакетов DHCP с указанием информационных параметров, содержимым которых является строка символов. Эта команда задается на порту, к которому подключается клиент
dhcp snooping information circuit-id hex [*xx-xx-xx-xx-xx-xx*]	Если для Option 82 задан ручной формат, вам необходимо настроить DHCP-Snooping для пересылки пакетов DHCP с указанием информационных параметров, содержимое которых представлено в

	шестнадцатеричной системе. Эта команда задается на порту, к которому подключается клиент
no dhcp snooping information circuit-id	Удаляет настроенный вручную идентификатор Option 82

Если для Option 82 установлен формат ручного режима ввода, выполните следующие команды в режиме интерфейса, чтобы настроить идентификатор Remote-ID:

Команда	Описание
dhcp snooping information remote-id string [*STRING*]	Если для Option 82 задан ручной формат, вам необходимо настроить DHCP-Snooping для пересылки пакетов DHCP с указанием информационных параметров, содержимым которых является строка символов. Эта команда задается на порту, к которому подключается клиент
dhcp snooping information remote-id hex [*xx-xx-xx-xx-xx-xx*]	Если для Option 82 задан ручной формат, вам необходимо настроить DHCP-Snooping для пересылки пакетов DHCP с указанием информационных параметров, содержимое которых представлено в шестнадцатеричной системе. Эта команда задается на порту, к которому подключается клиент
no dhcp snooping information remote-id	Удаляет настроенный вручную идентификатор Option 82

Если для Option 82 установлен формат ручного режима ввода, выполните следующие команды в режиме интерфейса, чтобы настроить VSI (информацию производителя):

Команда	Описание
dhcp snooping information vendor-specific string [*STRING*]	Если для Option 82 задан ручной формат, вам необходимо настроить DHCP-Snooping для пересылки пакетов DHCP с указанием информационных параметров, содержимым которых является строка символов. Эта команда задается на порту, к которому подключается клиент
dhcp snooping information vendor-specific hex [*xx-xx-xx-xx-xx-xx*]	Если для Option 82 задан ручной формат, вам необходимо настроить DHCP-Snooping для пересылки пакетов DHCP с указанием информационных

	параметров, содержимое которых представлено в шестнадцатеричной системе. Эта команда задается на порту, к которому подключается клиент
no dhcp snooping information vendor-specific	Удаляет настроенную вручную спецификацию

37.2.11 Настройка политики пакетов DHCP-Snooping с Option82

Вы можете установить политику обработки полученных пакетов запросов DHCP, содержащих Option 82.

Политика отбрасывания: выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
dhcp snooping information drop	Отбрасывает пакеты запроса, содержащие Option 82

Политика присоединения: выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
dhcp snooping information append	Включает функцию добавления Option 82 на порту
dhcp snooping information append first-subop9-param {**hex** *xx-xx-xx-xx-xx-xx* | **vlanip** | **hostname**}	Обозначает первый параметр, содержащийся в поле спецификации производителя Option 82 (subop9)
dhcp snooping information append second-subop9-param {**hex** *xx-xx-xx-xx-xx-xx* | **vlanip** | **hostname**}	Обозначает второй параметр, содержащийся в поле спецификации производителя Option 82 (subop9)

37.2.12 Настройка TFTP-сервера для резервного копирования привязки интерфейсов

После перезагрузки настроек коммутатора, ранее настроенные привязки интерфейсов будет потеряны. После включения мониторинга исходного IP-адреса, коммутатор откажет в передаче всех IP-пакетов. Если настроить TFTP-сервер для резервного копирования привязок, они будут скопированы на сервер через протокол TFTP. После перезагрузки

коммутатора, он автоматически загружает список связей с TFTP-сервера, обеспечивая нормальное функционирование сети.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip dhcp-relay snooping database-agent *ip-address*	Настраивает IP-адрес TFTP-сервера, который должен резервировать привязки интерфейсов
no ip dhcp-relay snooping database-agent *ip-address*	Отменяет использование TFTP-сервера для резервного копирования привязок интерфейсов

37.2.13 Настройка имени файла для резервного копирования привязки интерфейсов

При резервном копировании отношений привязки интерфейсов файл с соответствующим именем будет сохранен на TFTP-сервере. Таким образом, разные коммутаторы могут создавать резервные копии своих привязок на одном и том же TFTP-сервере.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip dhcp-relay snooping db-file *name* [**timestamp**]	Настраивает имя файла для резервной копии привязки интерфейсов
no ip dhcp-relay snooping db-file	Отменяет имя файла для резервной копии привязки интерфейсов

37.2.14 Настройка интервала проверки резервной копии привязки интерфейсов

Отношения привязки MAC-IP на интерфейсах изменяются динамически. Следовательно, вам необходимо проверить, обновились ли они через определенный интервал. Если таблица обновляется (добавляются или удаляются записи привязки), необходимо снова создать резервную копию. Временной интервал по умолчанию составляет 30 минут.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip dhcp-relay snooping write-immediately	Настраивает DHCP Snooping на немедленное резервное копирование при изменении информации о привязке

ip dhcp-relay snooping write-time *num*	Настраивает интервал проверки резервной копии привязки интерфейсов. Единица измерения – минута
no ip dhcp-relay snooping write-time	Возвращает интервал проверки привязки интерфейса к настройкам по умолчанию

37.2.15 Ручная настройка привязки интерфейса

Если хост не получает адрес через DHCP, вы можете добавить элемент привязки на интерфейс коммутатора, чтобы разрешить хосту доступ к сети. Вы можете запустить команду **no ip source binding** *MAC IP*, чтобы удалить элементы из соответствующего списка привязок.

Обратите внимание, что элементы привязки, настроенные вручную, имеют более высокий приоритет, чем элементы, настроенные динамически. Если элементы привязки, настроенные вручную и динамически, имеют один и тот же MAC-адрес, элемент, настроенный вручную, заменяет собой динамически настроенный элемент. Элемент привязки интерфейса принимает MAC-адрес в качестве уникального индекса.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip source binding *MAC IP* **interface** *name vlan-id*	Настраивает привязку интерфейса вручную
no ip source binding *MAC IP vlan-id*	Отменяет элемент привязки интерфейса

37.2.16 Мониторинг и поддержка DHCP-Snooping

Выполните следующие команды в режиме управления:

Команда	Описание
show ip dhcp-relay snooping	Отображает информацию о конфигурации DHCP-Snooping
show ip dhcp-relay snooping binding	Отображает действующие элементы адресной привязки на интерфейсе
show ip dhcp-relay snooping binding all	Отображает все элементы привязки, созданные DHCP-Snooping
[**no**] **debug ip dhcp-relay** [**snooping** | **binding** | **event** | **all**]	Используется для вывода отладочной информации, связанной с передачей пакетов DHCP на коммутаторе, и может быть настроена для отслеживания

	конкретных событий или аспектов этой передачи

Информация о конфигурации DHCP-Snooping:

```
switch#show ip dhcp-relay snooping
 ip dhcp-relay snooping vlan 3
ip arp inspection vlan 3
DHCP Snooping trust interface:
  GigaEthernet0/1
ARP Inspect interface:
  GigaEthernet0/11
```

Информация о действующих элементах адресной привязки на интерфейсе:

```
switch#show ip dhcp-relay snooping binding
Hardware Address    IP Address      remainder time Type          VLAN    interface

00:e0:0f:26:23:89   192.2.2.101     86400     DHCP_SN       3      GigaEthernet0/3
```

Информация обо всех элементах привязки, созданных DHCP-Snooping:

```
switch#show ip dhcp-relay snooping binding all
Hardware Address    IP Address      remainder time Type          VLAN    interface

00:e0:0f:32:1c:59   192.2.2.1       infinite     MANUAL        1      GigaEthernet0/2
00:e0:0f:26:23:89   192.2.2.101     86400     DHCP_SN       3      GigaEthernet0/3
```

Отладочная информация DHCP-Snooping:

```
switch#debug ip dhcp-relay all
DHCPR: receive l2 packet from vlan 3, dilD: 3
DHCPR: DHCP packet len 277
DHCPR: add binding on interface GigaEthernet0/3
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 1
DHCPR: DHCP packet len 300
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 3
DHCPR: DHCP packet len 289
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 1
DHCPR: DHCP packet len 300
DHCPR: update binding on interface GigaEthernet0/3
DHCPR:  IP address: 192.2.2.101, lease time 86400 seconds
DHCPR: send packet continue
```

37.2.17 Пример настройки DHCP-Snooping

Топология сети показана на рисунке 37-1.

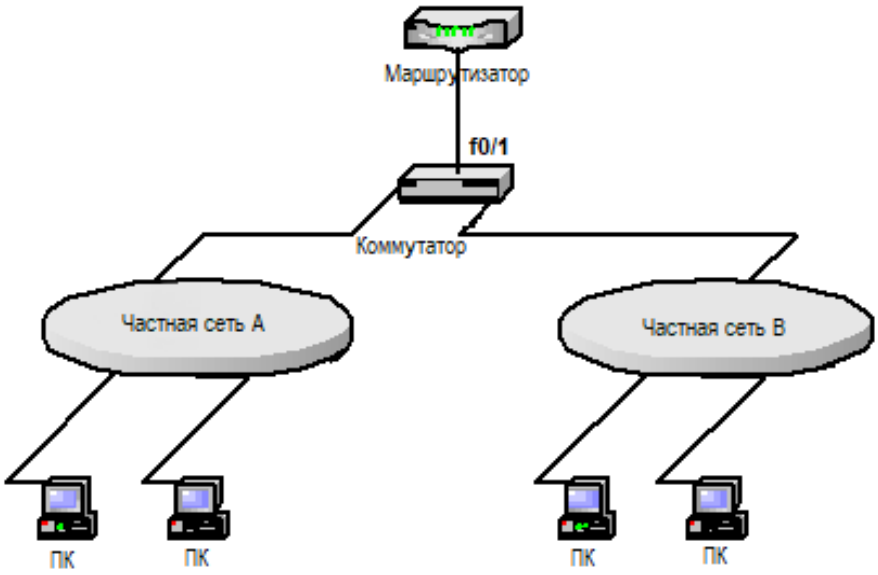

Рисунок 37-1 – Топология сети

Настройка коммутатора

1. Включите DHCP-Snooping в VLAN 1, которая объединяет частную сеть A:

   Switch_config# ip dhcp-relay snooping

   Switch_config# ip dhcp-relay snooping vlan 1

2. Включите DHCP-Snooping в VLAN 2, которая объединяет частную сеть B:

   Switch_config# ip dhcp-relay snooping

   Switch_config# ip dhcp-relay snooping vlan 2

3. Укажите доверенный интерфейс DHCP:

   Switch_config_g0/1#dhcp snooping trust

4. Настройте экземпляр Option 82 вручную.

   interface GigaEthernet0/1

   dhcp snooping information circuit-id hex 00-01-00-05

   dhcp snooping information remote-id hex 00-e0-0f-13-1a-50

```
 dhcp snooping information vendor-specific hex 00-00-0c-f8-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34
 dhcp snooping information append
 dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63
!
interface GigaEthernet0/2
 dhcp snooping trust
 arp inspection trust
 ip-source trust
!
!
!
ip dhcp-relay snooping
ip dhcp-relay snooping vlan 1-100
ip arp inspection vlan 1
ip verify source vlan 1
ip dhcp-relay snooping information option format manual
```

38. MACFF

38.1 Введение

Функция MACFF (MAC-based Forwarding Filter) предназначена для изоляции портов в одной и той же VLAN на коммутаторе, чтобы предотвратить обмен между ними ARP-пакетами. Функция позволяет перенаправить эти пакеты к клиентскому шлюзу через DHCP-сервер и затем к нисходящим портам. Кроме того, MACFF перехватывает ARP-пакеты между нисходящими портами и предоставляет MAC-адрес шлюза, что позволяет всем пакетам между этими портами проходить через шлюз. Для правильной работы MACFF необходима поддержка DHCP-snooping, а также требуется настройка VLAN-адреса управления для коммутатора, поддерживающего MACFF.

38.2 Настройка MACFF

Задачи настройки

- Включение и отключение MACFF
- Включение MACFF в VLAN

- Настройка AR по умолчанию для MACFF в VLAN
- Настройка других AR MACFF в VLAN
- Указание физического порта для отключения MACFF

38.2.1 Включение и отключение MACFF

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
macff enable	Включает MACFF
no macff enable	Восстанавливает настройки по умолчанию

Эта команда используется для включения MACFF в режиме глобальной конфигурации. После выполнения команды коммутатор прослушивает все пакеты ARP.

Прежде чем включить функцию MACFF, необходимо убедиться, что DHCP-Snooping активирован, иначе коммутатор не сможет правильно обработать привязку адресов клиентов.

38.2.2 Включение MACFF в VLAN

Если MACFF включен в VLAN, будут отслеживаться пакеты ARP, полученные от всех недоверенных физических портов DHCP-Snooping во всех VLAN. Если IP-адрес назначения является IP-адресом любого DHCP-клиента, на котором расположен физический порт, принимающий пакеты ARP, эти пакеты ARP будут отброшены; если это пакеты ответа ARP, эти пакеты также будут отброшены. Если другой DHCP-клиент, шлюз по умолчанию или другой служебный адрес запрашивает порт, соответствующий им MAC-адрес будет воспроизводить запрос ARP.

VLAN, в которой включен MACFF, должна иметь адрес управления. В этой VLAN также должно быть включено отслеживание DHCP.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
macff vlan *vlan_id* **enable**	Включает MACFF в VLAN
no macff vlan *vlan_id* **enable**	Отключает MACFF в VLAN

38.2.3 Настройка AR по умолчанию для MACFF в VLAN

Если вы вручную устанавливаете адрес на клиенте (или DHCP-сервер не настраивает шлюз по умолчанию, что не рекомендуется), то коммутатор автоматически включит AR по умолчанию в качестве шлюза, указанного MACFF. Существует только один такой адрес AR.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
macff vlan *vlan_id* **default-ar** *A.B.C.D*	Указывает AR по умолчанию для MACFF в VLAN
no macff vlan *vlan_id* **default-ar** *A.B.C.D*	Удаляет AR по умолчанию для MACFF в VLAN

Перед настройкой AR вы можете запустить **ip sourcebinding xx-xx-xx-xx-xx-xx A.B.C.D interface name**, чтобы добавить таблицу привязки клиента на коммутаторе. Если вы этого не сделаете, MACFF будет считать настроенного вручную клиента незаконным и не станет его обслуживать.

38.2.4 Настройка других AR MACFF в VLAN

После настройки других AR MACFF позволяет DHCP-клиенту получать доступ к этим AR напрямую, без пересылки пакетов через шлюз по умолчанию, назначенный DHCP-сервером.

Эту функцию можно применить на некоторых серверах в сетевом сегменте клиента или на других служебных адресах.

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
macff vlan *vlan_id* **other_ar** *A.B.C.D*	Указывает другие AR MACFF в VLAN
no macff vlan *vlan_id* **other_ar** *A.B.C.D*	Удаляет другие AR MACFF в VLAN

38.2.5 Указание физического порта для отключения MACFF

Если вы укажете физический порт, на котором не должен действовать MACFF, пакеты на этом порту не будут изолированы и пакеты ARP не будут отслеживаться.

Выполните следующие команды в режиме настройки интерфейса:

Команда	Описание
macff disable	Указывает физический порт для отключения MACFF
no macff disable	Указывает физический порт для включения MACFF (он включен по умолчанию)

В настройках по умолчанию портам разрешено включать MACFF.

38.2.6 Включение отладки MACFF

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
debug macff	Включает отладку MACFF
no debug macff	Выключает отладку MACFF

38.2.7 Пример настройки MACFF

Топология сети показана на рисунке 38-1.

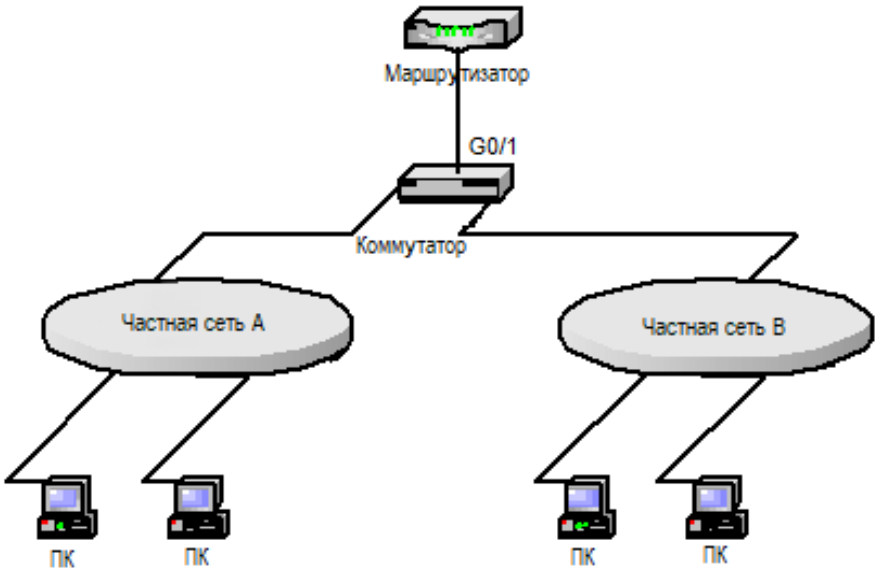

Рисунок 38-1 – Топология сети

1. Включите MACFF в VLAN1, которая соединяет частную сеть A. Шлюз по умолчанию, назначенный DHCP-сервером, – 192.168.2.1.

Switch_config# arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1

Switch_config# ip dhcp-relay snooping

Switch_config# ip dhcp-relay snooping vlan 1

Switch_config# macff enable

Switch_config# macff vlan 1 enable

2. Включите MACFF в VLAN2, которая соединяет частную сеть B. Шлюз по умолчанию, назначенный DHCP-сервером, – 192.168.2.2 (при необходимости шлюзом по умолчанию также может быть 192.168.2.1).

Switch_config# arp 192.168.2.2 00:e0:0f:ea:74:ee vlan 2

Switch_config# ip dhcp-relay snooping vlan 2

Switch_config# macff vlan 2 enable

3. Укажите порты, которые подключают DHCP-сервер, шлюз по умолчанию и другие AR, которым следует доверять.

Switch_config_g0/1#dhcp snooping trust

4. Если хост A нисходящей линии связи VLAN 1 имеет IP-адрес, настроенный вручную, и шлюз по умолчанию, IP-адрес – 192.168.2.102, а MAC-адрес – 6c-62-6d-59-18-b7. Шлюз по умолчанию, 192.168.2.1, позволяет MACFF вступить в силу. Если клиент не настроен вручную, этот шаг не будет выполнен.

Switch_config# arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1

Switch_config# ip source binding 6c:62:6d:59:18:b7 192.168.2.102 interface

GigaEthernet0/1

Switch_config# macff vlan 1 default-ar 192.168.2.1

5. Укажите физический порт в поддерживающей MACFF VLAN для выключения MACFF.

Switch_config_g0/1# macff disable

6. Настройте другие AR, находящиеся в том же сегменте сети клиента. MACFF позволяет клиенту осуществлять прямой доступ без помощи шлюза. Порты, на которых находятся другие точки доступа, должны быть настроены как доверенные порты.

Switch_config_g0/1# macff disable

39. Туннель протокола второго уровня

39.1 Введение

Туннель протокола второго уровня позволяет пользователям соединенных терминалов коммутатора прозрачно передавать пакеты протокола L2 в своих собственных сетях через коммутатор без воздействия соответствующего L2-модуля этого коммутатора. Коммутатор здесь – всего лишь прозрачная среда передачи для пользователей.

39.2 Настройка туннеля

Выполните следующие команды, чтобы настроить функцию туннеля L2:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface <*intf_name*>	Вход в режим настройки интерфейса. Только порты коммутатора поддерживают L2-туннелирование (включая физические порты и порты агрегации)
[**no**] **l2protocol-tunnel** [*stp*]	Указывает протокол L2, который используется для включения функции туннеля на этом порту коммутатора. В настоящее время поддерживается только туннельная функция протокола STP
no spanning-tree	Отключает STP на порту
exit	Возвращает в режим глобальной конфигурации
write	Сохраняет конфигурацию

Команда **no spanning-tree** используется для отключения STP на порту, на котором включена функция туннеля, предотвращая влияние этого порта на устройства, обращающиеся к туннелю, путем отправки пакетов STP.

39.3 Пример настройки туннеля

Топология сети показана на рисунке 39-1.

Рисунок 39-1 – Топология сети

A1/A2/Gather принадлежат базовой сети. C1/C2 обозначает два коммутатора, расположенные в двух филиалах заказчика. Клиент хочет, чтобы две сети управлялись как независимые, то есть базовая сеть является для этого клиента прозрачным каналом передачи. Чтобы реализовать прозрачную передачу STP, необходимо выполнить следующие настройки на каждом коммутаторе:

1. Установите порт g0/2 коммутатора A1, порт g0/1 коммутатора Gather и порт g0/1 коммутатора A2 в режим trunk соответственно.

2. Настройте порт f0/1 коммутатора A1 и порт f0/2 коммутатора A2 как порты доступа, отключите STP, а затем включите функцию туннелирования протокола STP на двух портах.

40. QoS

40.1 Основные понятия

В общем случае коммутатор функционирует в режиме «максимального усилия» (best-effort), при котором он обрабатывает все потоки данных одинаково и старается доставить весь трафик по назначению. Поэтому, если возникает перегрузка, все потоки имеют одинаковый шанс быть отброшенными. Однако в реальных сетях разные потоки имеют различное значение, и функция качества обслуживания (QoS) на коммутаторе может обеспечивать соответствующие услуги разным потокам в зависимости от их значимости. Важные потоки получают более высокий уровень обслуживания.

Для классификации значимости потоков в сети существуют два основных способа:

- В заголовке кадра 802.1Q есть два байта, и 3 бита используются для обозначения приоритета пакета. Существует 8 уровней приоритета, где 0 означает самый низкий приоритет, а 7 – самый высокий.
- Поле DSCP (Differentiated Services Code Point) в заголовке IP-пакета использует нижние 6 битов в области TOS (Type of Service) заголовка IP.

В реальных сетевых приложениях граничный коммутатор назначает разные приоритеты разным потокам данных в зависимости от их важности, а затем предоставляет разные услуги этим потокам на основе их приоритетов. Это способ реализации QoS от источника к приемнику.

Кроме того, вы также можете настроить коммутатор в сети так, чтобы он обрабатывал определенные пакеты с определенными атрибутами (на основе MAC-уровня или информации L3 в пакетах) особым образом. Эти виды поведения называются «одним прыжком» (one-leap behaviors).

Функция QoS коммутатора оптимизирует использование ограниченной пропускной способности, что значительно повышает общую производительность сети.

40.2 Модель QoS между терминалами

Модель описывает набор возможностей QoS между конечными устройствами, то есть возможности сети передавать определенные услуги сетевой связи от одного терминала к другому. Программное обеспечение QoS поддерживает два типа моделей обслуживания: обслуживание с максимальными усилиями и дифференцированное обслуживание.

- Обслуживание с максимальными усилиями – это единая модель обслуживания. В этой модели приложение может отправлять любой объем данных в любое необходимое время без применения разрешений или предварительного уведомления сети. Что касается облуживания с максимальными усилиями, если это разрешено, сеть может передавать данные без каких-либо гарантий надежности, времени задержки или пропускной способности. QoS коммутатора, на котором реализовано обслуживание с максимальными усилиями, по своей природе является услугой, выполняющейся по принципу «первым пришел – первым обслужен» (FCFS).
- Что касается дифференцированного обслуживания, то если в сети должна передаваться специальная услуга, каждый пакет должен быть промаркирован соответствующим тегом QoS. Это обозначение может быть реализовано в различных режимах, например, использование установки статуса приоритета IP в пакете IP-данных. Коммутатор использует это правило QoS для проведения классификации и создания интеллектуальной очереди. QoS коммутатора обеспечивает такие алгоритмы формирования очереди как строгий приоритет (SP), взвешенный циклический перебор (WRR), циклический перебор с дефицитом (DRR) и принцип «первым пришел – первым обслужен» (FCFS).

40.3 Алгоритмы очереди QoS

Каждый алгоритм очереди является важной основой для реализации QoS. QoS коммутатора обеспечивает следующие алгоритмы: строгий приоритет (SP), взвешенный циклический перебор (WRR), взвешенная справедливая очередь (WFQ) и принцип «первым пришел – первым обслужен» (FCFS).

1. Строгий приоритет

Этот алгоритм означает, что сначала предоставляется услуга потоку с наивысшим приоритетом, после чего следует услуга для потока с приоритетом, следующим за наивысшим. Этот алгоритм обеспечивает сравнительно хорошее обслуживание потоков с относительно высоким приоритетом, но его недостаток также очевиден: потоки с низким приоритетом не могут получить обслуживание и в итоге отбрасываются.

2. Взвешенный циклический перебор

Взвешенный циклический перебор (WRR) – эффективное решение проблемы строгого приоритета (SP), при котором очереди с низким приоритетом как правило затухают. WRR – это алгоритм, который выделяет каждой приоритетной очереди определенную полосу пропускания и обеспечивает обслуживание каждой очереди в порядке от высокого приоритета к низкому. После того как очередь с наивысшим приоритетом исчерпала всю свою пропускную способность, система автоматически предоставляет обслуживание очередям со следующим по величине приоритетом.

3. Взвешенная справедливая очередь

Взвешенная справедливая очередь (WFQ) присваивает каждому потоку (или классу обслуживания) вес или приоритет в зависимости от типа данных или других параметров. Это позволяет более важным потокам получать бóльшую полосу пропускания и обслуживаться первыми. WFQ стремится обеспечить справедливое распределение ресурсов между потоками, что означает, что ни один поток не должен доминировать и забирать все доступные ресурсы.

4. Первым пришел – первым обслужен

Алгоритм очереди «первым пришел – первым обслужен», сокращенно FCFS, обслуживает пакеты в соответствии с последовательностью их поступления на коммутатор, соответственно, первый прибывший пакет будет обслужен первым.

40.4 Взвешенное случайное раннее обнаружение

1. Предотвращение перегрузок и традиционный механизм потери пакетов.

Чрезмерная перегрузка может нанести ущерб сетевым ресурсам, поэтому существуют специальные меры для ее устранения. Предотвращение перегрузки – это своего рода метод управления потоком, позволяющий активно отбрасывать пакеты и регулировать сетевые потоки для устранения перегрузки сети посредством мониторинга сетевых ресурсов. Классическое решение проблемы перегрузки сети подразумевает отбрасывание всех входящих пакетов данных, когда длина очереди достигает критического предела. Но в случае с TCP-пакетами, значительная потеря данных может спровоцировать истечение времени ожидания TCP. Это, в свою очередь, может привести к замедленному запуску TCP и механизма избегания перегрузки, являясь причиной так называемой глобальной синхронизации TCP.

2. WRED

Алгоритм WRED используется для предотвращения глобальной синхронизации TCP. WRED помогает пользователям установить порог очереди. Если длина очереди меньше настроенного порога, пакеты не будут отбрасываться; в противном случае пакеты будут отбрасываться случайным образом. Поскольку WRED отбрасывает пакеты случайным образом, предотвращается одновременное замедление скорости передачи несколькими TCP-соединениями, в результате чего глобальная синхронизация TCP не происходит. WRED позволяет другим TCP-соединениям поддерживать относительно высокую скорость передачи, когда пакеты определенного TCP-соединения начинают отбрасываться и скорость их передачи снижается. Независимо от времени, всегда есть TCP-соединения для передачи пакетов с высокой скоростью, что обеспечивает эффективное использование полосы пропускания.

Алгоритм WRED срабатывает, когда пакеты попадают в очередь для отправки, и в зависимости от их размера и параметров **Start**, **Slop** и **Drop priority**, им предоставляются разные приоритеты обработки.

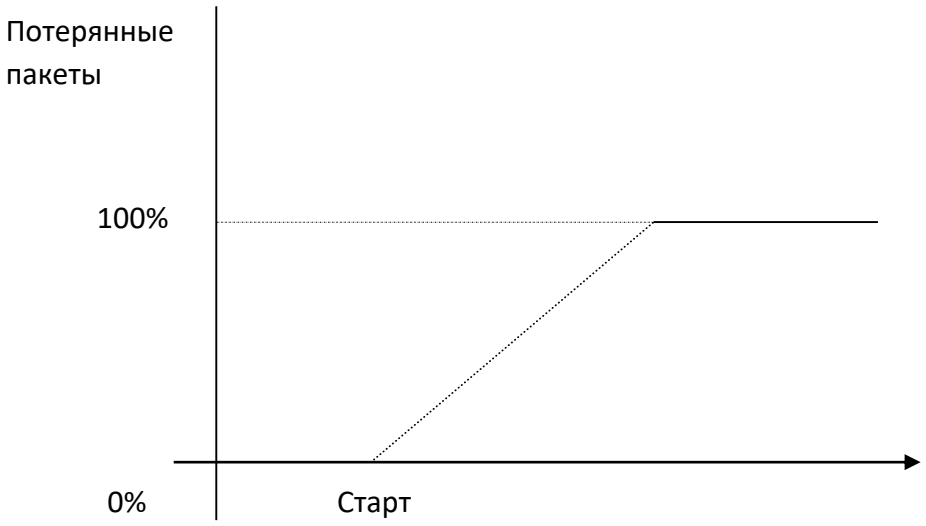

Рисунок 40-1 – Средняя длина очереди

- Если длина очереди меньше начальной, пакеты не будут отбрасываться.
- Когда длина очереди превышает начальную, входящие пакеты начинают отбрасываться случайным образом. Чем длиннее очередь, тем выше скорость отбрасывания.
- Скорость потери пакетов возрастает вместе с увеличением длины очереди.

40.5 Настройка QoS

В обычных условиях коммутатор старается доставить каждый пакет, и при перегрузке все пакеты имеют одинаковый шанс быть отброшенными. Однако в реальности разные пакеты имеют разную важность, и более важные пакеты должны получать более качественное обслуживание. QoS – это механизм, который обеспечивает различные приоритетные услуги для пакетов с разной важностью, что позволяет сети работать более эффективно и с высокой производительностью.

Данная глава рассматривает, как настраивать QoS на коммутаторе, чтобы обеспечить более эффективное управление приоритетами пакетов в сети.

Задачи настройки

- Настройка очереди глобальных приоритетов CoS
- Настройка полосы пропускания для приоритетной очереди CoS
- Настройка политики расписания приоритетных очередей CoS
- Установка значения CoS по умолчанию для порта
- Настройка очереди приоритетов CoS для порта
- Настройка полосы пропускания порта для приоритетной очереди CoS
- Настройка политики планирования очереди приоритетов CoS для порта
- Установка очереди приоритетов CoS на основе DSCP
- Создание карты политики QoS
- Настройка описания карты политики QoS
- Настройка сопоставления потока данных с картой политики QoS
- Настройка действий для потока данных в рамках управления политикой QoS
- Применение политики QoS к порту
- Глобальное применение политики QoS
- Настройка режима доверия
- Отображение таблицы сопоставления политик QoS

40.5.1 Настройка очереди глобальных приоритетов CoS

Задача настройки очереди приоритетов QoS состоит в том, чтобы сопоставить 8 значений CoS, определенных стандартом IEEE802.1p, с очередями приоритетов в коммутаторе. Коммутаторы данной серии имеют 8 очередей приоритетов. В зависимости от очередей коммутатор будет использовать разные политики расписания для реализации QoS.

Если приоритетная очередь CoS настроена в глобальном режиме, это повлияет на конфигурацию всех портов. Если очередь настроена на порту L2, она сможет работать только на этом порту L2.

Войдите в режим управления и выполните одну за другой следующие команды, чтобы настроить глобальную приоритетную очередь CoS:

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] **cos map** *quid cos1…cosn*	Устанавливает приоритетную очередь CoS. *quid* обозначает идентификатор приоритетной очереди CoS. *cos1…cosn* означает значение CoS, определенное стандартом IEEE802.1p
exit	Возвращает в режим EXEC
write	Сохраняет настройки

40.5.2 Настройка полосы пропускания для приоритетной очереди CoS

Полоса пропускания приоритетной очереди означает коэффициент распределения пропускной способности для каждой приоритетной очереди, который устанавливается, когда для политики планирования приоритетной очереди CoS задано значение WRR или WFQ. Всего эта серия коммутаторов имеет 8 очередей приоритетов.

Если команда запущена, это повлияет на пропускную способность для всех приоритетных очередей на всех интерфейсах. Эта команда выполняется только в том случае, если для режима расписания очереди установлено значение WRR/WFQ. Команда определяет значение веса пропускной способности очереди приоритетов CoS, когда используется политика расписания WRR/WFQ.

Выполните следующие команды одну за другой, чтобы установить пропускную способность для приоритетной очереди CoS:

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] **scheduler weight bandwidth** *weight1...weightn*	Устанавливает пропускную способность для очереди приоритетов CoS. *weight1…weightn* обозначает веса 8 очередей приоритетов CoS WRR/DRR
exit	Возвращает в режим EXEC
write	Сохраняет настройки

40.5.3 Настройка политики расписания приоритетных очередей CoS

Коммутатор имеет множество исходящих очередей на каждом своем порту. Данная серия коммутаторов имеет 8 приоритетных очередей. Исходящие очереди могут использовать следующие четыре режима расписания:

- SP (строгий приоритет) – это алгоритм, в котором пересылка пакетов в очереди с низким приоритетом возможна только тогда, когда очередь с высоким приоритетом равна нулю. Если в очереди с высоким приоритетом есть пакеты, они будут пересылаться безоговорочно.
- WRR (взвешенный циклический перебор) – это алгоритм, который выделяет каждой приоритетной очереди определенную полосу пропускания и обеспечивает обслуживание каждой приоритетной очереди в соответствии с порядком от высокого приоритета к низкому.
- WFQ (взвешенная справедливая очередь) – это алгоритм, который выделяет каждой приоритетной очереди определенную полосу пропускания в соответствии с приоритетом потока.
- FCFS (первым пришел – первым обслужен) это алгоритм, который обеспечивает обслуживание пакетов в соответствии с последовательностью их поступления на коммутатор. Первый прибывший пакет обслуживается в первую очередь.

Войдите в режим управления и установите политику планирования обработки приоритетных очередей CoS:

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] **scheduler policy** {**sp** | **wrr|wfq|fcfs** }	Устанавливает политику планирования обработки приоритетных очередей CoS
exit	Возвращает в режим EXEC
write	Сохраняет настройки

40.5.4 Установка значения CoS по умолчанию для порта

Если порт коммутатора получает кадр данных без тега, коммутатор добавит к нему приоритет CoS по умолчанию. Установка значения CoS по умолчанию для порта – это определение приоритета, который будет присвоен непомеченным данным при их получении на этом порту.

Войдите в режим управления и выполните следующие команды, чтобы установить значение CoS по умолчанию для порта:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в режим настройки выбранного интерфейса
[**no**] **cos default** *cos*	Устанавливает значение CoS для полученных нетегированных кадров. *cos* означает соответствующее значение CoS.

exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC
write	Сохраняет настройки

40.5.5 Установка очереди приоритетов CoS для порта

Если приоритетная очередь настроена на порту L2, она будет использоваться этим портом L2; в противном случае вам следует выполнить настройку глобальной очереди приоритетов CoS.

Войдите в режим управления и выполните следующие команды, чтобы установить значение CoS по умолчанию для порта:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в режим настройки выбранного интерфейса
[**no**] **cos map** *quid cos1…cosn*	Настраивает приоритетную очередь CoS. *quid* обозначает идентификатор приоритетной очереди CoS. *cos1…cosn* – значение CoS, определенное стандартом IEEE802.1p
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC

40.5.6 Настройка полосы пропускания порта для приоритетной очереди CoS

Если полоса пропускания приоритетной очереди задана на порту L2, она будет действительна только на этом порту L2; в противном случае вам следует выполнить глобальную настройку пропускной способности очереди.

Войдите в режим управления и выполните следующие команды одну за другой, чтобы настроить полосу пропускания порта для приоритетной очереди CoS:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в режим настройки выбранного интерфейса
[**no**] **scheduler weight bandwidth** *weight1...weightn*	Устанавливает пропускную способность приоритетной очереди CoS.

	weight1…weightn обозначает веса 8 очередей приоритетов CoS WRR/DRR
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC
write	Сохраняет настройки

40.5.7 Настройка политики планирования очереди приоритетов CoS для порта

Если политика планирования приоритетной очереди задана на порту L2, она будет действительна только на этом порту L2; в противном случае вам следует выполнить глобальную настройку политики.

Войдите в режим управления и выполните следующие команды одну за другой, чтобы установить политику планирования очереди приоритетов CoS для порта:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в режим настройки выбранного интерфейса
[**no**] **scheduler policy** {**sp** | **wrr** | **wfq**}	Устанавливает политику планирования приоритетной очереди CoS. **sp** означает использование политики расписания SP. **wrr** означает использование политики расписания WRR. **wfq** означает использование политики расписания WFQ. **drr** означает использование политики расписания DRR
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC
write	Сохраняет настройки

40.5.8 Установка очереди приоритетов CoS на основе DSCP

На основе значения DSCP (Differentiated Services Code Point) происходит переотображение очереди COS, изменяется значение DSCP и бит перегрузки.

Войдите в режим управления и выполните следующие команды, чтобы установить значение CoS по умолчанию для порта:

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**]**dscp map** *word* {**cos** *cos-value*} dscp	Задает соответствие между значениями DSCP и приоритетами CoS. *word* обозначает конкретный диапазон значений DSCP, который будет настраиваться. *cos-value* указывает на значение приоритета CoS, которое будет сопоставлено выбранному диапазону DSCP
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC

40.5.9 Создание карты политики QoS

Классификация потока означает идентификацию класса пакетов с определенными атрибутами путем применения определенных правил и выполнение определенных действий в отношении этих пакетов.

Выполните следующие действия, чтобы настроить политику QoS.

Войдите в режим управления, а затем выполните следующие команды, чтобы создать новую карту политики QoS.

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] **policy-map** *name*	Вход в режим настройки карты политики QoS. *name* означает имя политики
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC

40.5.10 Настройка описания карты политики QoS

Войдите в режим управления и выполните следующие команды, чтобы задать описание карты политики QoS. Эти настройки заменят предыдущие настройки.

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] **policy-map** *name*	Вход в режим настройки карты политики QoS. *name* означает имя политики

description description-text	Создает описание политики QoS. *description-text* означает текст, описывающий политику
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC

40.5.11 Настройка сопоставления потока данных с картой политики QoS

Правила классификации для потока данных QoS определяются в соответствии с требованиями администратора. Эти правила могут быть простыми, например, идентификация потоков с разными приоритетами на основе поля ToS в заголовке IP-пакета, или сложными, когда пакеты классифицируются на основе различной информации о комплексном уровне связи, сетевом уровне и транспортном уровне (например, MAC-адрес, исходный IP-адрес, целевой IP-адрес или идентификатор порта приложения). Обычно стандарт классификации ограничивается заголовком инкапсулированного пакета, но иногда в качестве критерия используется содержание пакета.

Войдите в режим управления, настройте потоки данных для сопоставления политике и замените ими предыдущие настройки, выполнив следующие действия:

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**]**policy-map** *name*	Вход в режим настройки карты политики QoS. *name* означает имя политики
description description-text	Создает описание политики QoS. *description-text* означает текст, описывающий политику
classify {**any** | **cos** *cos* | **icos** *icos* | **vlan** *vlanid* | **ivlan** *ivlanid* | **ethernet-type** *ethernet-type* | **precedence** *precedence-value* | **dscp** *dscp-value* | **tos** *tos-value* | **diffserv** *diffserv-value* | **ip** *ip-access-list* | **ipv6** *ipv6-access-list* | **mac** *mac-access-list*} **no classify** {**cos** | **icos** | **vlan** | **ivlan** | **ethernet-type** | **precedence** | **dscp** | **tos** | **diffserv** | **ip** | **ipv6** | **mac**}	Настраивает классификацию пакетов. ***cos*** – соответствующее значение CoS в диапазоне от 0 до 7. ***icos*** означает сопоставленное внутреннее значение CoS, которое может принимать значения от 0 до 7. ***vlanid*** обозначает соответствующую VLAN, которая находится в диапазоне от 1 до 4094. ***ivlanid*** обозначает соответствующую внутреннюю VLAN, которая находится в диапазоне от 1 до 4094.

	ethernet-type обозначает соответствующий тип пакета, который находится между 0x0600 и 0xFFFF. ***precedence-value*** обозначает значение приоритета в поле ToS IP-пакета, которое может быть от 0 до 7. ***dscp-value*** определяет значение поля DSCP в заголовке IP-пакета, диапазон от 0 до 63. ***tos-value*** – значение, которое устанавливается для полей latency, throughput, reliability и cost в поле ToS IP-пакета. Оно может варьироваться от 0 до 15. ***diffserv-value*** обозначает все поле ToS. ***ip-access-list*** и ***ipv6-access-list***: эти параметры используются для сопоставления пакетов с соответствующими списками доступа на основе IP-адресов и IPv6-адресов. Имена списков доступа могут содержать от 1 до 20 символов. ***mac-access-list*** настраивает имя соответствующего списка доступа MAC. Имя может содержать от 1 до 20 символов
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC

40.5.12 Настройка обработки потока данных в рамках управления политикой QoS

Команда **action** определяет, какие действия должны выполняться для потока данных в соответствии с правилами фильтрации. Например, ограничение пропускной способности, отбрасывание данных, их обновление и т. д.

Войдите в режим управления и выполните следующие команды, чтобы установить необходимые действия для политики, сопоставляющейся с потоком данных. Эти действия заменят предыдущие настройки.

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**]**policy-map** *name*	Вход в режим настройки карты политики QoS.

	name означает имя политики
action {**bandwidth** *max-band* |**cos** *cos* | **drop** | **dscp** *dscp-value* | **precedence** *precedence-value* | **forward** | **icos** *icos* | **ivlanid** {**add** *addivlanid* | *ivlanid*} | **monitor** *session-value* | **queue** *queue-value* | **redirect** *interface-id* | **stat-packet** | **stat-byte** | **vlanid** {**add** *addvlanid* | *vlanid*} | **copy-to-cpu**} **no action** {**bandwidth** | **cos** | **drop** | **dscp** | **precedence** | **forward** | | **icos** | **ivlanid** | **monitor** | **queue** | **redirect** | **stat-packet** | **stat-byte** | **vlanid** | **copy-to-cpu**}	Настраивает политику. ***max-band*** обозначает занимаемую максимальную полосу пропускания: 1 – 163840. Единица: 64 Кбит/с ***cos***: настраивает соответствующее значение CoS потока; допустимый диапазон от 0 до 7. ***drop*** означает отбросить совпавшие пакеты. ***dscp-value***: устанавливает для соответствующего поля DSCP значение 0 – 63. ***precedence-value*** обозначает значение приоритета в поле ToS IP-пакета, которое может быть от 0 до 7. ***forward***: не выполняет никаких операций с совпадающими пакетами. ***icos*** означает сопоставленное внутреннее значение CoS, которое может принимать значения от 0 до 7. ***ivlanid*** используется для замены или добавления внутреннего идентификатора виртуальной локальной сети в диапазоне от 1 до 4094. ***session-value*** используется для настройки зеркалирования; значение находится в диапазоне от 1 до 4. ***queue-value*** используется для настройки очереди сопоставления; значение находится в диапазоне от 1 до 8. ***interface-id***: перенаправляет выходной порт соответствующего потока. ***stat-packet*** означает количество пакетов в статистике. ***stat-byte*** означает количество байтов статистики. ***vlanid*** используется для замены или добавления внешнего идентификатора VLAN, который находится в диапазоне от 1 до 4094.

	copy-to-cpu означает отправку сообщения в процессор
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC

40.5.13 Применение политики QoS к порту

Политика QoS может быть применена к порту. К одному и тому же порту можно применить несколько политик QoS, а одну и ту же политику QoS можно применить к нескольким портам. При этом политики, примененные ранее, имеют больший приоритет перед политиками, которые применены позже. Если пакету назначены две политики, и действия в них противоречат друг другу, то применяются действия из первой сопоставленной политики. После применения QoS-политики к порту, коммутатор автоматически добавляет политику блокировки для предотвращения прохождения других потоков данных, которым не разрешено проходить через этот порт. Когда все политики на порту удаляются, коммутатор автоматически удаляет политику блокировки по умолчанию с порта.

Войдите в режим управления и выполните следующие команды, чтобы применить политику QoS.

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в режим настройки выбранного интерфейса
[**no**] **qos policy** *name* {**ingress** | **egress**}	Применяет политику QoS к порту. ***name*** означает имя карты политики QoS. **ingress** означает оказывать влияние на входящие потоки. **egress** означает оказывать влияние на исходящие потоки
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC

40.5.14 Глобальное применение политики QoS

Войдите в режим управления и выполните следующие команды, чтобы применить политику QoS:

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] **qos policy** *name* **ingress**	Применяет политику QoS глобально. ***name*** означает имя карты политики QoS.

	ingress означает оказывать влияние на входящие потоки
exit	Возвращает в режим EXEC

40.5.15 Настройка режима доверия

При настройке глобального режима доверия есть три варианта: **cos**, **dscp** или **untrust**. Данные будут сопоставляться с очередью в соответствии с выбранным вариантом. Если выбран вариант untrust, то приоритет пакета будет сопоставлен с очередью по умолчанию.

Выполните следующие команды в режиме управления:

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] **qos trust** {**cos** | **dscp** | **untrust**}	Настройка глобального режима доверия. **untrust** означает не доверять каким-либо режимам
exit	Возвращает в режим EXEC

40.5.16 Отображение карты политики QoS

Вы можете запустить команду **show**, чтобы отобразить все или некоторые назначенные карты политик QoS.

Выполните следующую команду в режиме управления, чтобы отобразить таблицу сопоставления:

Команда	Описание
show policy-map [*policy-map-name* | *interface* | **global**]	Отображает все или некоторые назначенные карты политик QoS. **policy-map-name** означает имя таблицы сопоставления QoS. **interface** обозначает политику QoS, применяемую к порту. **global** означает политику QoS для глобального применения

40.6 Пример настройки QoS

В следующем примере показано, как настроить политику QoS, соответствующую списку IP-доступа на порту g0/2:

```
ip access-list extended ipacl

permit ip 192.168.20.2 255.255.255.255 192.168.20.210 255.255.255.255
```

policy-map pmap

classify ip ipacl

action drop

interface g0/2

qos policy pmap ingress

41. Предотвращение атак

41.1 Введение

41.1.1 Функция фильтрации

Чтобы гарантировать оптимальное использование пропускной способности сети, в этой серии коммутаторов предусмотрена функция фильтрации, предотвращающая захват злонамеренным трафиком большого объема сетевой пропускной способности.

Фильтр может идентифицировать пакеты, полученные интерфейсом коммутатора, и вычислять их в соответствии с типом пакета. Учитывая распространенные методы атак, фильтр может вычислить количество ARP, IGMP или IP-сообщений, которые хост отправляет за определенное время. Как только их число превысит пороговое значение, коммутатор прекратит предоставлять какие-либо услуги этим хостам.

Фильтр ограничивает пакет от определенного хоста, блокируя адрес источника. При атаке ARP фильтр блокирует MAC-адрес источника; при IP-атаках, таких как сканирование Ping и сканирование TCP/UDP, фильтр блокирует исходный IP-адрес.

41.1.2 Режимы фильтрации

Режим фильтрации определяет, как коммутатор распознает источник атаки. Существует два режима:

- Временная блокировка адреса источника (Raw)

  В этом режиме коммутатор будет отбрасывать пакеты с источником атаки в течение определенного времени, после чего ограничение на атакующий источник будет снято и будет проведен новый расчет.

  В режиме Raw будут заблокированы все пакеты с исходным адресом источника. Например, если заблокирован MAC-адрес атакующего источника, то все пакеты с исходным MAC-адресом, совпадающим с MAC-адресом атакующего источника, будут отбрасываться, независимо от типа пакета (ARP, ICMP, DHCP и другие).

- Опрос заблокированного адреса источника (Hybrid)

  В режиме Hybrid, после блокировки атакующего источника, коммутатор продолжает отслеживать количество пакетов с этого источника в течение определенного интервала

времени. Если количество пакетов превышает заданный порог, блокировка остается в силе, в противном случае она снимается. В режиме Hybrid также можно настроить количество пакетов при первичном определении атакующего источника и порог пакетов при отслеживании.

Продолжая отслеживание заблокированного источника, коммутатор будет производить непрерывный подсчет пакетов, и при этом учитывая их тип. Например, если MAC-адрес хоста заблокирован из-за обнаружения ARP-атаки, коммутатор будет продолжать отправлять IP-пакеты от этого хоста, если при этом не обнаружена атака на уровне IP.

Выбор режима фильтрации зависит от потребностей конкретной сети. Режим Raw строго ограничивает атакующий источник и снижает нагрузку на процессор коммутатора. Режим Hybrid позволяет более гибко управлять атакующим источником и быстро возобновлять коммуникацию после окончания атаки. Однако в режиме Hybrid есть ограничение на количество одновременно поддерживаемых фильтров. В случае необходимости применения большего числа фильтров, автоматически будет использован режим Raw.

41.2 Настройка защиты от атак

Когда количество сообщений IGMP, ARP или IP, отправленных хостом за определенный интервал, превышает пороговое значение, считается, что хост атакует сеть.

Вы можете выбрать тип защиты (ARP, IGMP или IP), порт предотвращения атак и параметр обнаружения атак.

Задачи настройки

- Настройка параметров фильтрации атак
- Настройка типа защиты
- Включение функции предотвращения атак
- Проверка состояния защиты от атак

41.2.1 Настройка параметров фильтрации атак

В глобальной конфигурации выполните следующую команду, чтобы настроить параметры фильтрации:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **filter period** *time*	Устанавливает временной период обнаружения атак. Единица измерения – секунда
Switch_config# **filter threshold** [**arp** | **bpdu** | **dhcp** | **igmp** | **ip** | **icmp** | **icmpv6**] *value*	Устанавливает пороговое значение количества пакетов различных типов

Switch_config# **filter block-time** *time*	Устанавливает время отказа в обслуживании (время блокировки) источника атаки при его обнаружении. Единица измерения – секунда
Switch_config# **filter polling period** *time*	Устанавливает период опроса фильтра в режиме Hybrid. Единица измерения – секунда
Switch_config# **filter polling threshold** [**arp** | **bpdu** | **dhcp** | **igmp** | **ip** | **icmp** | **icmpv6**] *value*	Устанавливает пороговое значение для фильтрации определенных типов сетевого трафика
Switch_config# **filter polling auto-fit**	Настраивает параметры опроса, которые автоматически адаптируются к фильтру источника атаки. По умолчанию эта команда работает эффективно, устанавливая период опроса равным периоду фильтра атаки и порог пакетов опроса равным 3/4 от порога пакетов фильтра атаки. Команда позволяет опросному фильтру автоматически подстраиваться под параметры фильтра атаки для более эффективной работы
Switch_config# **filter shutdown-action**	Отключает порт при обнаружении атаки в режиме Raw

41.2.2 Настройка типа защиты

В режиме глобальной конфигурации и режиме настройки интерфейса используйте следующую команду для установки типа фильтра атак.

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **filter dhcp**	Включает фильтр атак пакетов DHCP в глобальной конфигурации
Switch_config# **filter icmp**	Включает фильтр атак пакетов ICMP
Switch_config# **filter icmpv6**	Включает фильтр атак пакетов ICMPv6
Switch_config# **filter igmp**	Включает фильтр атак пакетов IGMP
Switch_config# **filter ip source-ip**	Включает фильтр IP-атак в глобальной конфигурации
Switch_config# **interface intf-name**	Вход в режим настройки интерфейса
Switch_config_intf# **filter arp**	Включает фильтр атак пакетов ARP на интерфейсе
Switch_config_intf# **filter bpdu**	Включает фильтр атак пакетов BPDU на интерфейсе

Switch_config_intf# **filter dhcp**	Включает фильтр атак пакетов DHCP на интерфейсе
Switch_config_intf# **filter icmp**	Включает фильтр атак пакетов ICMP на интерфейсе
Switch_config_intf# **filter icmpv6**	Включает фильтр атак пакетов ICMPv6 на интерфейсе
Switch_config_intf# **filter ip source-ip**	Включает фильтр атак IP-пакетов на интерфейсе

Фильтр ARP-атак использует комбинацию MAC-адрес хоста + исходный порт в качестве источника атаки. То есть, для пакетов с одним и тем же MAC-адресом, но поступающих с разных портов, подсчет не будет суммироваться. Фильтры атак IGMP и IP используют в качестве источника атаки IP-адрес хоста и исходный порт.

- Невозможно одновременно активировать защиту от атак по протоколу IGMP и атак по протоколу IP.
- Фильтры для IP, ICMP, ICMPv6 и DHCP применяются только в режиме настройки глобальных параметров и режиме настройки интерфейса.

41.2.3 Включение функции предотвращения атак

После того, как все параметры фильтрации установлены, вы можете запустить функцию предотвращения атак. Обратите внимание, что при запуске функции задействуется часть ресурсов процессора.

Команда	Описание
Switch_config# **filter enable**	Включает функцию предотвращения атак
Switch_config# **filter mode** [**raw** | **hybrid**]	Устанавливает режим фильтрации Raw или Hybrid

Используйте команду **no filter enable**, чтобы отключить функцию и снять блокировку со всех источников атак.

41.2.4 Проверка состояния защиты от атак

После того, как функция предотвращения атак активирована, вы можете запустить следующую команду, чтобы проверить состояние защиты:

Команда	Описание
show filter	Отображает состояние защиты

show filter summary	Отображает конфигурацию параметров и сводную информацию фильтра

41.3 Примеры настройки защиты от атак

Примеры, показанные в этой главе, являются лишь справочной информацией по настройке фильтра. Проводить настройку следует в соответствии с фактическим состоянием конкретной сети.

41.3.1 Использование фильтра ARP для защиты локальной сети

Как показано на следующем рисунке, настройте фильтр ARP-атак на коммутаторе.

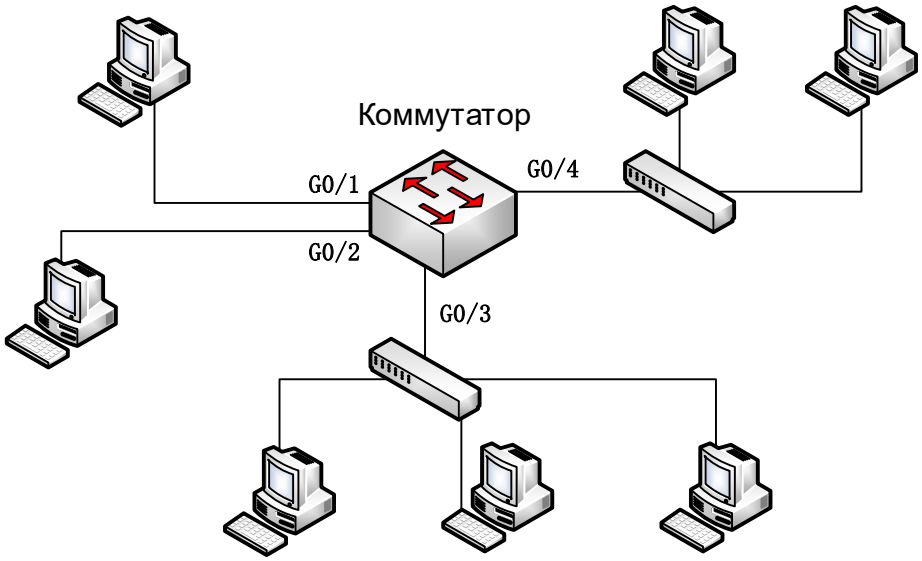

Рисунок 41-1 – Топология сети

Установите параметр фильтра. Хост, отправляющий более 100 ARP-сообщений за 10 секунд, будет считаться источником атаки:

Switch# config

Switch_config# filter period 10

Switch_config# filter threshold arp 100

Установите фильтр APR-атаки для четырех портов:

Switch_config# interface range g0/1-4

Switch_config_intf# filter arp

Установите режим Raw и включите фильтр:

Switch_config_intf# exit

Switch_config# filter mode raw

Switch_config# filter enable

41.3.2 Использование IP-фильтра для защиты сети 3-го уровня

Как показано на рисунке 41-2, коммутатор подключен к нескольким локальным сетям (LAN), серверам и интернету. Защита от атак по протоколу IP может блокировать сканирование IP-адресов между разными подсетями и быстро устанавливать блокировку для больших сетевых соединений, которые могут быть инициированы, например, при использовании BitTorrent.

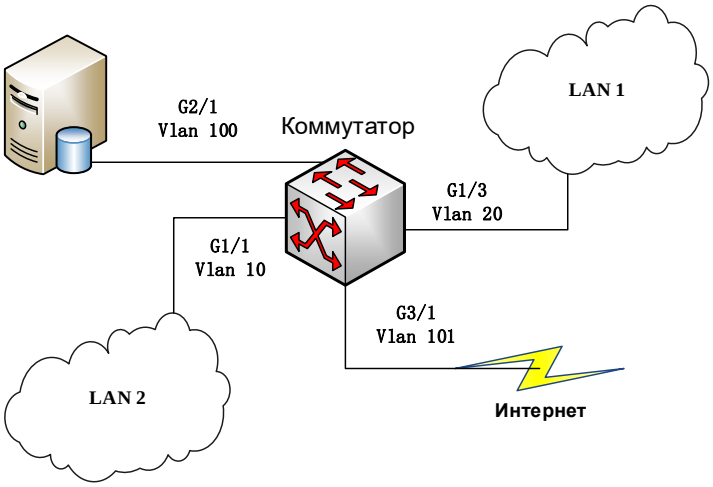

Рисунок 41-2 – Топология сети

Установите параметр фильтра. Источником атаки будет считаться хост, отправляющий более 300 ARP-сообщений за 1 минуту:

Switch# config

Switch_config# filter period 60

Switch_config# filter threshold ip 300

Включите фильтр IP-пакетов в режиме настройки глобальной конфигурации и режиме интерфейса. Обратите внимание, что интерфейс, соединяющий сервер и внешнюю сеть, настраивать не нужно:

Switch_config# filter ip source-ip

```
Switch_config# interface g1/1
Switch_config_g1/1# filter ip source-ip
Switch_config_g1/1# interface g1/3
Switch_config_g1/3# filter ip source-ip
Switch_config_g1/3# exit
Switch_config#
```

Включите фильтр:

```
Switch_config# filter enable
```

42. Предотвращение DoS-атак

42.1 Введение

42.1.1 Понятие DoS-атаки

DoS (Denial of Service) атака – это тип кибератаки, целью которой является нарушение или блокировка доступности определенного сервиса, ресурса или сети для законных пользователей. Распространенные DoS-атаки включают атаки на пропускную способность сети и атаки на подключение. В ходе DoS-атаки злоумышленники могут перегрузить серверы, сетевую инфраструктуру или приложения большим количеством запросов или данных, что может привести к отказу в обслуживании.

Для предотвращения DoS-атак, таких как Pingflood, SYNflood, Landattack, Teardrop и TCP с недопустимыми флагами, требуется коммутатор, обеспечивающий множество методов защиты. Когда коммутатор подвергается атаке, ему необходимо определить, какой это тип атаки, и особым образом обрабатывать пакеты атаки, например, отправляя их в ЦП и удаляя их.

42.1.2 Типы DoS-атак

Злоумышленники будут создавать различные типы DoS-пакетов для атаки на серверы. Ниже приведены распространенные пакеты DoS-атак.

1. Ping of Death

Ping of Death – это ненормальный пакет Ping, который утверждает, что его размер превышает порог ICMP, и вызывает выход из строя стека TCP/IP, что в конечном итоге приводит к выходу из строя принимающего хоста.

2. Tear Drop

Для реализации атаки TearDrop используется информация из заголовка пакета в доверенном фрагменте IP стека TCP/IP. Фрагмент IP имеет информацию, указывающую,

какая часть исходного пакета в нем содержится, и некоторые стеки TCP/IP выходят из строя при получении поддельного фрагмента, содержащего перекрывающееся смещение.

3. SYN Flood

Стандартное TCP-соединение должно пройти три процесса подтверждения. Клиент отправляет сообщение SYN на сервер, сервер возвращает сообщение SYN-ACK, а клиент отправляет сообщение ACK на сервер после получения сообщения SYN-ACK. Таким образом устанавливается TCP-соединение.

При атаке SYN Flood злоумышленник посылает большое количество запросов SYN на сервер, но не завершает установление соединения отправкой ACK. Это означает, что сервер остается в состоянии ожидания исходящих ACK от клиента. Поскольку сервер ожидает ACK для каждого запроса SYN, атака SYN Flood может привести к израсходованию ресурсов сервера, таких как память и количество одновременных соединений. Это может сделать сервер недоступным для легитимных запросов, так как все его ресурсы будут заняты обработкой поддельных соединений.

4. Land Attack

Злоумышленник отправляет специальное сообщение SYN (адрес источника и адрес назначения – это один и тот же служебный адрес). Сообщение SYN заставляет сервер отправлять сообщение SYN-ACK самому себе, следовательно, этот адрес также отправляет сообщение ACK и создает нулевую ссылку. Каждая из этих ссылок будет сохраняться до истечения времени ожидания, таким образом в итоге сервер выйдет из строя. Land Attack можно разделить на IPland и MACland.

42.2 Настройка защиты от DoS-атак

Для предотвращения DoS-атак необходимо настроить связанные подфункции, и после этого коммутатор будет отбрасывать соответствующие пакеты атаки. Это гарантирует, что пропускная способность коммутатора не будет использована до исчерпания.

42.2.1 Глобальная настройка предотвращения DoS-атак

При настройке предотвращения DoS-атак в глобальном режиме, и каждая подфункция может защитить от различных типов DoS-пакетов. Подфункция DoS IP может предотвратить атаки LAND, а подфункция DoS ICMP может предотвратить Ping of Death. Вы можете установить соответствующую подфункцию в соответствии с фактическими требованиями.

Настройте функцию предотвращения DoS-атак в режиме EXEC.

Команда	Описание
config	Вход в режим глобальной конфигурации

[**no**] **dos enable** {**all** | **icmp** *icmp-value* | **ip** | **l4port** | **mac** | **tcpflags** | **tcpfrag** *tcpfrag-value* | **tcpsmurf** | **icmpsmurf** | **ipsmurf**}	Настраивает опции для противодействия всем типам пакетов DoS-атак. **icmp**: настраивается для предотвращения атак PING на пакеты ICMP, длина которых превышает значение *icmp*, которое означает максимальную длину ICMP-пакета, то есть 0 – 1023 байта. **ip**: настраивается для предотвращения обработки тех IP-пакетов, адреса источника которых совпадают с адресами назначения. **l4port**: настраивается для предотвращения тех TCP/UDP-пакетов, чьи идентификаторы исходного порта являются идентификаторами порта назначения. **mac**: настраивается для предотвращения обработки пакета, MAC-адреса источника которого совпадают с MAC-адресами назначения. **tcpflags**: настраивается для предотвращения обработки TCP-пакетов, содержащих недопустимые TCP-флаги. **tcpfrag**: настраивается для предотвращения обработки обнаруженных TCP-пакетов, минимальное значение TCP-заголовка которых равно значению *istcpfrag*. **tcpsmurf**: настраивается для предотвращения обработки тех TCP-пакетов, адреса назначения которых являются широковещательными. **icmpsmurf**: настраивается для предотвращения обработки тех ICMP-пакетов, адреса назначения которых являются широковещательными. **ipsmurf**: настраивается для предотвращения обработки тех IP-пакетов, адреса назначения которых являются широковещательными
exit	Возвращает в режим EXEC
write	Сохраняет настройки

42.2.2 Отображение конфигурации защиты от DoS-атак

Выполните следующую команду в режиме EXEC, чтобы отобразить настроенные функции предотвращения DoS-атак:

Команда	Описание
show dos	Отображает конфигурацию защиты от DoS-атак

42.3 Примеры настройки предотвращения DoS-атак

В следующем примере показано, как настроить предотвращение атак TCP-пакетов с недопустимыми флагами, а затем отобразить конфигурация пользователя.

```
config
dos enable tcpflags
show dos
```

В следующем примере показано, как в глобальном режиме предотвратить атаки IP-пакетов, исходные IP-адреса которых являются IP-адресами назначения.

```
config
dos enable ip
```

43. IP-адресация

43.1 Введение

Интернет-протокол (IP) – это сетевой протокол для обмена данными в текстовой форме. IP имеет такие функции, как адресация, фрагментация, перегруппировка и мультиплексирование. На нем основана серия других протоколов (кластер протоколов IP). Как протокол, работающий на сетевом уровне, IP содержит информацию об адресации и управляющую информацию, которая используются для маршрутизации.

Протокол управления передачей (TCP) также основан на IP. TCP – это протокол, ориентированный на соединение, который регулирует формат данных и информации при передаче данных. TCP также предоставляет метод подтверждения успешной доставки данных. TCP позволяет нескольким приложениям в системе взаимодействовать одновременно, поскольку он может отправлять полученные данные каждому из приложений соответственно.

43.2 Настройка IP-адреса

Важным и обязательным требованием для настройки IP является настройка IP-адреса на сетевом интерфейсе маршрутизирующего коммутатора. Только в этом случае сетевой интерфейс может быть активирован, а IP-адрес может взаимодействовать с другими системами. При этом необходимо подтвердить маску IP-сети.

Для настройки IP-адресации необходимо выполнить указанные ниже задачи, среди которых первая является обязательной, а остальные – дополнительными.

Задачи настройки

- Настройка IP-адреса на сетевом интерфейсе
- Настройка нескольких IP-адресов на сетевом интерфейсе
- Настройка разрешения адресов
- Обнаружение и поддержание IP-адресации

43.2.1 Настройка IP-адреса на сетевом интерфейсе

IP-адрес определяет пункт назначения, куда отправляется IP-сообщение. Некоторые специальные IP-адреса зарезервированы и не могут использоваться в качестве IP-адреса хоста или сетевого адреса. В таблице 43-1 указан диапазон IP-адресов, зарезервированных и доступных IP-адресов.

Таблица 43-1 – Типы IP-адресов

Тип	Адрес или диапазон	Состояние
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Зарезервирован Доступен Зарезервирован
B	128.0.0.0 to 191.254.0.0 191.255.0.0	Доступен Зарезервирован
C	192.0.0.0 192.0.1.0 to 223.255.254.0 223.255.255.0	Зарезервирован Доступен Зарезервирован
D	224.0.0.0 – 239.255.255.255	Адрес для групповой коммуникации
E	240.0.0.0 – 255.255.255.254 255.255.255.255	Зарезервирован Широковещательный

Интерфейс имеет только один основной IP-адрес. Запустите следующую команду в режиме настройки интерфейса, чтобы настроить основной IP-адрес и маску подсети сетевого интерфейса:

Команда	Описание
ip address *ip-address mask*	Настраивает основной IP-адрес интерфейса

Маска – это часть IP-адреса, которая определяет сеть.

Коммутаторы данной серии поддерживают только маски, заданные последовательно, начиная с самого старшего байта, в соответствии с порядком характеристик сети.

43.2.2 Настройка нескольких IP-адресов на сетевом интерфейсе

Каждый интерфейс может иметь несколько IP-адресов, включая основной и несколько вторичных. Настраивать вторичные адреса имеет смысл в следующих случаях:

Если IP-адресов в сегменте сети недостаточно. Например, в определенной логической подсети всего 254 доступных IP-адреса, однако для подключения физической сети необходимо 300 хостов. В этом случае вы можете настроить вторичный IP-адрес на коммутаторе или сервере, разрешив двум логическим подсетям использовать одну и ту же физическую подсеть.

Большинство ранних сетей, основанных на мосте 2-го уровня, не разделены на подсети. Вы можете разделить такую сеть на несколько подсетей на основе маршрутов, правильно используя вторичные IP-адреса. Благодаря им маршрутизатор может распознавать несколько подсетей, которые соединяют одну и ту же физическую сеть.

Если две подсети в одной сети физически разделены другой сетью, в качестве вторичного IP-адреса можно взять адрес этой сети. Таким образом, две подсети в логической сети, которые физически разделены, будут логически связаны друг с другом.

Если вы настраиваете вторичный IP-адрес для коммутатора маршрутизации в сегменте сети, вам необходимо сделать это и для других маршрутизаторов в том же сегменте.

Запустите следующую команду в режиме настройки интерфейса, чтобы настроить несколько IP-адресов на порту:

Команда	Описание

ip address *ip-address mask* **secondary**	Настраивает несколько IP-адресов на сетевом интерфейсе

Когда протокол IP-маршрутизации используется для отправки информации об обновлении маршрута, вторичные IP-адреса могут обрабатываться по-разному.

43.2.3 Настройка разрешения адресов

IP может реализовывать такие функции, как управление разрешением IP-адресов. Далее подробно описано, как настроить разрешение адресов на коммутаторе.

- Создание разрешения адресов

IP-устройство может иметь два адреса: локальный адрес (сегмент локальной сети или устройство, однозначно идентифицируемое локальной сетью) и сетевой адрес (представляющий сеть, в которой расположено устройство). Локальный адрес – это адрес канального уровня. Он содержится в заголовке сообщения на канальном уровне, на котором считывается и используется устройствами. Его также называют MAC-адресом. Это связано с тем, что подуровень MAC на канальном уровне используется для обработки адресов.

Например, если вы хотите, чтобы ваш хост взаимодействовал с устройством через Ethernet, вы должны знать 48-битный MAC-адрес устройства или локальный адрес канального уровня. Процесс получения локального адреса канального уровня из IP-адреса называется протоколом разрешения адресов (ARP). Процесс получения IP-адреса из локального адреса канального уровня называется обратным разрешением адреса (RARP).

Наша система использует разрешение адресов двух типов: ARP и прокси-ARP. ARP и прокси-ARP определены в RFC 860 и 1027 соответственно.

ARP используется для сопоставления IP-адресов с носителем или MAC-адресом. Когда IP-адрес известен, ARP найдет соответствующий MAC-адрес. Если MAC-адрес известен, соотношение между IP-адресом и MAC-адресом сохраняется в кэше ARP для быстрого доступа. Затем IP-сообщение упаковывается в сообщение на канальном уровне и, наконец, отправляется в сеть.

- Определение статического кэша ARP

ARP и другие протоколы разрешения адресов обеспечивают динамическое сопоставление IP- и MAC-адреса. Статический элемент кэша ARP обычно не требуется, поскольку большинство хостов поддерживают динамическое разрешение адресов. При необходимости вы можете указать его в режиме настройки глобальных параметров. Система использует статический элемент кэша ARP для преобразования 32-битного IP-адреса в 48-битный MAC-адрес. Кроме того, вы можете указать коммутатору маршрутизации отвечать на запросы ARP от других хостов.

Вы можете установить активный период для записей ARP, если не хотите, чтобы такая запись существовала постоянно. Можно настроить два типа сопоставления между статическим IP-адресом и MAC-адресом.

Запустите одну из следующих команд в режиме глобальной конфигурации:

Команда	Описание
arp *ip-address hardware-address vlan*	Глобально сопоставляет IP-адрес с MAC-адресом в кэше ARP
arp *ip-address hardware-address vlan alias*	*alias* – опциональный параметр, который можно использовать в качестве альтернативного имени для данной записи ARP

Запустите следующие команды в режиме настройки интерфейса:

Команда	Описание
arp timeout *seconds*	Устанавливает время ожидания элемента кэша ARP в секундах. Это время определяет, сколько секунд система будет ожидать ответа от другого устройства при разрешении MAC-адреса по IP-адресу с использованием ARP, прежде чем считать, что разрешение не удалось
arp dynamic	Включает динамическое обучение ARP на интерфейсе

Запустите команду **show interfaces**, чтобы отобразить время ожидания ARP назначенного интерфейса. Запустите команду **show arp**, чтобы проверить содержимое кэша ARP. Запустите команду **clear arp-cache**, чтобы удалить все записи в кэше ARP.

- Настройка функции бесплатных сообщений ARP

Коммутатор может узнать, конфликтуют ли IP-адреса других устройств с его IP-адресом, отправив так называемое бесплатное сообщение ARP, в котором как исходный, так и целевой IP-адрес содержат локальный IP-адрес коммутатора, а MAC-адрес отправителя – его собственный MAC-адрес.

По умолчанию коммутатор обрабатывает бесплатные ARP-сообщения. Если он получает такое сообщение от устройства и обнаруживает, что IP-адрес в сообщении конфликтует с его собственным IP-адресом, он отправляет ARP-ответ устройству, информируя его о конфликте IP-адресов. Кроме того, коммутатор регистрирует информацию о конфликте в журнале событий.

Функция отправки бесплатных ARP-сообщений на коммутаторе по умолчанию отключена, но можно настроить её работу на порту коммутатора с помощью соответствующих команд:

Команда	Описание
arp send-gratuitous	Включает передачу бесплатных сообщений на интерфейсе

arp send-gratuitous interval *value*	Устанавливает интервал отправки бесплатного ARP-сообщения на интерфейс. Значение по умолчанию – 120 секунд.

➢ Установка максимального количества повторных передач пакетов Re-Detect

Чтобы обеспечить оперативность и правильность маршрутизации в подсети на уровне оборудования, необходимо периодически повторно обнаруживать записи ARP (с тегом G), от которых зависит шлюз маршрутизации. Чем больше количество передач пакетов Re-Detect, тем больше вероятность повторного обнаружения

Команда	Описание
arp max-gw-retries *number*	Устанавливает максимальное количество повторных передач пакетов Re-Detect. По умолчанию – 3

➢ Настройка повторной проверки при устаревании записи ARP

По умолчанию только записи ARP, от которых зависит шлюз маршрутизации, периодически проверяются на устаревание и обновление. Однако, после активации указанной команды, механизм периодической проверки на устаревание будет применяться ко всем записям ARP, независимо от их привязки к записям маршрутизации.

Команда	Описание
arp retry-allarp	Устанавливает повторное обнаружение, когда запись ARP устаревает

➢ Сопоставление имени хоста с IP-адресами

Любой IP-адрес может соответствовать имени хоста. В системе сохранен кэш сопоставления (имя хоста с адресом). Его можно использовать для выполнения операций, таких как telnet или ping, чтобы связать имя хоста с соответствующим IP-адресом и установить связь с хостом или проверить его доступность.

Чтобы назначить сопоставление имени хоста с адресом, выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip host *name address*	Статически сопоставляет имя хоста с IP-адресом

43.2.4 Обнаружение и поддержание IP-адресации

➢ Очистка кеша, списка и базы данных

Вы можете очистить весь контент в кэше, списке или базе данных. Если вы считаете, что какой-то контент неэффективен, вы можете удалить его.

Запустите следующую команду в режиме управления, чтобы очистить кэш, список и базу данных:

Команда	Описание
clear arp-cache	Очистка кэша IP ARP

➢ Отображение статистических данных о системе и сети

Система может отображать определенные статистические данные, такие как таблица IP-маршрутизации, кэш и база данных. Вся эта информация помогает узнать об использовании системных ресурсов и решить сетевые проблемы. Система также может отображать доступность порта и маршруты, по которым проходит сообщение в сети.

Соответствующие операции перечислены в следующей таблице. Выполните команды в режиме управления:

Команда	Описание
show arp	Отображает содержимое таблицы ARP
show hosts	Отображает таблицу сопоставления имен устройств с IP-адресами
show ip interface [*type number*]	Отображает состояние порта
ping {**host** | **address**}	Проверяет достижимость сетевого узла

43.3 Пример IP-адресации

В следующем примере показано, как настроить IP-адрес на интерфейсе VLAN11.

interface vlan 11

ip address 202.96.2.3 255.255.255.0

44. DHCP

44.1 Обзор

Протокол динамической настройки хоста (DHCP) используется для предоставления определенных параметров настройки сети для хостов в Интернете и подробно описан в стандарте RFC 2131. Одной из основных функций DHCP является распределение IP-адресов для интерфейсов. DHCP поддерживает следующие три механизма распределения IP-адресов:

- Автоматическое распределение

DHCP-сервер автоматически распределяет постоянный IP-адрес клиенту.

- Динамическое распределение

DHCP-сервер выделяет IP-адрес для использования клиентом в течение определенного периода времени или до тех пор, пока клиент не перестанет его использовать.

- Ручное распределение

Администратор DHCP-сервера вручную указывает IP-адрес и по протоколу DHCP отправляет его клиенту.

44.1.1 Применение DHCP

DHCP используется в следующих случаях:

- Настроив DHCP-клиент на Ethernet-интерфейсе, можно раздавать IP-адреса, указывать сетевые сегменты и связанные ресурсы (например, шлюз) для множества устройств, подключенных к этому интерфейсу.
- Когда коммутатор, который имеет доступ к DHCP-серверу, соединяется с несколькими устройствами, он сам может получить IP-адрес от DHCP-сервера и затем раздавать этот адрес устройствам через DHCP-ретрансляцию. Таким образом, коммутатор действует как посредник между DHCP-сервером и устройствами, которые нуждаются в IP-адресах.

44.1.2 Преимущества DHCP

В текущей версии программного обеспечения поддерживается клиент DHCP или клиент DHCP на интерфейсе Ethernet. DHCP имеет следующие сильные стороны:

- фиксация настроек;
- снижение количества ошибок конфигурации;
- управление IP-адресами некоторых портов устройств через DHCP-сервер.

44.1.3 Терминология DHCP

DHCP основан на режиме сервер/клиент. Таким образом, DHCP-сервер и DHCP-клиент должны существовать одновременно:

- DHCP-сервер

Это программа для распределения и обработки ресурсов, связанных с DHCP, таких как IP-адреса и время аренды.

- DHCP-клиент

Это программа для получения от DHCP-сервера информации, которая используется устройствами локальной системы, например, информации об IP-адресе.

- Срок аренды

В процессе динамического распределения DHCP существует понятие времени аренды. Под ним подразумевается срок действия IP-адреса, который начинается с момента его выдачи. По истечении срока аренды DHCP-сервер отзывает IP-адрес. Чтобы продолжать использовать этот IP-адрес, DHCP-клиенту необходимо запросить его еще раз.

44.2 Настройка DHCP-клиента

Задачи настройки

- Получение IP-адреса
- Указание адреса DHCP-сервера
- Настройка параметров DHCP
- Мониторинг DHCP

44.2.1 Получение IP-адреса

Выполните следующую команду на интерфейсе VLAN, чтобы получить IP-адрес интерфейса через протокол DHCP:

Команда	Описание
ip address dhcp	Устанавливает IP-адрес интерфейса Ethernet через DHCP

44.2.2 Указание адреса DHCP-сервера

Зная адреса некоторых DHCP-серверов, вы можете указать эти адреса на коммутаторе, чтобы сократить время обработки протокола. Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
ip dhcp-server *ip-address*	Указывает IP-адрес DHCP-сервера

Команда опциональна при выполнении операций по получению IP-адреса.

44.2.3 Настройка параметров DHCP

Чтобы настроить параметры связи DHCP в соответствии с фактическими требованиями, выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание

ip dhcp client minlease *seconds*	Указывает приемлемое минимальное время аренды
ip dhcp client retransmit *count*	Указывает время повторной передачи пакета DHCP
ip dhcp client select *seconds*	Указывает интервал для SELECT
ip dhcp client class_identifier *WORD*	Указывает классификационный код поставщика
ip dhcp client client_identifier hrd_ether	Указывает идентификатор клиента как тип Ethernet
ip dhcp client timeout_shut	Указывает время ожидания клиента для отключения интерфейса

Команды опциональны при выполнении операций по получению IP-адреса.

44.2.4 Мониторинг DHCP

Чтобы просмотреть соответствующую информацию о DHCP-сервере, который в данный момент обнаружен коммутатором, выполните следующую команду в режиме EXEC:

Команда	Описание
show dhcp server	Отображает информацию о DHCP-сервере, известном коммутатору

Чтобы просмотреть, какой IP-адрес в данный момент используется коммутатором, выполните следующую команду в режиме EXEC:

Команда	Описание
show dhcp lease	Отображает IP-ресурсы, которые в данный момент используются коммутатором, и связанную с ними информацию

Кроме того, если DHCP используется для распределения IP-адресов интерфейсам Ethernet, вы можете запустить команду **show interface**, чтобы проверить, успешно ли получен IP-адрес, требуемый интерфейсом.

44.2.5 Пример настройки DHCP-клиента

В следующем примере показано, что интерфейс vlan11 получает IP-адрес при помощи DHCP:

```
interface vlan 11
```

ip address dhcp

45. Дополнительные службы IP

45.1 Настройка IP-сервиса

Описанные ниже настройки не являются обязательными. Вы можете выполнять их в соответствии с вашими требованиями.

Задачи настройки

- Управление IP-соединением
- Настройка параметров производительности
- Проверка и поддержка IP-сети

45.1.1 Управление IP-соединением

Протокол IP предоставляет ряд служб для контроля и управления IP-соединениями. Большинство этих услуг предоставляется при помощи ICMP. ICMP (Internet Control Message Protocol) – это протокол в сетях TCP/IP, который используется для передачи сообщений об ошибках, управления и диагностики сети. ICMP позволяет сетевым устройствам отправлять сообщения о проблемах, таких как недоступность хоста или сетевые ошибки, и получать ответы на эти сообщения. Он также используется для выполнения утилит, таких как «ping», которые позволяют проверять доступность удаленных хостов в сети. ICMP в основном определен в стандарте RFC 792.

Сообщение ICMP отправляется на хост или другие коммутаторы, когда коммутатор маршрутизации или сервер доступа обнаруживает ошибки в заголовке IP-сообщения.

Выполните следующие операции в соответствии с различными условиями IP-соединения:

➢ Отправка ICMP-сообщения о недоступности

Если система получает сообщение и не может переслать его по назначению (например, из-за отсутствия маршрутов), система отправит ICMP-сообщение о недоступности на исходный хост. По умолчанию эта функция включена.

Если функция отключена, для ее включения выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
ip unreachables	Включает функцию отправки ICMP-сообщения о недостижимости пункта назначения

➢ Отправка ICMP-сообщения о перенаправлении

Иногда хост выбирает неоптимальный маршрут. После того, как маршрутизатор получает сообщение от хоста, он должен проверить таблицу маршрутизации, а затем переслать сообщение через интерфейс приема сообщений на другой маршрутизатор, который находится в том же сегменте сети, что и хост. В этом случае маршрутизатор не обрабатывает сообщение сам, а уведомляет хост-источник о том, что он должен напрямую отправить сообщение другому маршрутизатору. Это сообщение перенаправления указывает исходному хосту отказаться от первоначального пути и выбрать более прямой маршрут, предложенный в сообщении. Многие операционные системы хостов автоматически добавляют маршрут в свою таблицу маршрутизации, но маршрутизатор склонен больше доверять информации, полученной через протокол маршрутизации, и не добавляет маршрут хоста на основе этой информации.

Эта функция включена по умолчанию. Если на интерфейсе настроен протокол горячей резервной маршрутизации (HSRP – Hot Standby Routing Protocol), то эта функция автоматически отключается. Однако, даже если протокол горячей резервной маршрутизации отменен, функция не будет автоматически включена.

Чтобы включить эту функцию, выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
ip redirects	Разрешает отправку ICMP-сообщения о перенаправлении

- Отправка ICMP-сообщения с информацией о сетевой маске.

Когда хосту нужно узнать маску подсети, он отправляет ICMP-запрос об этой информации. Если маршрутизатор может подтвердить маску для хоста, он отвечает соответствующим ICMP-сообщением. По умолчанию, маршрутизатор может отправлять ICMP-ответ с маской подсети. Чтобы отправить ICMP-запрос о маске подсети, необходимо выполнить следующую команду в режиме настройки интерфейса:

Команда	Описание
ip mask-reply	Отправляет ICMP-запрос о маске подсети

- Поддержка определения MTU маршрута

Система поддерживает механизм определения MTU IP-маршрута, определенный в стандарте RFC 1191. Механизм позволяет хосту динамически находить и настраиваться на максимальную единицу передачи для разных маршрутов. Иногда маршрутизатор обнаруживает, что длина полученного IP-сообщения больше, чем MTU, установленный на интерфейсе для пересылки сообщения. В этом случае IP-сообщение должно быть сегментировано, но это невозможно из-за флага «unsegmented» и, следовательно, сообщение отбрасывается. В этом случае маршрутизатор отправляет ICMP-сообщение, чтобы уведомить исходный хост о причине неудачной пересылки и о значении MTU на интерфейсе пересылки. Исходный хост затем уменьшает длину сообщения, отправляемого к месту назначения, чтобы соответствовать минимальному MTU маршрута. Если какое-

либо соединение на маршруте разорвано, сообщение должно идти по другим маршрутам. Минимальный MTU на этих маршрутах может отличаться от исходного маршрута. Маршрутизатор уведомляет исходный хост о MTU нового маршрута. IP-сообщение должно быть упаковано с минимальным MTU маршрута насколько это возможно. Это позволяет избежать сегментации и улучшить эффективность обмена сообщениями. Соответствующие хосты должны поддерживать определение MTU для маршрута IP и могут настраивать длину IP-сообщения в соответствии с значением MTU, сообщенным маршрутизатором, чтобы избежать сегментации в процессе пересылки.

- Настройка MTU IP-передачи

Все интерфейсы имеют MTU по умолчанию, то есть максимальную длину передаваемого IP-сообщения. Если длина IP-сообщения превышает MTU, маршрутизирующий коммутатор сегментирует сообщение.

Изменение значения MTU интерфейса влияет на значение IP-MTU. Если IP-MTU равен MTU, то IP-MTU автоматически изменяется, чтобы быть таким же, как новое значение MTU при его изменении. Однако изменение IP-MTU не влияет на MTU. IP-MTU не может быть больше, чем MTU, настроенный на текущем интерфейсе. Нормальная коммуникация может быть установлена только в том случае, если все устройства, подключенные к одной и той же физической среде, имеют одинаковый протокол MTU.

Чтобы установить IP-MTU на специальном интерфейсе, выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
ip mtu *bytes*	Устанавливает IP-MTU на интерфейсе

- Авторизация IP-маршрута отправителя

IP позволяет отправителю указать для сообщения маршрут в сети IP. Указанный маршрут называется исходным маршрутом, и его можно указать, выбрав опцию исходного маршрута в заголовке IP. Маршрутизирующий коммутатор должен пересылать IP-сообщение в соответствии с этой опцией или отбрасывать сообщение согласно требованиям безопасности. По умолчанию коммутатор поддерживает опцию исходного маршрута. В каждом сообщении он проверяет опции заголовка IP, определенные в RFC 791: строгий и гибкий исходный маршрут, запись маршрута и временную метку. Если коммутатор обнаруживает, что опция выбрана неверно, он отправляет отправителю уведомление ICMP о проблеме параметра и отбрасывает сообщение. Если возникают проблемы с исходным маршрутом, маршрутизирующий коммутатор отправит отправителю ICMP-сообщение о недоступности (сбой исходного маршрута).

Если исходный IP-маршрут отключен, для его авторизации выполните следующую команду в режиме настройки глобальных параметров:

Команда	Описание
ip source-route	Авторизация исходного IP-маршрута

45.1.2 Настройка параметров производительности

➢ Установка времени ожидания TCP-соединения

Когда маршрутизирующий коммутатор устанавливает TCP-соединение, он считает его неудачным, если соединение не устанавливается в течение определенного времени ожидания, после чего уведомляет об этом верхний уровень программы. Вы можете настроить время ожидания для установки TCP-соединения. Значение по умолчанию в системе составляет 75 секунд. Эта настройка не влияет на TCP-соединения, которые коммутатор пересылает т.е., передает другим устройствам. Она влияет только на соединения, которые коммутатор создает самостоятельно.

Запустите следующую команду в режиме глобальной конфигурации, чтобы установить время ожидания для TCP-соединений:

Команда	Описание
ip tcp synwait-time *seconds*	Устанавливает время ожидания TCP-соединения

➢ Настройка размера окон TCP

Размер окон TCP по умолчанию составляет 2000 байт. Запустите следующую команду в режиме глобальной конфигурации, чтобы изменить размер окна по умолчанию:

Команда	Описание
ip tcp window-size *bytes*	Указывает размер окон TCP

45.1.3 Проверка и поддержка IP-сети

Вы можете очистить весь контент в кэше, списке или базе данных, выполнив следующую команду:

Команда	Описание
clear tcp statistics	Удаляет статистику TCP

Чтобы отключить TCP-соединение, выполните следующую команду:

Команда	Описание
clear tcp {**local** *host-name port* **remote** *host-name port* | **tcb** *address*}	Очищает указанное TCP-соединение. **tcb** означает блок управления TCP

Система может отображать содержимое кэша, списка и базы данных. Эти статистические данные помогают узнать об использовании системных ресурсов и решить сетевые проблемы.

Выполните следующие команды в режиме EXEC:

Команда	Описание
show ip access-lists *name*	Отображает содержимое одного или всех списков доступа
show ip sockets	Отображает всю информацию о сокетах коммутатора маршрутизации
show ip traffic	Отображает статистические данные IP-протокола
show tcp	Отображает подробную информацию о состоянии TCP-соединений
show tcp brief	Отображает краткую информацию о состоянии TCP-соединений
show tcp statistics	Отображает статистические данные TCP
show tcp tcb	Отображает подробности о текущих активных TCP-соединениях

При возникновении проблемы в сети можно отобразить отладочную информацию.

Выполните следующие команды в режиме EXEC:

Команда	Описание
debug arp	Отображает интерактивную информацию ARP
debug ip icmp	Отображает интерактивную информацию ICMP
debug ip raw	Отображает информацию о низкоуровневых операциях, связанных с IP-пакетами, такими как их прием, обработка и отправка
debug ip packet	Отображает интерактивную информацию IP
debug ip tcp	Отображает интерактивную информацию TCP
debug ip udp	Отображает интерактивную информацию UDP

45.2 Настройка списка управления доступом

45.2.1 Фильтрация IP-пакетов

Фильтрация сообщений помогает контролировать движение сетевых пакетов в сети. Этот контроль может ограничивать передачу данных по сети и использование сети определенными пользователями или устройствами. Для определения, допустимы ли или недопустимы сетевые пакеты для прохождения через определенный интерфейс, данный маршрутизирующий коммутатор предоставляет функцию списка контроля доступа (ACL). Список доступа можно использовать в следующих режимах:

- контроль передачи пакетов через интерфейс;
- контроль доступа к виртуальным терминалам;
- ограничение содержания обновления маршрута.

Этот раздел описывает, как создавать списки IP-доступа и как их использовать для управления потоком данных в сети.

Список IP-доступа – это упорядоченный набор условий для разрешения или запрета применения IP-адресов. Программное обеспечение ROS данного коммутатора проверяет адреса по одному в соответствии с правилами, заданными в списке доступа. Первое совпадение определяет, принимается ли адрес или отклоняется. После первого совпадения программное обеспечение ROS завершает проверку по заданным правилам. Порядок условий имеет важное значение. Если ни одно правило не совпадает, адрес отклоняется. Для использования списка доступа необходимо вначале его создать, указав его имя и условия, а затем применить к выбранному интерфейсу.

45.2.2 Создание стандартного и расширенного списка IP-доступа

Используйте строку символов для создания списка доступа IP.

Стандартный и расширенный список доступа не могут иметь одинаковые имена.

Запустите следующую команду в режиме глобальной конфигурации, чтобы создать стандартный список доступа:

Команда	Описание
ip access-list standard *name*	Создает стандартный список доступа *name* означает имя списка
deny {*source* [*source-mask*] | **any**} [**log** | **location**] or **permit** {*source* [*source-mask*] | **any**} [**log** | **location**]	Указывает одно или несколько условий разрешения/запрета в режиме настройки стандартного списка доступа. Параметр **permit** или **deny** определяет, будет ли пакет одобрен или отклонен
Exit	Выход из режима настройки списка доступа

Запустите следующую команду в режиме глобальной конфигурации, чтобы создать расширенный список доступа:

Команда	Описание
ip access-list extended *name*	Создает расширенный список доступа *name* означает имя списка
{**deny** | **permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** time-range] [**location** location]	Обозначает одно или несколько условий разрешения/запрета в режиме настройки расширенного списка доступа. Параметр **permit** или **deny** определяет, будет ли

[**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq** | **gt** | **lt** *length*] [**ttl eq** |**gt** | **lt** *time*] [**offset-not-zero**] [**offset-zero**] {**deny** | **permit**} *protocol* **any any** [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq** |**gt** | **lt** *length*] [**ttl eq** | **gt** | **lt** *time*] [**offset-not-zero**] [**offset-zero**]	пакет одобрен или отклонен. **precedence** означает приоритет IP-пакета. **tos** означает тип услуги. Если список настраивается для физического порта и используется протокол TCP или UDP, то нужно выбрать от 1 до 14 портов из определенного диапазона (см. раздел «Примеры применения расширенного списка доступа»).
Exit	Выход из режима настройки списка доступа

После первоначального создания списка доступа любую часть, добавленную позже, можно поместить в конец списка. То есть вы не можете добавить команду в существующий список доступа. Однако можно использовать команды **no permit** и **no deny** для удаления элементов из списка.

При создании списка доступа в конце его автоматически добавляется неявное правило «запретить все». Если при создании списка доступа не указана маска для IP-адреса хоста, то используется маска 255.255.255.255 по умолчанию.

После создания списка доступа, его необходимо применить к маршруту или интерфейсу, чтобы он начал работать и влиять на трафик в сети.

45.2.3 Применение списка доступа

После создания списка доступа можно применить его к одному или нескольким интерфейсам.

Запустите следующую команду в режиме настройки интерфейса:

Команда	Описание
ip access-group *name* {**in** | **out**}	Применяет список доступа к интерфейсу

Список контроля IP-доступа можно использовать на входном или выходном интерфейсе. После получения пакета адрес его источника будет проверен в соответствии со стандартным списком контроля доступа, примененным к интерфейсу. Для расширенного списка контроля доступа маршрутизирующий коммутатор также проверяет адрес назначения. Если список разрешает адрес назначения, система продолжит обработку

пакета, если запрещает – система отбросит пакет, а затем вернет ICMP-сообщение о недоступности.

Если назначенный список управления доступом не существует, прохождение всех пакетов разрешено.

Созданный список контроля доступа может быть применен как к отдельным портам, так и глобально.

Для применения ACL на интерфейсе запустите следующие команды в режиме управления:

Команда	Описание
config	Вход в режим глобальной конфигурации
interface g0/1	Вход в режим настройки интерфейса
[**no**] {**ip** | **ipv6**} **access-group** *name*	Применяет или отменяет список IP-доступа на интерфейсе. *name*: имя списка IP-доступа
exit	Возвращает в режим глобальной конфигурации
exit	Возвращает в режим EXEC
write	Сохраняет настройки

Для глобального применения ACL запустите следующие команды в режиме управления:

Команда	Описание
config	Вход в режим глобальной конфигурации
[**no**] {**ip** | **ipv6**} **access-group egress** [**vlan** {**add** *word* | **remove** *word*}]	Применяет или отменяет созданный список IP-доступа в глобальном режиме. **egress** означает, что ACL применяется для выходных интерфейсов. **vlan** означает, что ACL применяется к входящему трафику на уровне определенной VLAN. *word* означает таблицу диапазонов VLAN. **add** означает добавление таблицы диапазонов VLAN. **remove** означает удаление таблицы диапазонов VLAN
exit	Возвращает в режим EXEC
write	Сохраняет настройки

Список IP-доступа можно применить к VLAN в глобальном режиме, но не в режиме настройки интерфейса.

45.2.4 Примеры применения расширенного списка доступа

- Применение к логическому интерфейсу

В следующем примере первая строка позволяет любому новому TCP подключаться к порту назначения при условии, что номер порта источника (порт отправителя) больше 1023. Вторая строка позволяет любому новому TCP подключаться к SMTP-порту хоста.

```
ip access-list extended aaa
permit tcp any 130.2.0.0 255.255.0.0 gt 1023
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```

Ниже приведен еще один пример применения расширенного списка доступа. Предположим, что сеть подключена к Интернету, и вы ожидаете, что любой хост в локальной сети Ethernet может создать TCP-соединение с хостом в Интернете. Однако хосты из Интернета не должны создавать TCP-соединений с хостами в Ethernet, если только это не подключение к порту SMTP почтового сервера.

SMTP подключается к TCP-порту на одном конце и к произвольному номеру порта на другом конце. В период соединения используются одни и те же два номера портов. Почтовый пакет из Интернета имеет порт назначения, то есть порт 25. Исходящий пакет имеет номер противоположного порта. Фактически, система безопасности, стоящая за коммутатором маршрутизации, всегда получает почту с порта 25. Именно по этой причине входящие и исходящие сервисы могут контролироваться однозначно. Список доступа может быть настроен как для исходящего, так и для входящего сервиса.

В данном случае Ethernet представляет собой сеть B-типа с адресом 130.20.0.0. Адрес почтового хоста – 130.20.1.2. Для протокола TCP используется ключевое слово «established», что означает, что соединение уже создано. Список контроля доступа будет содержать два правила: первое правило разрешает TCP от любых источников в сети Ethernet только в том случае, если соединение уже установлено (это определяется наличием флага ACK или RST в пакетах). Второе правило разрешает только TCP-соединения от любых источников к конкретному хосту с адресом 130.20.1.2, если они направлены на порт 25 (порт SMTP).

```
ip access-list aaa
permit tcp any 130.20.0.0 255.255.0.0 established
permit tcp any 130.20.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```

- Применение к физическому интерфейсу с поддержкой TCP/UDP

Формат настройки следующий:

{**deny | permit**} {tcp | udp}

source source-mask [{[src_portrange begin-port end-port] | [{gt | lt } port]}]

destination destination-mask [{[dst_portrange begin-port end-port] | [{gt | lt } port]}]

[**precedence** *precedence*] [**tos** *tos*]

Настраивая список доступа с использованием диапазона портов необходимо учитывать требования этого метода к ресурсам системы:

- Если вы настраиваете ACL, указывая диапазон портов как на стороне отправителя, так и на стороне получателя, это может потребовать больших ресурсов и привести к неудачной конфигурации. В таком случае рекомендуется указать диапазон портов на одной стороне и конкретный порт на другой стороне.
- Фильтрация по диапазону портов может потребовать значительных ресурсов, и, если ее использовать слишком часто, это может привести к ухудшению производительности других программ, которые используют ACL.

В следующем примере первая строка позволяет любому новому TCP подключиться к порту SMTP хоста 130.2.1.2:

```
ip access-list extended aaa
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface g0/1
ip access-group aaa
```

46. Протоколы маршрутизации

46.1 Введение

46.1.1 Протокол IP-маршрутизации

Коммутаторы данной серии реализуют несколько протоколов динамической маршрутизации IP. Их описание представлено в этой главе.

Протоколы IP-маршрутизации подразделяются на две категории: протокол внутреннего шлюза (IGP) и протокол внешнего шлюза (EGP). Коммутаторы нашей компании поддерживают RIP, OSPF, BGP и BEIGRP. Каждый протокол можно настроить отдельно в зависимости от реальных потребностей. Поддерживается одновременная настройка нескольких протоколов маршрутизации, включая неограниченное количество процессов OSPF (если достаточно памяти), процесс BGP, процесс RIP и неограниченное количество процессов BEIGRP. Команду **redistribute** (перераспределить) можно использовать для добавления других протоколов маршрутизатора в базу данных текущего протокола, чтобы их можно было связать.

Чтобы настроить протокол динамической маршрутизации IP, необходимо запустить соответствующий процесс и связать соответствующие сетевые интерфейсы и конкретный процесс динамической маршрутизации, указав, на каких интерфейсах выполняется процесс. Термин «маршрутизатор» в данной главе относится к коммутатору, выполняющему функции маршрутизации.

46.1.2 Выбор протокола маршрутизации

Выбор протокола маршрутизации – сложный процесс. При выборе необходимо учитывать следующие факторы:

- размер и сложность сети;
- нужна ли поддержка VLSM;
- сетевой трафик;
- требование безопасности;
- требования к надежности;
- политика.

Выбранный протокол маршрутизации должен соответствовать реальному состоянию сети и удовлетворять вашим требованиям.

46.1.2.1 Протокол маршрутизации внутреннего шлюза

Протокол маршрутизации внутреннего шлюза используется для сети в одной автономной системе (AS). Весь протокол маршрутизации внутреннего шлюза IP при запуске должен быть связан с некоторыми конкретными сетями (указывается в настройках **network**). Каждый процесс маршрутизации прослушивает сообщения обновлений от других маршрутизаторов в сети и одновременно передает в сеть свою собственную информацию о маршрутизации. Протоколы маршрутизатора внутреннего шлюза, поддерживаемые коммутаторами данной серии, включает в себя:

- RIP
- OSPF
- BEIGRP

46.1.2.2 Протокол маршрутизации внешнего шлюза

Протокол маршрутизации внешнего шлюза используется для обмена информацией о маршрутизации между различными автономными системами. Обычно требуется настроить соответствующих соседей для обмена маршрутами, доступные сети и номер локальной автономной системы. Протокол маршрутизации внешнего шлюза, поддерживаемый коммутаторами данной серии, – BGP.

46.2 VRF

46.2.1 Обзор

VRF (Virtual Routing and Forwarding) расшифровывается как виртуальная маршрутизация и пересылка. Это технология, позволяющая создавать несколько виртуальных маршрутизационных таблиц внутри одного маршрутизатора. Каждая из этих таблиц функционирует независимо, что позволяет разделять сетевой трафик между разными сегментами сети, предотвращая их взаимное воздействие. Это особенно полезно в многотеневых сетях и виртуализированных средах, где требуется изоляция трафика между различными сетевыми сегментами.

Одной из ключевых целей VPN является обеспечение безопасности и изоляции данных, а также предотвращение связи между станциями, которые не принадлежат к одной и той же VPN. Для того чтобы отличать, какой пользователь VPN отправляет маршруты через какой локальный интерфейс на устройстве PE (Provider Edge), на этом устройстве создаются виртуальные маршруты. Каждый виртуальный маршрут имеет свою собственную таблицу маршрутизации и таблицу пересылки. Вместе они составляют так называемый виртуальный маршрутизирующий и переадресующий экземпляр – VRF. Он включает в себя связанные таблицу маршрутизации, интерфейс, экземпляры маршрутизации и политику маршрутизации, относящиеся к одной и той же станции. На устройстве PE физический или логический порт одной VPN соответствует одному VRF.

46.2.2 Настройка VFR

Задачи настройки

- Создание таблицы VRF
- Связь интерфейса с VRF
- Настройка атрибута расширения целевой VPN для VRF
- Настройка описания VRF
- Настройка статического маршрута VRF
- Мониторинг VRF
- Поддержка VRF
- Пример настройки VRF

46.2.2.1 Создание таблицы VRF

Чтобы создать таблицу маршрутизации и пересылки VPN, выполните следующие действия в режиме глобальной конфигурации:

Команда	Описание
PE_config# **ip vrf** ce	Вход в режим настройки VRF, определение таблицы VRF
PE_config_vrf_ce# **rd** *ASN:nn or IP-address:nn*	Назначает тег маршрутизации VRF, создает таблицу маршрутизации и пересылки VRF
PE_config_vrf_ce# **route-target** [**export** | **import** | **both**] ASN:nn or IP-address:nn	Создает входной атрибут VRF и выходной целевой атрибут расширения VPN

46.2.2.2 Связь интерфейса с VRF

Для связи интерфейса с VRF, выполните следующие команды:

Команда	Описание
PE_config# **interface vlan** 1	Вход в режим настройки интерфейса
PE_config_v1# **ip vrf forwarding** *vrf-name*	Связывает интерфейс с VRF
PE_config_v1# **ip address** *ip-address subnet-mask*	Настраивает IP-адрес интерфейса

46.2.2.3 Настройка атрибута расширения целевой VPN для VRF

Для настройки атрибута расширения целевой VPN выполните следующие действия:

Команда	Описание
PE_config# **ip vrf** ce	Вход в режим настройки VRF
PE_config_vrf_ce# **rd** *ASN:nn or IP-address:nn*	Настраивает тег маршрутизации VRF и создает таблицу VRF
PE_config_vrf_ce# **route-target** [**export** | **import** | **both**] *ASN:nn or IP-address:nn*	Настраивает входной атрибут VRF и выходной целевой атрибут расширения
PE_config_vrf_ce# **import map** *WORD*	Настраивает фильтр карты маршрутов для добавления маршрутов в таблицу маршрутизации VRF
PE_config_vrf_ce# **export map** *WORD*	Добавление атрибута расширения целевой VPN, соответствующего условиям карты маршрутов, к выходному атрибуту расширения целевой VPN для VRF

Прежде чем передать информацию о локальном маршруте другому PE-устройству, входной PE добавит атрибут цели маршрута к каждому маршруту, полученному от непосредственно подключенной станции. Значение этого атрибута основывается на значении VRF, настроенном в атрибуте расширения цели вывода.

Перед установкой удаленного маршрута, опубликованного другим PE на локальном VRF, каждый VRF на входном PE-устройстве будет настроен с одним входным целевым

атрибутом расширения. Устройство PE может использоваться для маршрутизации на определенном VRF, только если идентификатор маршрута, используемый VPN-IPv4 (т.е. маршрутизационный целевой атрибут), совпадает с идентификатором маршрута, который ожидается в этом VRF (т.е. целевым вводом VRF). Если они не совпадают, устройство PE не сможет правильно маршрутизировать данные.

46.2.2.4 Настройка описания VRF

Чтобы настроить описание VRF, выполните следующие команды:

Команда	Описание
PE_config# **ip vrf** ce	Вход в режим настройки VRF
PE_config_vrf_ce# **rd** *ASN:nn or IP-address:nn*	Настраивает тег маршрутизации VRF и создает таблицу VRF
PE_config_vrf_ce# **description** *LINE*	Настраивает описание VRF

46.2.2.5 Настройка статического маршрута VRF

Чтобы настроить статический маршрут VRF, выполните следующие команды:

Команда	Описание
PE_config# **ip vrf** ce	Вход в режим настройки VRF
PE_config_vrf_ce# **rd** *ASN:nn or IP-address:nn*	Настраивает тег маршрутизации VRF и создает таблицу VRF
PE_config_vrf_ce# **exit**	Выход из режима настройки VRF
PE_config# **ip route** [**vrf** *vrf-name*] dest mask {type num | nexthop} [distance]	Настраивает статический маршрут VRF

46.2.2.6 Мониторинг VRF

Для отображения статистики VRF выполните следующие команды:

Команда	Описание
PE# **show ip vrf**	Показывает VRF и связанную с ним информацию об интерфейсе
PE# **show ip vrf** [{**brief** | **detail** | **interfaces**}] *vrf-name*	Показывает конфигурацию VRF и связанную с ней информацию об интерфейсе
PE# **show ip route vrf** *vrf-name* [A.B.C.D | **all** | **beigrp** | **bgp** | **ospf** | **rip** | **connect** | **static** | **summary**]	Показывает информацию о маршрутизации в таблице VRF

46.2.2.7 Поддержка VRF

Для поддержки VRF необходимо отслеживать основную таблицу маршрутизации, а также изменение таблицы маршрутизации и информации о конфигурации VRF. Выполните следующие команды в режиме управления:

Команда	Описание
PE# **debug ip routing**	Отслеживает добавление, удаление и изменение маршрута в основной таблице маршрутизации
PE# **debug ip routing message**	Отслеживает полученную и отправленную информацию VRF
PE# **debug ip routing vrf** *vrf-name*	Отслеживает изменение указанной таблицы маршрутизации VRF, включая добавление, удаление и изменение

46.2.3 Пример настройки VRF

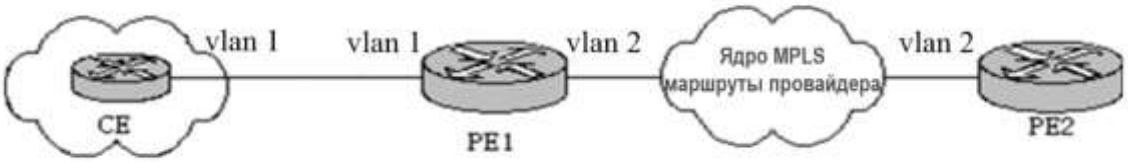

Рисунок 46-1 – Топология сети

Настройка устройств маршрутизации следующая:

Устройство CE:

```
interface loopback 0
  ip address 22.1.1.1 255.255.255.0
!
interface vlan 1
ip address 170.168.20.152 255.255.255.0
!
router ospf 1
  network 170.168.20.0 255.255.255.0 area 0
  network 22.1.1.0 255.255.255.0 area 0
!
```

Устройство PE1:

```
ip vrf pe1
rd 1:1
route-target 1:1
!
interface vlan 1
ip vrf forwarding pe1
ip address 170.168.20.153 255.255.255.0
!
interface vlan 2
 ip address 176.168.20.152 255.255.255.0
!
router ospf 1 vrf pe1
 network 170.168.20.0 255.255.255.0 area 0
!
router bgp 1
neighbor 176.168.20.154 remote-as 2

address-family vpnv4
    neighbor 176.168.20.154 activate
    exit-address-family

    address-family ipv4 vrf pe1
    no synchronization
    redistribute ospf 1
    exit-address-family
```

Устройство PE2:

```
ip vrf pe2
rd 1:1
route-target 1:1
!
interface loopback 0
 ip vrf forwarding pe2
 ip address 44.1.1.1 255.255.255.0
!
interface vlan 2
 ip address 176.168.20.154 255.255.255.0
!
router bgp 2
neighbor 176.168.20.153 remote-as 1

address-family vpnv4
```

```
neighbor 176.168.20.153 activate
exit-address-family

address-family ipv4 vrf pe2
no synchronization
redistribute connected
exit-address-family
```

46.3 Статическая маршрутизация

46.3.1 Обзор

Статическая маршрутизация – это специальная конфигурация маршрутизации, настраиваемая администратором. В сети такая структура относительно проста, вам нужно только настроить статические маршруты для обеспечения совместимости сетей. Правильная настройка и использование статических маршрутов может улучшить производительность сети и гарантировать пропускную способность для важных сетевых приложений.

Недостатки статического маршрута: он не может автоматически адаптироваться к изменениям топологии сети. При сетевых неполадках или изменении топологии маршрут может стать недоступным, что приведет к сбоям в работе сети. Поэтому администратор должен будет вручную изменить конфигурацию статических маршрутов.

Маршрут по умолчанию используется, когда маршрутизатор не может найти соответствующую запись в таблице маршрутизации:

если адрес назначения пакета не совпадает ни с одной записью в таблице маршрутизации, пакет выберет маршрутизацию по умолчанию;

если и маршрут по умолчанию, и пункт назначения пакета отсутствуют в таблице маршрутизации, пакет будет отброшен.

Маршрут по умолчанию может быть настроен со статическими маршрутами и отображаться в таблице маршрутов в виде сети 0.0.0.0/0.

46.3.2 Настройка статической маршрутизации

Задачи настройки

- Настройка соответствующих физических параметров интерфейса
- Настройка атрибутов канального уровня соответствующего интерфейса
- Настройка IP-адреса соответствующего интерфейса

Чтобы активировать статическую маршрутизацию, необходимо выполнить следующие шаги в режиме глобальной конфигурации:

Команда	Описание
ip route *A.B.C.D mask* {next-hop | interface} [distance] [tag *tag*] [global] [description]	Настройка статической маршрутизации

46.3.3 Пример настройки статической маршрутизации

Чтобы назначить сегменту сети 10.0.0.0/8 порт интерфейса vlan 1, команда настройки выглядит следующим образом:

ip route 10.0.0.0 255.0.0.0 vlan 1

46.4 RIP

46.4.1 Обзор

Протокол RIP (Route Information Protocol) – это относительно старый, но все еще широко используемый протокол внутреннего шлюза (IGP), который в основном применяется в небольших однотипных сетях. RIP – это традиционный протокол векторной маршрутизации, описанный в RFC 1058.

RIP обменивается информацией о маршрутизации посредством широковещательной передачи пакетов UDP. Маршрутизатор отправляет обновленную информацию каждые 30 секунд. Если в течение 180 секунд не было получено никакой обновленной информации от соседнего маршрутизатора, его маршруты будут помечены в таблице маршрутизации как неиспользуемые. И если в течение следующих 120 секунд обновленная информация по-прежнему не поступит, эти маршруты будут удалены из таблицы маршрутизации.

Число переходов (хопов) RIP использует в качестве показателя для измерения различных маршрутов. Подсчет переходов относится к количеству пройденных пакетами маршрутизаторов на пути от источника к пункту назначения. Метрика маршрута, который напрямую подключен к сети, равна «0», метрика маршрута, сеть которого недостижима, равна «16». Поскольку метрика маршрута, используемая RIP, находится в относительно небольшом диапазоне, она неприменима к крупномасштабной сети.

Если маршрутизатор имеет маршрут по умолчанию, RIP объявит маршрут к ложной сети 0.0.0.0. На самом деле сети 0.0.0.0 не существует, она используется только для реализации функции маршрута по умолчанию в RIP. Если RIP изучил маршрут по умолчанию или у маршрутизатора настроен шлюз по умолчанию со стандартными настройками, маршрутизатор объявит сеть по умолчанию.

RIP отправит обновления на интерфейс назначенной сети. Если сеть самого интерфейса не назначена, то сеть потом не будет анонсирована ни в одном обновлении RIP.

RIP-2 в устройствах данной серии поддерживает аутентификацию Plaintext и MD5, Route Summary, CIDR и VLSM.

46.4.2 Настройка RIP

Задачи настройки

- Запуск RIP
- Включение одноадресной рассылки сообщений об обновлении маршрута RIP
- Применение смещения к метрике маршрута
- Настройка таймеров
- Назначение номера версии RIP
- Активация аутентификации RIP
- Активация «пассивного» и «глухого» статуса интерфейса
- Запрет суммирования маршрутов
- Запрет аутентификации исходного IP-адреса
- Активация или запрет режима расщепления горизонта

46.4.2.1 Запуск RIP

Чтобы активировать RIP, выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
router rip *process-id* [**vrf** *vrf-name*]	Активация процесса маршрутизации RIP и вход в режим настройки маршрутизатора

46.4.2.2 Генерация интерфейса экземпляра RIP

После включения экземпляра RIP только интерфейсы, связанные с этим экземпляром, могут создавать сегменты сети RIP и использоваться для обмена информацией о маршрутизации. Экземпляры должны быть связаны с интерфейсами. В режиме настройки интерфейса выполните следующую команду:

Команда	Описание
router rip *process-id* **enalbe**	Связывает интерфейс с экземпляром указанного процесса. *process-id* – идентификатор процесса

Чтобы сделать интерфейс активным интерфейсом RIP (создать прямой маршрут к интерфейсу, чтобы он мог отправлять и получать пакеты протокола RIP), необходимо выполнение следующих условий: интерфейс связан с экземпляром RIP, интерфейс имеет допустимый IP-адрес и статус интерфейса «включен».

Кроме того, если на интерфейсе включен экземпляр RIP, если VRF экземпляра и назначенный VRF на интерфейсе несовместимы, интерфейс не может стать активным интерфейсом RIP до тех пор, пока его VRF не будет изменен.

Если интерфейс связан с еще не созданным экземпляром RIP, экземпляр RIP будет создан с параметрами VRF (если они указаны) и идентификатором процесса, который будет активирован на этом интерфейсе.

Каждый интерфейс может принадлежать только одному экземпляру RIP.

46.4.2.3 Включение одноадресной рассылки сообщений об обновлении маршрута RIP

RIP – это протокол широковещательного типа. Обновление маршрутов можно настроить так, чтобы они достигали сети, работающей по протоколу без широковещания. Для этого маршрутизатор должен быть настроен таким образом, чтобы обеспечить обмен информацией с нужным устройством.

Выполните следующую команду в режиме настройки маршрутизатора:

Команда	Описание
neighbor *ip-address*	Определяет соседний маршрутизатор для обмена с ним информацией о маршрутизации

Кроме того, если вы хотите контролировать, какие интерфейсы могут использоваться для обмена информацией о маршрутизации, можно выполнить команду **ip rip passive** для обозначения одного или нескольких интерфейсов, запрещающих отправку обновления маршрутов.

46.4.2.4 Использование смещений в метрике маршрута

Список смещений используется для увеличения смещения на входных и выходных маршрутах, которые были изучены с помощью RIP. С другой стороны, вы можете использовать список доступа или интерфейс для ограничения списка смещений. Для увеличения метрики маршрута в режиме настройки маршрутизатора необходимо выполнить следующую команду:

Команда	Описание
offset-list {*interface-type number* | * } {**in** | **out**} *access-list-name offset*	Увеличивает смещение метрики маршрута

46.4.2.5 Настройка таймеров

Протоколы маршрутизации используют несколько таймеров, которые определяют частоту отправки обновлений маршрутов, время, через которое маршрутизатор станет недействительным и другие параметры. Вы можете регулировать эти таймеры, чтобы производительность протоколов маршрутизации более соответствовала требованиям сети.

Также можно регулировать протокол маршрутизации, чтобы ускорить время конвергенции всех видов вычислений IP-маршрутизации, быстро выполнить копирование на резервный маршрутизатор для минимизации времени восстановления после сбоя. Для настройки таймеров следует использовать следующие команды режиме настройки маршрутизатора:

Команда	Описание
timers holddown *value*	Регулирование времени (единица измерения: секунда), необходимого для удаления определенного маршрута из таблицы маршрутизации
timers expire *value*	Регулирование времени (единица измерения: секунда), в течение которого маршрутизатор объявляется недействительным
timers update *value*	Интервал времени между отправкой обновлений маршрутизации (единица измерения: секунда)
timers trigger *value*	Интервал обновления триггера (единица измерения: секунда)
timers peer *value*	интервал тайм-аута однорангового узла (единица измерения: секунда)

46.4.2.6 Назначение номера версии RIP

RIP-2 маршрутизатора данной серии поддерживает аутентификацию, управление паролями, сводку маршрутов, CIDR и VLSM.

По умолчанию маршрутизатор может получать обновления RIPv1 и RIPv2, а отправлять – только обновления RIP-1. Маршрутизатор можно настроить на получение и отправку только обновлений RIPv1 или на получение и отправку только обновлений RIPv2. Для этого в режиме настройки маршрутизатора необходимо выполнить следующую команду:

Команда	Описание
version {**1** | **2**}	Настройка маршрутизатора для отправки и получения обновлений только RIPv1 или RIPv2

Эта команда контролируют поведение RIP по умолчанию. Также можно настроить определенный интерфейс, чтобы изменить это поведение. Для этого необходимо использовать следующие команды в режиме настройки интерфейса:

Команда	Описание
ip rip send version 1	Настраивает интерфейс для отправки только обновлений RIP-1
ip rip send version 2	Настраивает интерфейс для отправки только обновлений RIP-2
ip rip send version compatibility	Отправка путем широковещания сообщений обновления RIP-2
ip rip v1demand	Отправка пакетов RIP-1 при получении запроса
ip rip v2demand	Отправка пакетов RIP-2 при получении запроса

В то же время для управления интерфейсом для получения обновлений RIP-1 и RIP-2 в режиме настройки интерфейса необходимо использовать следующие команды:

Команда	Описание
ip rip receive version 1	Настройка интерфейса для получения обновлений только RIP-1
ip rip receive version 2	Настройка интерфейса для получения обновлений только RIP-2
ip rip receive version 1 2	Настройка интерфейса для получения обновлений RIP-1 и RIP-2

46.4.2.7 Активация «пассивного» и «глухого» статуса интерфейса

По умолчанию интерфейс, поддерживаемый RIP, может пересылать и получать обновления маршрутизации, гибко применяя протокол RIP.

Для настройки пассивного и глухого статуса выполните следующие команды в режиме настройки интерфейса:

Команда	Описание
ip rip passive	Интерфейс не будет пересылать RIP-обновления
ip rip deaf	Интерфейс не будет принимать пакеты RIP-обновлений

46.4.2.8 Активация аутентификации RIP

Протокол RIP-1 не поддерживает аутентификацию, то есть он не может проверять, что маршрутная информация, которую он получает, действительно от надежных источников.

В случае использования протокола RIP-2 с настройками для передачи и приема информации, можно включить аутентификацию RIP на интерфейсе. Это позволяет обеспечить безопасность при обмене данными маршрутов.

На активированном интерфейсе RIP-2 поддерживает несколько методов аутентификации: аутентификацию в виде обычного текста, аутентификацию с использованием MD5, и динамическую аутентификацию с применением MD5 и SHA1. По умолчанию, каждая группа RIP-2 использует аутентификацию в виде обычного текста.

Из соображений безопасности не рекомендуется использовать аутентификацию в виде открытого текста в группе RIP, поскольку ключ аутентификации без шифрования пересылается в каждую группу RIP-2. Если безопасность не учитывается (например, хост с ошибочной конфигурацией не может участвовать в маршруте), аутентификация по открытому тексту допустима.

Чтобы настроить аутентификацию RIP по открытому тексту, выполните следующие действия в режиме настройки интерфейса:

Команда	Описание
ip rip authentication simple	Настраивает интерфейс с аутентификацией в виде открытого текста
ip rip password *string*	Настраивает ключ аутентификации в виде открытого текста

Чтобы настроить аутентификацию RIP при помощи MD5, выполните следующие действия в режиме настройки интерфейса:

Команда	Описание
ip rip authentication md5	Настраивает интерфейс с аутентификацией MD5
ip rip md5-key *key-ID* **md5** *key*	Настраивает ключ аутентификации MD5 и идентификатор аутентификации

Чтобы настроить динамическую аутентификацию RIP, выполните следующие действия в режиме настройки интерфейса:

Команда	Описание
ip rip authentication dynamic	Настраивает интерфейс с динамической аутентификацией (MD5 и SHA1.
ip rip dynamic-key *key-ID* {**md5** | **sha1** } *key xxxx-xx-xx-xx:xx xx:xx*	Настраивает ключ динамической аутентификации и идентификатор аутентификации

После настройки конфигурации аутентификации RIP выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
ip rip authentication commit	Применяет внесенные изменения, активируя выбранный метод аутентификации для протокола RIP

46.4.2.9 Запрет суммирования маршрутов

По умолчанию протокол RIP-2 автоматически суммирует маршруты при пересечении границ сети, чтобы уменьшить объем информации. Это означает, что маршруты объединяются в более крупные блоки при передаче за пределы классифицированной сети. Функция автоматического сбора маршрутов RIP-1 всегда активирована.

Однако, если у вас есть отдельная подсеть, которую вы не хотите объединять в более крупный блок при пересечении границы сетей, то вам нужно запретить автоматическое суммирование маршрутов.

В режиме настройки маршрутизатора выполните следующую команду:

Команда	Описание
no auto-summary	Запрещает автоматическое суммирование

46.4.2.10 Запрет аутентификации исходного IP-адреса и нулевого домена

По умолчанию маршрутизатор проверяет подлинность IP-адреса источника полученного обновления маршрута. Если этот адрес недопустим, обновление маршрутизатора будет отклонено.

Если у вас есть маршрутизатор и вы надеетесь получить от него обновление, но не настроили соответствующую информацию о сети или соседнем узле на приемнике, эту функцию следует запретить. Однако в обычной практике такую команду использовать не рекомендуется. По умолчанию маршрутизатор аутентифицирует нулевой домен полученной записи маршрута в соответствии с версией 1. Если соответствующее поле не проходит аутентификацию нулевого домена, запись маршрутизации будет отброшена. Если конфигурация не включает эту аутентификацию, это может привести к тому, что локальный узел узнает неверную информацию о маршрутизации от однорангового узла.

Для запрета вышеописанных функций, настроенных по умолчанию, выполните следующие команды в режиме настройки маршрутизатора:

Команда	Описание
no validate-update-source	Запрещает аутентифицировать исходный IP-адрес входящего обновления RIP
no check-zero-domain	Запрещает аутентифицировать нулевой домен входящего обновления RIP

46.4.2.11 Максимальное количество эквивалентных маршрутов

По умолчанию локальная таблица маршрутизации RIP может содержать до 4 эквивалентных маршрутов. Если система учит информацию о маршрутизации от нескольких соседей на одном и том же сетевом сегменте и генерирует эквивалентные маршруты, и если количество таких маршрутов на определенном сетевом сегменте превышает текущий максимум, то такие маршруты не могут быть добавлены в базу данных RIP.

Выполните команды из следующей таблицы, чтобы настроить максимальное количество эквивалентных маршрутов в локальной таблице маршрутизации RIP в режиме настройки маршрутизатора.

Команда	Описание
maximum-nexthop *number*	Настраивает максимальное количество эквивалентных маршрутов для таблицы маршрутизации RIP
No maximum-nexthop	Восстанавливает максимальное количество маршрутов по умолчанию в таблице маршрутизации RIP

46.4.2.12 Активация или запрет режима расщепления горизонта

В обычных условиях маршрутизатор, подключенный к IP-сети и использующий протокол дистанционно-векторной маршрутизации, будет использовать расщепление горизонта для оптимизации общения между несколькими маршрутизаторами, особенно когда образуется петля.

Расщепленный горизонт препятствует передаче информации о маршруте обратно по тому интерфейсу, с которого эта информация была получена. Однако, при работе с нешироковещательными сетями, например, Frame Relay (FR), применение данной функции может обернуться сложностями, поэтому во многих случаях рекомендуется ее отключить.

Также стоит упомянуть, что, если интерфейс настроен с дополнительным IP-адресом, и при этом включено расщепление горизонта, исходный IP-адрес обновления маршрута может не включать все вторичные IP-адреса. В каждом обновлении маршрутизации исходный IP-адрес будет включать только один номер сети, если, конечно, расщепление горизонта не отключено.

Чтобы активировать или запретить расщепление горизонта, в режиме настройки интерфейса необходимо выполнить следующие команды:

Команда	Описание
ip rip split-horizon {**simple** | **poisoned**}	Активирует расщепление горизонта
no ip rip split-horizon {**simple** | **poisoned**}	Запрещает расщепление горизонта

По умолчанию для интерфейса «точка-точка» активируется расщепленный горизонт; для интерфейса «точка-множество точек» расщепление горизонта запрещено. Необязательные параметры **simple** и **poisoned** представляют собой простое расщепление горизонта и расщепление горизонта с отравлением обратного маршрута соответственно.

Обычно рекомендуется оставить состояние по умолчанию неизменным, если только вы не уверены, что ваше приложение не сможет правильно объявить маршрут, пока вы не измените настройки. Всегда помните: если расщепление горизонта запрещено на последовательном интерфейсе (и интерфейс подключен к сети с коммутацией пакетов), вам необходимо запретить расщепление горизонта для всех маршрутизаторов соответствующей группы многоадресной рассылки в этой сети.

46.4.2.13 Мониторинг и поддержка RIP

При мониторинге и обслуживании RIP может отображаться сетевая статистика, такая как: конфигурация параметров протокола RIP, использование сети, отслеживание сетевых коммуникаций в реальном времени и т. д. Эта информация может помочь оценить использование сетевых ресурсов, а также решить сетевые проблемы и узнать о доступности сетевых узлов.

Следующие команды можно использовать для отображения информации о всех видах маршрутов, по которым собирается статистика:

Команда	Описание
show ip rip	Отображает текущее состояние всех процессов RIP
Show ip rip *process-id*	Отображает текущее состояние указанного процесса RIP
show ip rip *process-id* **database**	Отображает все маршруты RIP
show ip rip *process-id* **protocol**	Отображает всю необходимую информацию о протоколе RIP
Show ip rip *process-id* **interface**	Отображает все интерфейсы и состояния интерфейсов указанного RIP
show ip rip *process-id* **peer**	Отображает все одноранговые узлы и состояния указанного RIP

Отладочная информация RIP доступна в режиме управления:

Команда	Описание
debug ip rip database	Отслеживает информацию о процедуре маршрутизации RIP, такую как вставка в

	таблицу маршрутизации, удаление из таблицы маршрутизации, изменение маршрутов и т. д.
debug ip rip packet [**send** | **receive**]	Отслеживает сообщения протокола RIP
debug ip rip message	Отслеживает события RIP, например, стечение тайм-аута

46.4.3 Пример настройки RIP

Два коммутатора, A и B, соединяются следующим образом:

Коммутатор A:

```
interface vlan1
ip address 192.168.20.81 255.255.255.0
ip rip 1 enable
!
interface loopback 0
ip address 10.1.1.1 255.0.0.0
ip rip 1 enable
!
router rip 1
!
```

Коммутатор B:

```
interface vlan1
ip address 192.168.20.82 255.255.255.0
ip rip 1 enable
!
interface loopback 0
ip address 20.1.1.1 255.0.0.0
ip rip 1 enable
!
router rip 1
!
```

46.5 BEIGRP

46.5.1 Обзор

Технология, используемая динамическим протоколом BEIGRP, аналогична протоколу дистанционно-векторной маршрутизации:

- маршрутизатор принимает решения о маршрутизации только на основе информации, предоставленной напрямую подключенными соседями;
- маршрутизатор предоставляет информацию о маршрутизации, которую он использует, только напрямую подключенным соседям.

Но BEIGRP имеет некоторые основные отличия от протокола дистанционно-векторной маршрутизации, что дает ему больше преимуществ:

- BEIGRP сохраняет в таблице топологии все маршруты от всех соседей, а не только лучшие на данный момент маршруты;
- BEIGRP отправляет запросы соседям, когда не может получить доступ к месту назначения и нет альтернативных маршрутов, поэтому скорость конвергенции BEIGRP может конкурировать с лучшими протоколами состояния канала.

Алгоритм диффузного обновления (DUAL) важная функция, дающая BEIGRP преимущество перед другими традиционными дистанционно-векторными протоколами. Функция всегда активно работает и опрашивает соседей, когда не может получить доступ к месту назначения и нет альтернативных маршрутов (возможная замена). Поскольку процесс конвергенции является активным, а не негативным (ожидание тайм-аута маршрутизаторов), скорость конвергенции BEIGRP очень высока.

BEIGRP – это специальный протокол маршрутизации, разработанный для адаптации к требованиям EIGRP и непосредственно основанный на IP. BEIGRP выполняет следующие требования:

- динамическое обнаружение новых соседей и исчезновение старых соседей через сообщение «Hello»;
- передача данных надежна;
- протокол передачи позволяет передавать данные в режимах одноадресной и многоадресной передачи;
- протокол передачи сам может адаптироваться к изменению сетевых условий и реакции соседей;
- BEIGRP может ограничить процент занятости пропускной способности сети в соответствии с требованиями.

46.5.2 Настройка BEIGRP

Для настройки BEIGRP необходимо выполнить следующие задачи, среди которых необходима активация BEIGRP, а другие можно решить в соответствии с требованиями:

- Активация протокола BEIGRP
- Настройка процента используемой пропускной способности
- Настройка арифметического коэффициента суммарного расстояния BEIGRP
- Использование смещения для настройки суммарного расстояния
- Отключение автоматического суммирования
- Импортирование других маршрутов в процесс BEIGRP
- Настройка таймеров BEIGRP
- Отключение расщепления горизонта
- Мониторинг и поддержка BEIGRP

46.5.2.1 Активация протокола BEIGRP

Для создания процесса BEIGRP необходимо выполнить следующие команды:

Команда	Описание
router beigrp *as-number*	Добавляет процесс BEIGRP в режиме глобальной конфигурации
network *network-number network-mask*	Добавляет адреса к указанному процессу BEIGRP в режиме настройки маршрутизатора

После завершения вышеуказанной настройки BEIGRP начнет работать на всех интерфейсах, принадлежащих этому адресу, обнаружит новых соседей через «Hello» и осуществит первоначальное взаимодействие по маршрутизации через «Update».

46.5.2.2 Настройка процента используемой пропускной способности

По умолчанию BEIGRP может занимать не более 50 % пропускной способности. Возможно, вы захотите изменить это значение по умолчанию, чтобы гарантировать нормальное взаимодействие других данных, или захотите настроить фактическую используемую полосу пропускания BEIGRP с помощью команды, чтобы согласовать ее с имеющимися настройками пропускной способности интерфейса. В этих случаях необходимо использовать следующие команды в режиме настройки интерфейса:

Команда	Описание

ip beigrp bandwidth-percent *percent*	Настраивает максимальный процент полосы пропускания, используемый сообщениями BEIGRP

46.5.2.3 Настройка арифметического коэффициента суммарного расстояния BEIGRP

В определенных ситуациях может потребоваться корректировка арифметического коэффициента суммарного расстояния BEIGRP, что, в конечном итоге, влияет на политику маршрутизации. Хотя арифметический коэффициент BEIGRP по умолчанию удовлетворяет требованиям большинства сетей, при определенных условиях его все же может потребоваться скорректировать. Эта настройка может привести к большим изменениям во всей сети, поэтому ее должны выполнять самые опытные инженеры.

Используйте следующую команду в режиме настройки маршрутизатора:

Команда	Описание
metric weights *k1 k2 k3 k4 k5*	Настройка арифметического коэффициента суммарного расстояния BEIGRP

46.5.2.4 Использование смещения для настройки суммарного расстояния

С помощью списка смещения можно умышленно увеличивать значение расстояния для всех входящих и исходящих маршрутов в соответствии с заданными требованиями. Это делается для определенных маршрутов, удовлетворяющих определённым условиям. Цель такого подхода – влияние на итоговую маршрутизацию, чтобы она соответствовала нашим ожиданиям. На этапе настройки пользователь может выбирать между списком доступа или применяемым интерфейсом в списке смещения, в зависимости от своих потребностей, чтобы конкретно указать, для каких маршрутов следует применять операцию увеличения смещения.

Выполните следующую команду:

Команда	Описание
offset {*type number* | *} {**in** | **out**} *access-list-name offset*	Применяет список смещения

46.5.2.5 Отключение автосуммирования

Автоматическое суммирование BEIGRP отключено по умолчанию и в настоящее время не поддерживается:

Команда	Описание
no auto-summary	Отключает автосуммирование

46.5.2.6 Импортирование других маршрутов в процесс BEIGRP

Операция перераспределения следует следующим правилам:

- Нет необходимости настраивать параметры с помощью команды **default-metric** при перераспределении статических и прямо подключенных маршрутов. Соответствующий параметр (например, пропускная способность, задержка, надежность, нагрузка и MTU) получается из соответствующих настроек интерфейса.
- Нет необходимости настраивать параметры с помощью команды **default-metric** при перераспределении маршрутов другого процесса BEIGRP. Соответствующий параметр получается из исходного процесса.
- Необходимо настроить параметры с помощью команды **default-metric** при импортировании маршрутов из других протоколов (например, RIP, OSPF). Соответствующий параметр проверяется конфигурацией **default-metric**. Если перераспределить маршруты этих типов без команды **default-metric**, то перераспределение не сработает.

В маршрутизаторе, использующем протокол BEIGRP и протокол RIP, необходимо настроить параметры с помощью следующих команд, когда нужно получить маршруты из протокола RIP в протокол BEIGRP:

Команда	Описание
default-metric *bandwidth delay reliability loading mtu*	Настраивает параметр перераспределения по умолчанию
redistribute *protocol* [*process*] [**route-map** *name*]	Перераспределяет маршруты в протокол BEIGRP

46.5.2.7 Настройка дополнительных параметров BEIGRP

Чтобы адаптироваться к различным сетевым средам и сделать BEIGRP более эффективным и полнофункциональным, может потребоваться настроить следующие параметры:

- временной интервал BEIGRP для отправки сообщений «Hello» и таймаут времени устаревания информации о соседних устройствах;
- расщепление горизонта

1. Настройка временного интервала BEIGRP для отправки сообщений «Hello» и таймаута времени устаревания информации о соседних устройствах

Алгоритм отправки сообщений «Hello» выполняет три функции, обеспечивающие правильную работу BEIGRP:

- обнаруживает доступных новых соседей. Обнаружение происходит автоматически и не требует ручной настройки;

- проверяет конфигурацию соседей и разрешает связь только с соседями, настроенными в совместимом режиме;
- продолжает поддерживать доступность соседей и обнаруживает их исчезновение.

Маршрутизатор отправляет многоадресный пакет «Hello» на все интерфейсы, на которых работает BEIGRP. Все маршрутизаторы, поддерживающие BEIGRP, входят в эти группы многоадресной рассылки, чтобы они могли обнаружить всех соседей.

Протокол «Hello» использует два таймера для обнаружения исчезновения соседей: интервал приветствия определяет частоту отправки сообщений приветствия BEIGRP на интерфейс маршрутизатора, а таймер удержания определяет интервал времени, в течение которого маршрутизатор должен ждать данные связи от соседнего устройства до объявления о его исчезновении. Каждый раз, когда маршрутизатор получает пакет BEIGRP от соседнего узла, он сбрасывает таймер удержания.

Для разных типов сети и разной пропускной способности будет использоваться разное значение таймера приветствия по умолчанию (см. таблицу 46-1).

Таблица 46-1 – Значение таймеров по умолчанию

Инкапсуляция типа интерфейса		Таймер приветствия (секунды)	Таймер удержания (секунды)
Интерфейс LAN	Любой	5	15
Интерфейс WAN	HDLC или PPP	5	15
	Интерфейс NBMA, пропускная способность <=T1	60	180
	Интерфейс NBMA, пропускная способность >T1	5	15
	Субинтерфейс типа «точка-точка» интерфейса NBMA	5	15

Разница в значении таймера по умолчанию в протоколе «Hello» может привести к тому, что соседи BEIGRP, подключенные к разным IP-подсетям, будут использовать разные таймеры приветствия и удержания. Для решения этой проблемы каждый маршрутизатор указывает свой собственный таймер Hold в Hello-пакете, и каждый маршрутизатор BEIGRP использует этот указанный таймер от соседей для определения времени ожидания данного соседа. Это может привести к появлению разных таймеров обнаружения ошибок соседей в разных частях одной и той же сети WAN. Но в некоторых случаях значения таймеров по умолчанию не подходят, поэтому если вы хотите настроить интервал отправки сообщений «Hello», используйте следующую команду:

Команда	Описание

ip beigrp hello-interval *seconds*	Регулирует временной интервал отправки приветственного сообщения из этого интерфейса

Если вы хотите настроить время ожидания соседа, используйте следующую команду:

Команда	Описание
ip beigrp hold-time *seconds*	Регулирует временной интервал, по истечении которого соседний узел объявляется несуществующим

2. Отключение расщепления горизонта

В обычных условиях целесообразно использовать функцию расщепления горизонта. Это предотвратит передачу информации о маршрутизации обратно на ее исходный интерфейс, чтобы избежать зацикливания маршрута. Но при определенных обстоятельствах это неоптимальный выбор, в таком случае можно использовать следующую команду, чтобы отключить данную функцию:

Команда	Описание
no ip beigrp split-horizon	Отключает расщепление горизонта

46.5.2.8 Мониторинг и поддержка BEIGRP

Чтобы очистить информацию об окружении, используйте следующую команду:

Команда	Описание
clear ip beigrp neighbors [*as-number* | *interface*]	Удаляет информацию о соседях

Чтобы отобразить различную статистическую информацию BEIGRP, выполните следующие команды:

Команда	Описание
show ip beigrp interface [*interface*] *[as-number*]	Отображает информацию об интерфейсе
show ip beigrp neighbors [*as-number* | *interface*]	Отображает информацию о соседях
show ip beigrp topology [*as-number* | **all-link | summary | active**]	Отображает информацию о топологии

46.6 OSPF

46.6.1 Обзор

OSPF – это протокол динамической маршрутизации внутреннего шлюза (IGP), основанный на технологии отслеживания состояния канала. Он предназначен для маршрутизации IP-трафика внутри сети, поддерживает информацию о подсетях IP и внешних маршрутах, а

также обеспечивает аутентификацию сообщений и поддерживает многоадресную рассылку.

Реализация OSPF коммутатора данной серии соответствует спецификации OSPF V2 (относится к RFC2328). Некоторые ключевые моменты реализации перечислены ниже:

Тупиковая зона – поддержка тупиковой зоны (Stub Area), что означает, что внутри этой области используются особые правила маршрутизации.

Перераспределение маршрутов – возможность передачи маршрутов, полученных одним маршрутизационным протоколом, другому. Например, маршруты, изученные OSPF, могут быть переданы протоколу RIP, и наоборот. Это также работает между разными автономными системами и другими протоколами, такими как BGP.

Аутентификация – поддержка методов аутентификации, включая Plaintext и MD5, для обеспечения безопасности при обмене данными между соседними маршрутизаторами в одной области.

Параметры интерфейса маршрутизатора – возможность настройки различных параметров интерфейса, таких как стоимость исходящего соединения, интервал переотправки, задержка передачи, приоритет маршрутизатора, интервал передачи Hello-сообщений и пароль аутентификации.

Зона NSSA – это отсылка к RFC 1587 и связанным с ним особенностям области NSSA (Not So Stubby Area) в OSPF.

OSPF и виртуальный канал – упоминается RFC 1793, который связан с использованием OSPF в контексте виртуальных каналов.

46.6.2 Настройка OSPF

OSPF требует обмена данными маршрутизации между всеми маршрутизаторами ABR и ASBR в области. Чтобы упростить настройку, можно позволить им всем работать с параметрами по умолчанию (без аутентификации и т. д.), но, если вы хотите изменить некоторые параметры, необходимо гарантировать идентичность параметров на всех маршрутизаторах.

Чтобы настроить OSPF, выполните следующие задачи. Помимо необходимости активации OSPF, все остальные настройки не являются обязательными.

- Запуск OSPF
- Настройка параметров интерфейса OSPF
- Настройка типа сети OSPF
- Настройка широковещательной сети «один-ко-множеству»
- Настройка нешироковещательной сети
- Настройка домена OSPF
- Настройка зоны NSSA

- Настройка суммирования маршрутов в домене OSPF
- Настройка сбора данных пересылающим маршрутизатором
- Создание маршрута по умолчанию
- Выбор идентификатора маршрутизатора через интерфейс Loopback
- Настройка административной дистанции OSPF
- Настройка таймера расчета маршрута
- Настройка функции связи по требованию
- Мониторинг и поддержка OSPF

46.6.2.1 Запуск OSPF

Как и другие протоколы маршрутизации, активация OSPF требует создания процесса маршрутизации, выделения диапазона IP-адресов, связанного с исполняемым процессом, выделения идентификатора области, связанного с диапазоном IP-адресов. В режиме глобальной конфигурации используйте следующие команды:

Команда	Описание
router ospf *process-id*	Активирует протокол маршрутизации OSPF и входит в режим настройки маршрутизатора
network *address mask* **area** *area-id*	Настраивает интерфейс(ы), на которых работает OSPF, и идентификатор зоны

46.6.2.2 Настройка параметров интерфейса OSPF

Во время реализации OSPF разрешено изменять параметры OSPF, относящиеся к интерфейсу, в соответствии с требованиями. Нет необходимости изменять какой-либо параметр, но идентичность параметров должна быть гарантирована на всех маршрутизаторах в подключенной сети.

В режиме настройки интерфейса используйте следующие команды:

Команда	Описание
ip ospf authentication	Настраивает метод аутентификации для отправки и получения пакетов OSPF
ip ospf cost *cost*	Настраивает метрику интерфейса OSPF для пересылки пакетов
ip ospf retransmit-interval *seconds*	Устанавливает интервал повторной передачи LSA между соседями, принадлежащими одному и тому же интерфейсу OSPF (в секундах)
ip ospf transmit-delay *seconds*	Настраивает расчетное время передачи LSA на интерфейсе OSPF (в секундах)

ip ospf priority *number*	Настраивает приоритет маршрутизатора, необходимый для выбора DR
ip ospf hello-interval *seconds*	Настраивает временной интервал для отправки пакета приветствия через интерфейс OSPF
ip ospf dead-interval *seconds*	Настраивает время ожидания ответа соседнего узла (в секундах). Если маршрутизатор не получает пакет «Hello» от соседа в течение определенного интервала времени, он считает, что соседний маршрутизатор выключен
ip ospf password *key*	Устанавливает пароль простой текстовой аутентификации OSPF на соседнем маршрутизаторе. Этот пароль используется для обеспечения безопасности и аутентификации маршрутизаторов в процессе обмена маршрутной информацией через OSPF. Только маршрутизаторы, знающие этот пароль, могут установить соседство и обмениваться маршрутной информацией
ip ospf message-digest-key *keyid* **md5** *key*	Настраивает аутентификацию MD5
ip ospf passive	Устанавливает интерфейс OSPF в пассивный режим. Когда интерфейс находится в пассивном режиме, он не будет отправлять OSPF Hello-пакеты и, следовательно, не участвует в процессе обнаружения и обмена OSPF маршрутной информацией
ip ospf mtu-ignore	Запрещает проверку значения MTU пакета на порту

OSPF делит физическую среду сети на следующие три категории:

- широковещательная сеть (Ethernet, Token Ring, FDDI);
- нешироковещательная сеть с множественным доступом (SMDS, Frame Relay, X.25);
- сеть «точка-точка» (HDLC, PPP).

Сети X.25 и Frame Relay предоставляют дополнительные возможности широковещательной передачи. OSPF можно настроить для работы в широковещательных сетях с помощью map-команды. Информацию о команде **map** см. в описании команд x.25 и Frame Relay в Справочнике команд WAN.

46.6.2.3 Настройка типа сети OSPF

Независимо от типа физической среды сети, вы можете настроить свою сеть как широковещательную или как нешироковещательную сеть с множественным доступом. Это позволяет гибко настраивать сеть, например, можно преобразовать физическую сеть с широковещательной рассылкой в сеть без нее, а также наоборот. Это также упрощает настройку соседей в сети.

Для уменьшения количества физических подключений можно настроить сеть, включая виртуальные связи между каждым маршрутизатором и другими маршрутизаторами. Это делает сеть более надежной и экономичной. Маршрутизаторы, не расположенные рядом друг с другом, могут обмениваться информацией о маршрутизации через виртуальные каналы.

Интерфейс OSPF «точка-множество точек» может быть определен как несколько сетевых интерфейсов «точка-точка», которые создают несколько маршрутов к хостам. Сеть OSPF «точка-множество точек» имеет следующие преимущества перед нешироковещательной сетью с множественным доступом и сетью «точка-точка»:

Сеть «точка-множество точек» легко настраивается, она не требует специальной настройки соседнего узла, использует только один IP-адрес и не создает DR.

Поскольку для такой сети не требуется построения физической топологии, это обходится дешевле.

Такая сеть более надежна. Даже если виртуальные каналы выходят из строя, соединение все равно сохраняется.

В режиме конфигурации интерфейса настройте тип сети OSPF с помощью следующей команды:

Команда	Описание
ip ospf network {**broadcast** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**]}}	Настраивает тип сети OSPF

В конце этой главы вы можете увидеть пример настройки сети OSPF «точка-множество точек».

46.6.2.4 Настройка широковещательной сети «один-ко-множеству»

Вам не нужно описывать отношения соседства в сети «точка-множество точек» и широковещательной сети. Но вы можете использовать команду **neighbor**, чтобы описать приоритет определенного соседа.

До применения этой команды следует учитывать, что некоторый трафик протокола «точка-множество точек» OSPF является многоадресным. Таким образом, для интерфейса «точка-множество точек» команда **neighbor** не требуется. Пакеты приветствия, обновления и

подтверждения передаются посредством широковещательной рассылки, в частности, многоадресный пакет «Hello» может динамически обнаруживать всех соседей.

В сети «точка-множество точек» маршрутизатор предполагает, что все соседи имеют одинаковую метрику. Это значение можно настроить с помощью команды **ip ospf cost**. На самом деле пропускная способность каждого соседа разная, поэтому и значение должно быть разным. Эта функция применима только к интерфейсу «точка-множество точек».

Используйте следующую команду, чтобы настроить интерфейс как интерфейс «точка-множество точек» и выделить метрику для каждого соседа:

Команда	Описание
ip ospf network point-to-multipoint	Настраивает сеть как «точка-множество точек»
exit	Возвращает в режим глобальной конфигурации
router ospf *process-id*	Настраивает процесс OSPF маршрутизатора и входит в режим настройки маршрутизатора
neighbor *ip-address* **cost** *number*	Назначает соседа и метрику для него. Повторите приведенную выше команду настройки для каждого соседа, которому нужно указать вес. В противном случае соседние устройства используют вес, указанный командой **ip ospf cost**

46.6.2.5 Настройка нешироковещательной сети

Поскольку в сети OSPF много маршрутизаторов, должен быть выбран один DR. Если возможность широковещания не предусмотрена, требуется выполнить настройку параметров для процесса выбора.

Эти параметры выполняют настройку только на маршрутизаторах, которые имеют право стать DR или BDR.

В режиме настройки маршрутизатора используйте следующую команду для настройки маршрутизаторов нешироковещательной сети, которые связаны друг с другом:

Команда	Описание
neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	Настраивает маршрутизатор, подключенный к нешироковещательной сети

Для соседнего маршрутизатора можно назначить следующие параметры:

- приоритет соседнего маршрутизатора;
- интервал опроса без широковещательной передачи;
- определение интерфейса, через который можно обращаться к соседнему маршрутизатору.

В многоточечной нешироковещательной сети вы можете использовать команду **neighbor** для установки отношения с соседним маршрутизатором и назначения опционального приоритета.

В предыдущих версиях программного обеспечения некоторые пользователи настраивали соединения типа «точка-множество точек» в нешироковещательной среде (IP через ATM), поэтому маршрутизатор не мог динамически обнаруживать соседний маршрутизатор. Для решения этой проблему можно использовать команду **neighbor**.

В сети «точка-множество точек» маршрутизатор предполагает, что все соседи имеют одинаковую метрику. Значение метрики можно настроить с помощью команды **ip ospf cost**. Фактически, поскольку пропускная способность каждого соседа различна, значение также должно быть разным. Эта функция применима только к многоточечным интерфейсам.

В режиме конфигурации интерфейса используйте следующие команды для настройки интерфейсов типа точка-множество точек в среде, которая не поддерживает широковещание:

Команда	Описание
ip ospf network point-to-multipoint non-broadcast	Настраивает интерфейс «точка-многоточка» в нешироковещательной среде
exit	Вход в режим глобальной конфигурации
router ospf *process-id*	Создает процесс маршрутизации OSPF и входит в режим настройки маршрутизатора
neighbor *ip-address* [**cost** *number*]	Назначает соседа OSPF и выделяет для него метрику. Повторите приведенную выше команду настройки для каждого соседа, которому необходимо установить значение приоритета

46.6.2.6 Настройка домена OSPF

Настраиваемые параметры зоны включают в себя: аутентификацию, назначение тупиковой зоны, назначение метрики для суммарного маршрута по умолчанию. Аутентификация использует защиту на основе паролей.

Тупиковые зоны (Stub Area) – это те области, в которых не распределяются внешние маршруты. Вместо этого ABR генерирует внешний маршрут по умолчанию для связи с тупиковой зоной, позволяющий ей выйти во внешнюю сеть автономной системы. Чтобы использовать функции поддержки тупиковой зоны OSPF, следует использовать в ней маршрут по умолчанию. Чтобы дополнительно уменьшить количество LSA, отправляемых в тупиковую зону, можно запретить ABR собирать и отправлять сводные сообщения данного типа в эту область.

В режиме настройки маршрутизатора используйте следующие команды для определения параметров зоны:

Команда	Описание
area *area-id* **authentication simple**	Активирует аутентификацию зоны OSPF
area *area-id* **authentication message-digest**	Позволяет OSPF использовать MD5 для аутентификации
area *area-id* **stub [no-summary]**	Определяет тупиковую зону
area *area-id* **default-cost** *cost*	Устанавливает метрику для маршрута по умолчанию в тупиковой зоне

46.6.2.7 Настройка зоны NSSA

Зона NSSA аналогична зоне STUB. Однако NSSA позволяет вводить внешние маршруты. Во время передачи также поддерживаются суммирование маршрутов и фильтрация пакетов. Если интернет-провайдеру требуется использовать удаленную сеть с разными протоколами маршрутизации, NSSA может упростить управление.

Граничный маршрутизатор ядра не может работать в тупиковой зоне OSPF, если не применяется NSSA. Это связано с тем, что маршруты удаленной сети не могут быть перенаправлены в тупиковую зону. Простые протоколы маршрутизации, такие как RIP, могут быть объявлены, но необходимо поддерживать два типа протоколов маршрутизации. NSSA может поместить центральный и удаленный маршрутизаторы в одну и ту же область NSSA, и таким образом OSPF будет применен к удаленной сети.

При использовании зоны NSSA обратите внимание, что маршрут, созданный маршрутизатором ABR, может войти в NSSA после ее настройки. Каждый маршрутизатор в одной и той же зоне должен признать, что он находится в зоне NSSA, иначе разные маршрутизаторы не смогут взаимодействовать друг с другом. Для предотвращения путаницы в передаче пакетов маршрутизатором необходимо использовать определенную версию программного обеспечения на ABR. Это связано с тем, что ABR обрабатывает как внутренний трафик области, так и трафик, идущий через NSSA. Использование правильной версии программного обеспечения помогает избежать ошибок в маршрутизации и обеспечивает корректную передачу пакетов в сети OSPF.

Выполните следующую команду в режиме настройки маршрутизатора, чтобы настроить область NSSA OSPF:

Команда	Описание
area *area-id* **nssa** [**no-redistribution**][**no-summary**][**default-information-originate**] [**translate-always**]	Настраивает зону NSSA

46.6.2.8 Настройка суммирования маршрутов в домене OSPF

Эта функция позволяет маршрутизатору ABR передавать суммарный маршрут другим зонам. В OSPF ABR передает информацию о каждой сети в другие зоны. Однако, если номера сетей можно сгруппировать по определенному методу, и они идут подряд,

целесообразно настроить ABR для передачи другим областям суммарного маршрута. Он может охватывать все сети в определенном диапазоне.

В режиме настройки маршрутизатора используйте следующую команду для определения диапазонов адресов:

Команда	Описание
area area-id **range** address mask	Определяет диапазон адресов для суммирования маршрутов

46.6.2.9 Настройка сбора данных пересылающим маршрутизатором

Когда рамках OSPF маршруты передаются из одной области маршрутизатора в другую в, каждый маршрутизатор выполняет независимую передачу информации в виде внешних LSA. Однако вы можете настроить маршрутизатор так, чтобы он передавал маршруты, которые охватывают определенный диапазон адресов. Этот метод позволяет уменьшить размер базы данных состояния связей OSPF.

В режиме настройки маршрутизатора используйте следующую команду для настройки сбора данных о маршрутах:

Команда	Описание
summary-address *prefix mask* [not advertise]	Описывает адрес и маску, охватывающую распространяемые маршруты. Транслируется только один суммарный маршрут

46.6.2.10 Создание маршрута по умолчанию

Можно указать маршрутизатору, работающему как ASBR, создавать маршрут по умолчанию для входа в область маршрутизации OSPF. Когда вы настраиваете маршрутизатор для распространения маршрутов в область OSPF, этот маршрутизатор автоматически становится ASBR. Однако изначально ASBR не создает маршрут по умолчанию для входа в область маршрутизации OSPF. В режиме настройки маршрутизатора используйте следующую команду, чтобы ASBR создавал маршрут по умолчанию:

Команда	Описание
default-information originate [**always**] [**route-map** *map-name*]	Указывает маршрутизатору ASBR создать маршрут по умолчанию, входящий в область маршрутизации OSPF

46.6.2.11 Выбор идентификатора маршрутизатора через интерфейс Loopback

Интерфейс обратной связи (Loopback) представляет собой виртуальный интерфейс на маршрутизаторе. Он создается программно и не имеет ассоциированных с ним физических аппаратных устройств. Этот интерфейс имеет особое значение в протоколе OSPF.

OSPF использует наибольший IP-адрес, настроенный на интерфейсе, в качестве идентификатора маршрутизатора. Если интерфейс, подключенный к этому IP-адресу, перейдет в состояние ВЫКЛЮЧЕНО или этот IP-адрес будет удален, процесс OSPF перезапустится для расчета нового идентификатора маршрутизатора и повторной отправки информации о маршрутизации со всех интерфейсов.

Если один интерфейс Loopback настроен с IP-адресом, то маршрутизатор использует этот IP-адрес в качестве идентификатора маршрутизатора, поскольку такой интерфейс никогда не отключается, и все это делает таблицу маршрутизации более стабильной.

Маршрутизатор предпочтительно использует интерфейс Loopback в качестве идентификатора маршрутизатора, при этом в качестве идентификатора маршрутизатора выбирает самый большой IP-адрес среди всех Loopback-интерфейсов. Если интерфейс Loopback отсутствует, используется наибольший IP-адрес маршрутизатора. Вы не можете указать OSPF использовать какой-либо конкретный интерфейс.

В глобальном режиме используйте следующую команду для настройки интерфейса IP Loopback:

Команда	Описание
interface loopback 0	Создает интерфейс обратной связи и входит в режим настройки интерфейса
ip address *ip-address mask*	Выделяет IP-адрес для интерфейса

46.6.2.12 Настройка административной дистанции OSPF

Административная дистанция определяет уровень надежности источника информации о маршрутах, такого как маршрутизатор или группа маршрутизаторов. Общими словами, административная дистанция – это целое число от 0 до 255, и чем выше значение, тем ниже уровень надежности. Если административная дистанция равна 255, то источник информации о маршруте не считается надежным и его следует игнорировать.

В OSPF используются три типа административной дистанции: для маршрутов внутри зоны (inner-domain), для маршрутов к другим зонам (inter-domain) и для маршрутов, распространяемых из других протоколов маршрутизации (exterior). Значение административной дистанции по умолчанию для каждого типа маршрута равно 110.

В режиме настройки маршрутизатора используйте следующую команду для установки значения административной дистанции OSPF:

Команда	Описание
distance ospf [**intra-area** *dist1*] [inter-area *dist2*] [**external** *dist3*]	Изменяет значение административной дистанции для внутреннего, междоменного и внешнего маршрута OSPF

46.6.2.13 Настройка таймера расчета маршрута

Вы можете настроить временную задержку между моментом получения OSPF информации о топологических изменениях и началом расчета таблицы маршрутизации по алгоритму SPF. Также можно настроить интервал между двумя последовательными расчетами SPF. В режиме настройки маршрутизатора используйте следующие команды:

Команда	Описание
timers delay *delaytime*	Устанавливает задержку начала расчета маршрута после получения данных
timers hold *holdtime*	Устанавливает минимальный временной интервал между двумя последовательными расчетами SPF

46.6.2.14 Настройка функции связи по требованию

Настройка связи по требованию (On-Demand Link) в протоколе OSPF позволяет сделать работу протокола более эффективной в случае использования сетей, где соединение устанавливается только по необходимости (например, при дозвоне).

Основная идея заключается в том, что OSPF обменивается пакетами HELLO и пакетами обновления состояния связи между подключенными маршрутизаторами после установки соединения или изменения информации в маршрутах. Это означает, что минимальное связующее дерево будет пересчитываться и пакеты будут передаваться только тогда, когда топология действительно изменяется.

Если соединение представляет из себя связь «точка-точка», то настройка проводится на одном из терминалов. Конечно же, маршрутизатор на другом конце также должен поддерживать эту функцию. Если соединение «точка-множество точек», то настройка проводится на многоточечном терминале.

Рекомендуется настраивать функцию связи по требованию в зоне типа STUB. Если эта настройка применяется ко всем маршрутизаторам в тупиковой зоне, то маршрутизаторы вне этой области могут не поддерживать связь по требованию. Если функция настроена в стандартной области, то все стандартные области должны ее поддерживать.

Когда связь по требованию настроена в сети, работающей на основе широковещательной передачи, пакеты обновления состояния связи могут быть ограничены, в отличие от пакетов HELLO, которые ничем не ограничиваются. Это происходит потому, что пакеты HELLO используются для поддержания коммуникации соседей и выбора маршрутизатора DR.

Запустите следующую команду в режиме настройки интерфейса:

Команда	Описание
ip ospf demand-circuit	Настраивает функцию связи по требованию

46.6.2.15 Мониторинг и поддержка OSPF

Команда **show** позволяет отображать статистическую информацию о сети, такую как статистика содержимого таблицы IP-маршрутизации, кэша, базы данных и т. д. Эта информация может помочь оценить использование сетевых ресурсов и решить возникшую сетевую проблему. Вы можете проверить доступность сетевых узлов, узнать маршрут, по которому пакет данных проходит через сеть.

Используйте следующие команды для отображения различной статистики маршрутизации:

Команда	Описание
show ip ospf [*process-id*]	Отображает общую информацию о процессе маршрутизации OSPF
show ip ospf [*process-id*] **database** [**router**| **network**| **summary**| **asbr-summary**| **external**| **database-summary**] { *link-state-id* | **self-originate** | **adv-router** [*ip-address*]}	Отображает соответствующую информацию о базе данных OSPF
show ip ospf border-routers	Отображает запись внутренней таблицы маршрутизации ABR и ASBR
show ip ospf interface	Отображает информацию об интерфейсе OSPF
show ip ospf neighbor	Отображает информацию о соседях OSPF в соответствии с интерфейсом
debug ip ospf adj	Отображает информацию об установлении коммуникации соседних узлов OSPF
debug ip ospf events	Отображает информацию о событиях, связанных с OSPF, таких как изменения состояния интерфейсов, обмен OSPF-пакетами и т.д.
debug ip ospf flood	Отображает информацию о процессе заполнения базы данных OSPF
debug ip ospf lsa-generation	Отображает информацию о генерации LSA OSPF
debug ip ospf packet	Отображает информацию о сообщениях OSPF
debug ip ospf retransmission	Отображает информацию о повторной передаче сообщений OSPF
debug ip ospf spf [**intra**| **external**]	Отображает информацию о расчетах SPF
debug ip ospf tree	Отображает информацию о создании дерева SPF

46.6.3 Примеры настройки OSPF

46.6.3.1 Примеры настройки двухточечной нешироковещательной OSPF

Коммутатор A:

```
interface vlan 1
 ip address 10.0.1.1 255.255.255.0
 ip ospf network point-to-multipoint non-broadcast
!
router ospf 1
 network 10.0.1.0 255.0.0.0 area 0
 neighbor 10.0.1.3 cost 5
 neighbor 10.0.1.4 cost 10
```

Коммутатор B:

```
interface vlan 1
 ip address 10.0.1.3 255.255.255.0
 ip ospf network point-to-multipoint non-broadcast
!
router ospf 1
 network 10.0.1.0 255.0.0.0 area 0
 neighbor 10.0.1.1
 neighbor 10.0.1.4 cost 14
```

Коммутатор C:

```
interface vlan 1
 ip address 10.0.1.4 255.255.255.0
 ip ospf network point-to-multipoint non-broadcast
!
router ospf 1
 network 10.0.1.0 255.0.0.0 area 0
 neighbor 10.0.1.1
 neighbor 10.0.1.3
```

46.6.3.2 Пример настройки маски подсети переменной длины

OSPF и статическая маршрутизация поддерживают маски подсети переменной длины (VLSM). С помощью VLSM вы можете использовать разные маски для одного и того же номера сети на разных интерфейсах, что экономит IP-адреса и позволяет более эффективно использовать адресное пространство.

В следующем примере используется 30-битная маска подсети, а двухбитное адресное пространство зарезервировано в качестве адреса хоста последовательного порта. Этого достаточно для последовательного соединения двух адресов хостов «точка-точка».

```
interface vlan 1
 ip address 131.107.1.1 255.255.255.0
!
interface serial 1/1
 ip address 131.107.254.1 255.255.255.252
!
router ospf 107
 network 131.107.0.0 255.255.0.0 area 0.0.0.0
```

46.6.3.3 Примеры настройки маршрута OSPF и распределения маршрутов

OSPF требует обмена информацией между многими внутренними маршрутизаторами, ABR и ASBR. При минимальной конфигурации маршрутизаторы на базе OSPF могут работать с параметрами по умолчанию и не требуют аутентификации.

Ниже представлены три примера настройки.

- В первом примере используется базовая команда OSPF.
- Второй пример показывает настройку внутреннего маршрутизатора, ABR и ASBR в одной автономной системе OSPF.
- Третий пример иллюстрирует более сложный пример настройки с использованием различных инструментов OSPF.

1. Пример базовой конфигурации OSPF

Следующий пример иллюстрирует простую настройку OSPF. Активируйте процесс маршрутизации 90, затем подключите виртуальную локальную сеть 1 к зоне 0.0.0.0. Также перераспределите RIP в OSPF, OSPF в RIP.

```
interface vlan 1
 ip address 130.130.1.1 255.255.255.0
!
router ospf 90
 network 130.130.0.0 255.255.0.0 area 0
 redistribute rip 1
!
router rip 1
 redistribute ospf 90
```

2. Пример базовой конфигурации внутреннего маршрутизатора, ABR и ASBR

В следующем примере выделяется 4 идентификатора областей для 4 диапазонов IP-адресов. Сначала активируется процесс маршрутизации 109, 4 зоны: 10.9.5.0, 2, 3, 0. Маски 10.9.50.0,2,3 обозначают диапазон адресов, но область 0 включает в себя все сети.

```
router ospf 109
 network 131.108.20.0 255.255.255.0 area 10.9.50.0
 network 131.108.0.0 255.255.0.0 area 2
 network 131.109.10.0 255.255.255.0 area 3
 network 0.0.0.0 0.0.0.0 area 0
 redistribute static
!
interface vlan 1
 ip address 131.108.20.5 255.255.255.0
!
interface vlan 2
 ip address 131.108.1.5 255.255.255.0
!
interface vlan 3
 ip address 131.108.2.5 255.255.255.0
!
```

```
interface vlan 4
 ip address 131.109.10.5 255.255.255.0
!
interface vlan 5
 ip address 131.109.1.1 255.255.255.0
!
interface vlan 6
 ip address 10.1.0.1 255.255.0.0
!
ip route 44.0.0.0 255.0.0.0 VLAN1
!
```

Функции команды настройки сетевой зоны **network** являются порядковыми, поэтому последовательность команд важна. Маршрутизатор по порядку сопоставляет пару адрес/маска каждого интерфейса.

Вернемся к первой сетевой области в приведенном выше примере. Идентификатор зоны 10.9.50.0 настроен с маской подсети интерфейса 131.108.20.0. Итак, vlan 1 соответствует. Таким образом, vlan 1 существует только в зоне 10.0.50.0.

Затем переходите ко второй области. За исключением vlan 1, примените тот же процесс к другим интерфейсам, тогда vlan 2 совпадет. Итак, vlan 2 подключается к зоне 2.

Продолжайте сопоставление других зон сети. ОБРАТИТЕ ВНИМАНИЕ, что последняя команда является особым случаем, она означает, что все остальные интерфейсы подключены к сетевой области 0.

3. Пример настройки виртуального канала

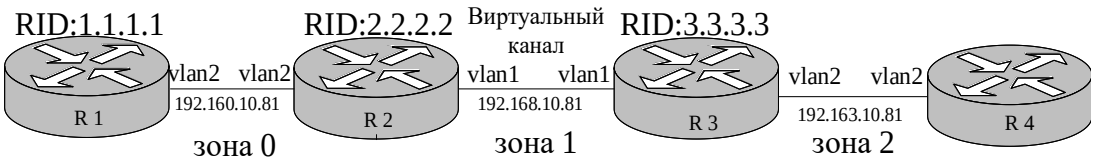

Рисунок 46-2 – Топология сети

Настройка маршрутизаторов, изображенных на рисунке 46-2

R1:

```
interface vlan 2
 ip address 192.160.10.81 255.255.255.0
!
router ospf 1
 router-id 1.1.1.1
 network 192.160.10.81 255.255.255.0 area 0
!
```

R2:

```
interface vlan 1
 ip address 192.168.10.81 255.255.255.0
!
interface vlan 2
 ip address 192.160.10.82 255.255.255.0
!
router ospf 192
 router-id 2.2.2.2
 network 192.168.10.81 255.255.255.0 area 1
 network 192.160.10.82 255.255.255.0 area 0
 area 1 virtual-link 3.3.3.3
!
```

R3:

```
interface vlan 1
 ip address 192.168.10.82 255.255.255.0
!
interface vlan 2
 ip address 192.163.10.81 255.255.255.0
!
router ospf 192
```

```
 router-id 3.3.3.3
 network 192.168.10.82 255.255.255.0 area 1
 network 192.163.10.81 255.255.255.0 area 2
 area 1 virtual-link 2.2.2.2
!
```

4. Пример комплексной настройки OSPF на маршрутизаторе ABR

Следующий пример иллюстрирует несколько задач, связанных с настройкой ABR. Процесс настройки можно разделить на два направления:

- базовая настройка OSPF;
- распределение маршрутов.

Задачи этой конфигурации кратко описаны ниже. Рисунок 46-3 иллюстрирует диапазон и распределение сетевых адресов.

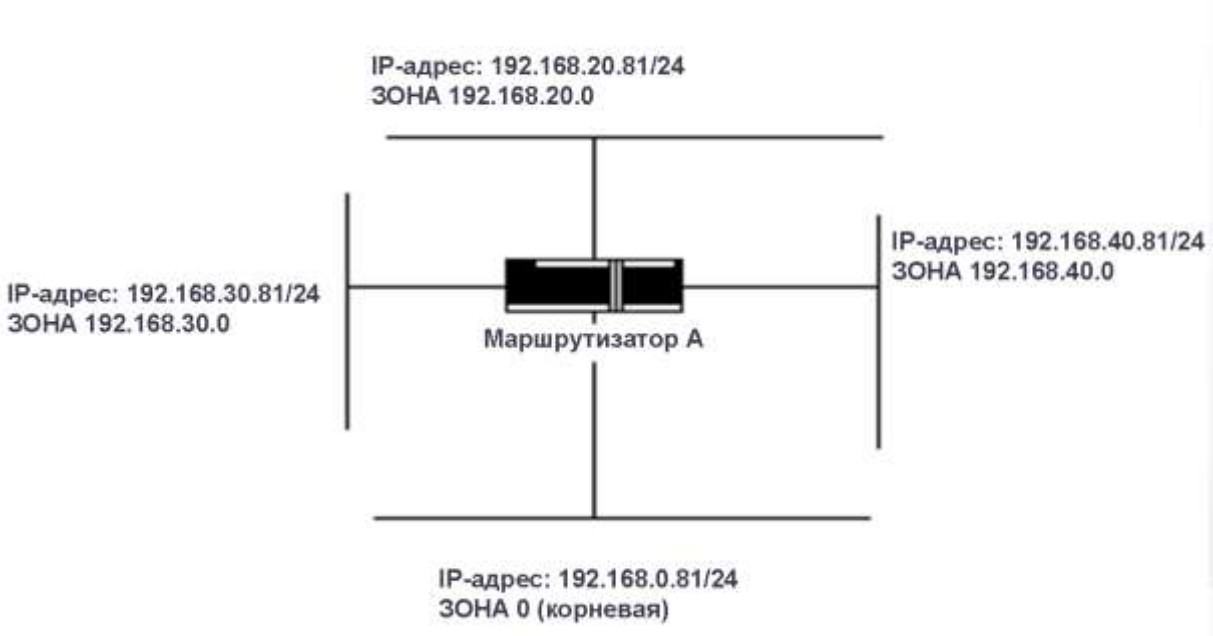

Рисунок 46-3 – Диапазон и распределение сетевых адресов

Задачи базовой настройки OSPF

- Настройка диапазона адресов для VLAN от 1 до 4
- Активация OSPF на каждом интерфейсе

- Установка паролей аутентификации OSPF для каждой зоны и сети
- Установка стоимости пути и других параметров интерфейса
- Создание сети 36.0.0.0 в тупиковой зоне. Для настройки параметров аутентификации и тупиковой зоны используйте команду area соответственно или выполните настройки сразу одной командой.
- Настройка корневой зоны (зона 0).

Задачи настройки, связанные с распределением маршрутов

- Распределение маршрутов IGRP и RIP в настройках параметров OSPF (включая тип метрики, метрику, тег и подсеть).
- Распределение маршрутов IGRP и OSPF в RIP.

```
interface vlan 1
ip address 192.168.20.81 255.255.255.0
ip ospf password GHGHGHG
ip ospf cost 10
!
interface vlan 2
ip address 192.168.30.81 255.255.255.0
ip ospf password ijklmnop
ip ospf cost 20
ip ospf retransmit-interval 10
ip ospf transmit-delay 2
ip ospf priority 4
!
interface vlan 3
ip address 192.168.40.81 255.255.255.0
ip ospf password abcdefgh
ip ospf cost 10
!
interface vlan 4
ip address 192.168.0.81 255.255.255.0
```

ip ospf password ijklmnop

ip ospf cost 20

ip ospf dead-interval 80

!

router ospf 192

network 192.168.0.0 255.255.255.0 area 0

network 192.168.20.0 255.255.255.0 area 192.168.20.0

network 192.168.30.0 255.255.255.0 area 192.168.30.0

network 192.168.40.0 255.255.255.0 area 192.168.40.0

area 0 authentication simple

area 192.168.20.0 stub

area 192.168.20.0 authentication simple

area 192.168.20.0 default-cost 20

area 192.168.20.0 authentication simple

area 192.168.20.0 range 36.0.0.0 255.0.0.0

area 192.168.30.0 range 192.42.110.0 255.255.255.0

area 0 range 130.0.0.0 255.0.0.0

area 0 range 141.0.0.0 255.0.0.0

redistribute rip 1

RIP in network 192.168.30.0:

router rip 1

redistribute ospf 192

!

46.7 BGP

46.7.1 Обзор

В этой главе описывается, как настроить протокол граничного шлюза (BGP). BGP – это протокол внешнего шлюза (EGP), определенный в RFC1163, 1267 и 1771. Он позволяет установить механизм выбора маршрута между различными автономными системами и гарантировать обмен информацией о маршрутизации без образования петель.

46.7.1.1 Реализация BGP маршрутизатора

В BGP каждый маршрут включает в себя номер сети, список автономных систем, которые этот маршрут проходит (так называемый AS-путь), и другие атрибуты. Программное обеспечение данного маршрутизатора поддерживает BGP v4, определенный в RFC1771. Основная функция BGP – обмен информацией о доступности сети с другими системами BGP, включая информацию о AS-пути. Эта информация может использоваться для построения графа связи между автономными системами (AS), что позволяет избегать петель в маршрутизации, а также для реализации политики маршрутизации на уровне AS с использованием графа связи между AS. BGP v4 поддерживает бесклассовый междоменный маршрутизатор (CIDR), что позволяет сократить размер таблицы маршрутизации за счет создания суммарных маршрутов, объединяемых в «суперсеть». CIDR также устраняет концепцию сетевого уровня в BGP и поддерживает трансляцию IP-префиксов. Маршруты CIDR могут передаваться через различные протоколы маршрутизации, такие как OSPF, Enhanced IGRP, ISIS-IP и RIP2.

Важное различие между внешней и внутренней маршрутизацией заключается в том, что маршрутизатор внешнего шлюза имеет более широкие возможности контроля. Для управления маршрутами в BGP предусмотрено несколько дополнительных методов:

1. Фильтрация маршрутов. Для отбора маршрутов можно использовать различные параметры, такие как списки доступа на основе соседей, списки AS-путей (aspath-list), списки префиксов (prefix-list), а также списки доступа на основе интерфейсов и префиксов. Также можно управлять выбором следующего перехода (nexthop) для маршрутов.

2. Изменение атрибутов маршрутов. С помощью карты маршрутизации (route-map) можно изменять атрибуты маршрутов BGP, такие как MED, локальный приоритет, значение маршрута и другие атрибуты.

3. Интеграция с протоколами динамической маршрутизации внутри сети (например, OSPF, RIP). Можно осуществлять автоматическую генерацию информации о маршрутизации BGP через перераспределение маршрутов из внутренних протоколов. Также можно вручную настраивать сети и агрегировать маршруты в BGP. При генерации маршрутов BGP можно использовать **route-map** для настройки их атрибутов.

4. Управление приоритетом маршрутов BGP. Можно использовать команду **distance** для настройки административной дистанции маршрутов BGP в системе.

46.7.1.2 Выбор пути

Процесс принятия решения BGP происходит на основе сравнения значений атрибутов маршрута. Если в одной сети имеется несколько маршрутов, BGP выбирает лучший маршрут к месту назначения. Далее описывается, как BGP выбирает лучший маршрут.

- Если маршрут не может дойти до следующего перехода, он не будет рассматриваться.
- Если путь внутренний, а синхронизация активирована, а также если маршрута нет в IGP, маршрут учитываться не будет.
- Выбирается маршрут с наивысшим приоритетом.

- Если у каждого маршрута одинаковый приоритет, предпочтительным считается маршрут с наивысшим локальным приоритетом.
- Если у каждого маршрута одинаковый локальный приоритет, выбирается маршрут, сгенерированный локальным маршрутизатором. Это может быть маршрут, созданный с помощью команды **network aggregate** или путем перераспределения маршрутов IGP.
- Если локальные приоритеты одинаковы или нет маршрутов, сгенерированных локальным маршрутизатором, то выбирается маршрут с кратчайшим AS-путем.
- Если длины AS-пути одинаковы, выбирается маршрут с наименьшим значением атрибута «origin» (IGP < EGP < INCOMPLETE).
- Если значения атрибута «origin» совпадают, выбирается маршрут с наименьшим значением MED. Если не активирована функция «bgp always-compare-med», это сравнение может быть выполнено только между маршрутами от одной и той же соседней AS.
- Если каждый маршрут имеет одно и то же значение MED, предпочтение отдается внешнему маршруту (EBGP) перед внутренним (IBGP). Внутри конфедерации автономной системы все маршруты считаются внутренними, но предпочтение отдается конфедерации EBGP, а не IBGP.
- Если у каждого маршрута одинаковые характеристики соединения, выбирается маршрут с меньшим идентификатором маршрутизатора (router-id).

46.7.2 Настройка BGP

Настройку BGP можно разделить на базовую и расширенную. Первые две задачи базовой настройки необходимы для работы BGP. Остальные, как и все задачи расширенной настройки, не являются обязательными.

Задачи базовой настройки

- Активация выбора маршрута BGP
- Настройка параметров соседнего устройства
- Мягкая перенастройка BGP
- Сброс соединения BGP
- Настройка синхронизации между BGP и IGP
- Настройка значения маршрута BGP
- Настройка фильтрации маршрутов BGP на основе соседа
- Настройка фильтрации маршрутов BGP на основе интерфейса
- Отключение обработки следующего перехода при обновлении BGP

Задачи расширенной настройки

- Использование карты маршрутов для фильтрации и изменения обновлений маршрутов
- Настройка агрегированных адресов
- Настройка атрибута сообщества BGP
- Настройка конфедерации автономной системы
- Настройка маршрутного рефлектора
- Отключение однорангового узла
- Настройка внешнего узла с несколькими переходами
- Настройка административной дистанции маршрутов BGP
- Настройка таймера BGP
- Сравнение MED маршрутов от разных AS.
- Настройка аутентификации MD5 для соседа BGP

46.7.2.1 Базовая настройка

1. Активация выбора маршрута BGP

Чтобы активировать выбор маршрута BGP, используйте следующие команды в режиме глобальной конфигурации:

Команда	Описание
router bgp *autonomous-system*	В режиме настройки маршрутизатора активирует процесс выбора маршрута BGP
network *network-number* | *masklen* [**route-map** *route-map-name*]	Помечает сеть как локальную автономную систему и добавляет ее в список BGP

В отличие от протоколов внутренней маршрутизации (например, RIP), где команда **network** определяет, куда отправлять обновления, в BGP эта команда используется для импорта маршрутов в таблицу BGP. Ограничение на использование команды **network** устанавливается ресурсами маршрутизатора, такими как выделенная оперативная память (RAM). При необходимости можно использовать команду **redistribute** для достижения того же эффекта.

2. Настройка параметров соседнего устройства

Настройка соседства BGP необходима для обмена данными о маршрутах с внешней сетевой средой. BGP поддерживает два вида соседей: внутренние (IBGP) и внешние (EBGP). Внутренние соседи находятся в одной AS, а внешние – в разных. Обычно внешние соседи

смежны и используют одну и ту же подсеть, в то время как внутренние могут находиться в любой части одной и той же AS.

Чтобы указать соседнее устройство BGP, выполните следующие команды:

Команда	Описание
neighbor {*ip-address* | *peer-group-name*} **remote-as** *number*	Определяет соседнее устройство

3. Мягкая перенастройка BGP

Обычно BGP-соседи обмениваются всеми доступными маршрутами при установлении соединения, а затем – только обновленными маршрутами. Если внесли изменения в настроенную политику маршрутизации, для применения этих изменений к полученным маршрутам необходимо очистить сессию BGP. Это может привести к нежелательному влиянию на работу сети, так как при очистке сессии происходит аннулирование кэша.

Во избежание необходимости очистки сессии предлагается использовать функцию мягкой перенастройки. Мягкая перенастройка позволяет настраивать и активировать политику маршрутизации без очистки сессии BGP. Она может быть применена как для входящих маршрутов, так и для исходящих маршрутов к соседям. При использовании мягкой перенастройки входящих маршрутов можно сделать новую политику маршрутизации активной без сброса сессии BGP. Для этого необходимо настроить BGP на сохранение всех принятых обновлений маршрутов.

С другой стороны, мягкая перенастройка исходящих маршрутов не требует дополнительного использования памяти и всегда эффективна. Вы можете запустить мягкую перенастройку исходящих маршрутов на стороне соседа, чтобы сделать новую локальную политику входящих маршрутов активной, без сброса сессии BGP. Мягкая перенастройка исходящих маршрутов не требует предварительной настройки.

Используйте следующую команду настройки маршрутизатора для активации мягкой перенастройки BGP:

Команда	Описание
neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]	Включает мягкую перенастройку BGP

Если вы используете параметр «peer-community-name» для обозначения однорангового комьюнити BGP, все его участники унаследуют функцию этой команды.

4. Сброс соединения BGP

Как только два маршрутизатора определены как соседи BGP, они создают соединение BGP и обмениваются информацией о маршрутизации. Если политика маршрутизации BGP была изменена или были изменены другие настройки, вам следует сбросить соединение BGP,

чтобы изменения вступили в силу. В режиме управления используйте одну из следующих команд для сброса соединения BGP:

Команда	Описание
clear ip bgp *	Перезапускает все сессии BGP на маршрутизаторе
clear ip bgp *address*	Перезапускает BGP-сессию с конкретным соседом, указанным по IP-адресу

5. Настройка синхронизации между BGP и IGP

Если вы разрешаете другой AS передавать данные в третью AS через вашу AS, то очень важна синхронизация между состоянием внутренней маршрутизации вашей AS и информацией о маршрутизации, которую она передает другим AS. Например, если ваш протокол BGP начинает передавать маршруты до того, как все маршрутизаторы в вашей AS узнают об этих маршрутах через внутренний протокол маршрутизации (IGP), то некоторые маршрутизаторы в вашей AS могут получить информацию о маршрутах, которые им неизвестны.

Чтобы избежать подобных ситуаций, BGP должен дождаться, пока все маршрутизаторы, работающие с IGP, узнают о новых маршрутах. Это называется синхронизацией между BGP и IGP, и эта синхронизация активирована по умолчанию.

Однако в некоторых ситуациях синхронизация не является необходимой. Например, если вы не разрешаете другим AS передавать данные через вашу AS, или если все маршрутизаторы в вашей AS используют BGP, вы можете отключить функцию синхронизации. Отключение этой функции позволит вам использовать меньше маршрутов в вашем IGP и обеспечит более быструю сходимость BGP.

Для отмены синхронизации используйте следующую команду:

Команда	Описание
no synchronization	Отменяет синхронизацию между BGP и IGP

При отмене синхронизации следует использовать команду **clear ip bgp**, чтобы очистить диалог BGP. Пример синхронизации BGP приведен в конце данного раздела.

Обычно не требуется перераспределять все маршруты в вашем внутреннем протоколе маршрутизации (IGP). Как правило перераспределяют один или два маршрута и обозначают их как внешние маршруты в вашем IGP или заставляют сеанс BGP генерировать AS-маршрут по умолчанию. Перераспределяются только маршруты, полученные через EBGP.

Вместо импорта вашего IGP в BGP используйте команду **network**, чтобы перечислить сети в вашей автономной системе. Эти сети называются локальными сетями и позволяют BGP иметь атрибут «origin» от IGP. Они должны присутствовать в основной таблице IP-маршрутизации и могут быть непосредственно подключенными маршрутами, статическими маршрутами или маршрутами, известными через IGP.

Будьте осторожны при перераспределении маршрутов между BGP и IGP, поскольку эти маршруты могут быть внедрены другими маршрутизаторами через BGP. Это может привести к ситуации, когда BGP внедряет информацию в IGP, а затем отправляет ее обратно в BGP. И наоборот.

6. Настройка значения маршрута BGP

Значение, или вес маршрута BGP – это номер, установленный для управления процессом выбора маршрута. Значение является локальным для маршрутизатора. Оно варьируется от 0 до 65535. Маршрут BGP, сгенерированный локально, имеет по умолчанию значение 32768, маршрут, полученный от соседа, имеет значение 0. Администратор может реализовать политику маршрутизации путем изменения значения маршрута.

В режиме настройки маршрутизатора используйте следующую команду для установки веса маршрута BGP:

Команда	Описание
neighbor {*ip-address* | *X:X::X:X* } **weight** *weight*	Назначает вес для каждого маршрута от одного соседа

Кроме того, вы можете изменить вес маршрута через карту маршрутизации при помощи команды **route-map**.

7. Настройка фильтрации маршрутов BGP на основе соседа

В реализации программного обеспечения маршрутизатора BGP существует 4 метода фильтрации маршрутов соседей:

Используйте фильтр на основе списка Aspath при помощи команды глобальной конфигурации **ip aspath-list** и команды **neighbour filter-list**.

Команда	Описание
ip as-path access-list *aspaths-list-name* {**permit** | **deny**} *as-regular-expression*	Определяет список доступа, относящийся к BGP
router bgp *autonomous-system*	Вход в режим настройки маршрутизатора
neighbor {*ip-address* | *X:X::X:X* } **filter-list** *aspath-list-name* {**in | out** }	Устанавливает фильтр BGP

Используйте один из ранее созданных списков доступа при помощи команды глобальной конфигурации **ip access-list** и команды **neighbour distribute-list**.

Команда	Описание
ip access-list standard *access-list-name*	Определяет список доступа, относящийся к BGP

router bgp *autonomous-system*	Вход в режим настройки маршрутизатора
neighbor {*ip-address* | *X:X::X:X*} **distribute-list** *access-list-name* {**in** | **out**}	Устанавливает фильтр BGP

Используйте фильтр на основе префиксов при помощи команды глобальной конфигурации **ip prefix-list** и команды **neighbour prefix-list**.

Команда	Описание
ip prefix-list *prefix-list-name* {**permit** | **deny**} A.B.C.D/n **ge** x **le** y	Определяет список префиксов
router bgp *autonomous-system*	Вход в режим настройки маршрутизатора
neighbor {*ip-address* | *X:X::X:X*} **prefix-list** *prefix-list-name* {**in** | **out**}	Устанавливает фильтр BGP

Используйте карту маршрутизации при помощи команды глобальной конфигурации **route-map** и команды **neighbour route-map**.

Использование карты не только фильтрует маршруты, но и изменяет их атрибуты. Более подробно эти настройки будут описаны в следующих разделах.

8. Настройка фильтрации маршрутов BGP на основе интерфейса

Настроить фильтрацию маршрутов BGP на основе интерфейса можно с помощью списка доступа и списка префиксов. Можно фильтровать сетевой номер и адрес шлюза маршрутов. Можно указать опцию «access-list» для использования списка доступа при фильтрации сетевого номера маршрутов, указать опцию «prefix-list» для использования списка префиксов при фильтрации сетевого номера маршрутов, указать опцию «gateway» для использования списка доступа при фильтрации атрибута «nexthop». Также можно фильтровать и сетевой номер, и атрибут «nexthop» маршрутов одновременно, но опцию «access-list» нельзя использовать вместе с опцией «prefix-list». Опция «*» может фильтровать маршруты на всех интерфейсах.

Чтобы настроить фильтрацию маршрутов BGP на основе интерфейса, необходимо в режиме настройки BGP выполнить следующие действия:

Команда	Описание
filter interface {**in** | **out**} (**access-list** *access-list-name*) (**prefix-list** *prefix-list-name*) (**gateway** *access-list-name*)	Фильтрует маршруты BGP на основе интерфейса

9. Отключение обработки следующего перехода при обновлении BGP

Вы можете настроить отключение обработки следующего перехода при обновлении соседнего BGP. Это может быть полезно в нешироковещательной сети (например, FR или

X.25). В сети FR или X.25 сосед BGP не может напрямую обращаться ко всем другим соседям в той же IP-подсети. Существует два способа отмены обработки nexthop:

- использование локального IP-адреса этого соединения BGP, чтобы заменить адрес следующего перехода исходящего маршрута;
- использование карты маршрутизации, чтобы указать адрес следующего перехода для входящих или исходящих маршрутов (см. описание расширенных настроек).

В режиме настройки маршрутизатора выполните следующую команду, чтобы отключить обработку следующего перехода и использовать локальный IP-адрес этого соединения BGP для замены адреса следующего перехода исходящих маршрутов:

Команда	Описание
neighbor {*ip-address* | *X:X::X:X*} **next-hop-self**	Отключает обработку следующего перехода при выполнении обновления BGP соседа

Данная команда позволяет настроить маршрутизатор так, чтобы он сообщал, что он является следующим узлом для определенного маршрута. Это значит, что другие соседи BGP будут пересылать пакеты к этой сети через текущий маршрутизатор. Такой подход полезен в средах, где не производится широковещательной передачи, так как между текущим маршрутизатором и указанным соседом существует путь. Однако в условиях широковещательной сети такая настройка может привести к ненужным дополнительным переходам между узлами.

46.7.2.2 Расширенная настройка

1. Использование карты маршрутов для фильтрации и изменения обновлений маршрутов.

Вы можете использовать карту маршрутов для фильтрации обновления маршрута и изменения атрибутов параметров в зависимости каждого соседа. Карта маршрутов может применяться как к входящему обновлению, так и к исходящему. При отправке или принятии обновления могут обрабатываться только маршруты, проходящие карту маршрутов.

Карта маршрутов поддерживает входящие и исходящие обновления в соответствии с атрибутами, такими как путь AS, сообщество и номер сети. Сопоставление в соответствии с путем AS требует использования команды **aspath-list**; сопоставление на основе комьюнити требует использования команды **community-list**, сопоставление на основе сети требует использования команды **ip access-list**.

В режиме настройки BGP используйте следующую команду, чтобы настроить карту маршрутизации для фильтрации и изменения обновления маршрутов:

Команда	Описание
neighbor {*ip-address* | *X:X::X:X*} **route-map** *route-map-name* {**in** | **out**}	Применение карты для входящих или исходящих маршрутов

2. Настройка агрегированных адресов

Для того чтобы уменьшить размер таблицы маршрутизации, использующейся в BGP, можно создавать агрегированные маршруты, которые объединяют несколько меньших маршрутов в один. Это можно сделать, либо путем перераспределения агрегированных маршрутов в BGP, либо с использованием условных атрибутов агрегации. Если в таблице маршрутизации BGP уже есть более детальные записи, то можно добавить в нее агрегированный адрес. Таким образом оптимизируется размер таблицы.

Для создание агрегированного адреса используйте следующие команды:

Команда	Описание
aggregate *network/len*	Создает агрегированный адрес в таблице маршрутизации BGP
aggregate *network/len* **summary-only**	Только общий адрес широковещательной рассылки
aggregate *network/len* **attribute-map** *map-name*	Генерирует агрегированный адрес в соответствии с условиями, указанными в карте маршрутизации

3. Настройка атрибута комьюнити BGP

Политика маршрутизации, поддерживаемая BGP, в основном базируется на одном из трех значений информации о маршрутизации:

- количество маршрутов сети;
- значение атрибута «as_path» маршрутов;
- значение атрибута «community» маршрутов.

Разделение маршрутов на сообщества посредством атрибута «community» и применение политики маршрутизации на основе комьюнити упрощает настройку управления информацией маршрутизации.

Комьюнити (сообщество) – группа маршрутов с общими атрибутами; каждый маршрут может принадлежать нескольким комьюнити. Администраторы AS могут определить, что определенный маршрут принадлежит определенному комьюнити.

Атрибут сообщества «community» – это необязательный и передаваемый глобальный атрибут в диапазоне от 1 до 4 294 967 200. В BGP существуют определенные комьюнити, которые предназначены для тегирования маршрутов и помогают в их управлении, используя различные подходы к объявлению маршрутов:

- **no-export** – не объявлять этот маршрут одноранговому узлу EBGP (включая одноранговые узлы EBGP внутри конфедерации автономной системы);
- **no-advertise** – не объявлять этот маршрут никому из одноранговых узлов;

- **local-as** – не объявлять этот маршрут за пределами автономной системы (можно отправить этот маршрут другим узлам суб-AS в конфедерации автономной системы).

При создании, принятии или отправке маршрутов узлы BGP могут настраивать, добавлять или изменять атрибут комьюнити маршрута. при агрегировании маршрутов сгенерированная агрегация включает совокупные атрибуты «community» из сообществ всех исходных маршрутов.

По умолчанию атрибуты «community» соседу не отправляются. Используйте следующую команду, чтобы указать отправку атрибута комьюнити соседу:

Команда	Описание
neighbor {*ip-address* | *X:X::X:X*} **send-community**	Активирует отправку соседу атрибута «community»

Чтобы настроить атрибут комьюнити для маршрутизатора, необходимо выполнить следующие действия:

Команда	Описание
route-map *map-name sequence-number* {**deny** | **permit**}	Настраивает карту маршрутизации
set community *community-value*	Устанавливает значение атрибута комьюнити
router bgp *autonomous-system*	Вход в режим настройки маршрутизатора
neighbor {*ip-address* | *X:X::X:X*} **route-map** *access-list-name* {**in** | **out**}	Применяет карту маршрутизации к входящим или исходящим маршрутам

Чтобы отфильтровать информацию о маршрутизации на основе атрибутов комьюнити, необходимо выполнить следующие действия:

Команда	Описание
ip community-list {**expanded** | **standard**} *community-list-name* {**permit** | **deny**} *community-expression*	Определяет список сообществ
route-map *map-name sequence-number* {**deny** | **permit**}	Настраивает карту маршрутизации
match community *community-list-name*	Настраивает правила сопоставления
router bgp *autonomous-system*	Вход в режим настройки маршрутизатора
neighbor {*ip-address* | *peer-group-name*} **route-map** *route-map-name* {**in** | **out**}	Применяет карту маршрутизации

4. Настройка конфедерации автономной системы

Способ уменьшить количество IBGP-соединений – разделить AS на несколько суб-AS, а затем сформировать из них конфедерацию. С внешней точки зрения конфедерация выглядит как AS. В конфедерации каждая суб-AS внутри является полносвязной и имеет соединения с другими суб-AS в той же конфедерации. Даже если между узлами разных суб-AS существуют сеансы EBGP, они все равно могут обмениваться информацией о выборе маршрутизации, как узлы IBGP, сохраняя информацию о следующем переходе, MED и локальном приоритете.

Чтобы настроить конфедерацию автономной системы BGP, необходимо указать идентификатор конфедерации. Идентификатор конфедерации – это номер AS. С внешней точки зрения конфедерация аналогична отдельной AS, где номер AS является идентификатором конфедерации.

Используйте следующую команду, чтобы настроить идентификатор конфедерации автономной системы:

Команда	Описание
bgp confederation identifier *autonomous-system*	Настраивает ID конфедерации

Чтобы обозначить номер автономной системы, принадлежащей конфедерации, используйте следующую команду:

Команда	Описание
bgp confederation peers *autonomous-system* [*autonomous-system ...*]	Указывает номер автономной системы, принадлежащей конфедерации

5. Настройка маршрутного рефлектора

Другой способ уменьшить количество соединений IBGP вместо настройки конфедерации автономной системы – настроить рефлектор, или отражатель маршрутов.

Внутренние узлы рефлектора маршрута делятся на две группы: клиентские узлы и все остальные маршрутизаторы (неклиентские узлы). Рефлектор отражает маршруты между двумя группами; он и его одноранговые клиентские узлы образуют кластер. Неклиентские одноранговые узлы обязаны быть подключенными к полносвязной сети, а клиентские – не обязаны. Клиенты в кластере не взаимодействуют с узлами IBGP за пределами кластера.

Когда рефлектор получает информацию о маршрутизации, он выполняет следующие задачи:

- трансляция маршрутов от внешнего узла BGP всем клиентским и неклиентским узлам;
- трансляция маршрутов от неклиентских узлов всем клиентам;
- трансляция маршрутов от клиентов всем клиентам и неклиентским узлам. Таким образом, клиентские узлы не обязательно должны быть подключены к полносвязной сети.

Используйте следующую команду, чтобы настроить локальный маршрутизатор как рефлектор и назначить соседей в качестве его клиентов:

Команда	Описание
neighbor {*ip-address* | *X:X::X:X*} **route-reflector-client**	Настраивает локальный маршрутизатор как рефлектор и назначает соседей в качестве его клиентов

Автономная система может иметь несколько маршрутных рефлекторов для более эффективной маршрутизации данных. Рефлекторы обрабатывают информацию о маршрутизации аналогично тому, как это делают спикеры IBGP. Обычно группа клиентов имеет только один рефлектор, и определяется его идентификатором (router ID). Для повышения надежности и предотвращения отказов одиночных узлов в сети, группа может иметь более одного маршрутного рефлектора. В этом случае каждый маршрутный рефлектор в группе должен быть настроен с 4-битным идентификатором кластера (cluster ID), чтобы однозначно идентифицировать информацию о маршрутах внутри этой группы. Все отражатели маршрутов, принадлежащие одному кластеру, должны быть полносвязными и иметь одинаковый набор клиентских и неклиентских одноранговых узлов.

Если в группе имеется более одного маршрутного отражателя, выполните следующую команду для настройки идентификатора кластера:

Команда	Описание
bgp cluster-id *cluster-id*	Настраивает идентификатор кластера

6. Отключение одноранговой узла

В режиме настройки BGP используйте следующую команду, чтобы отключить BGP-соседа:

Команда	Описание
neighbor {*ip-address* | *X:X::X:X*} **shutdown**	Завершает работу соседнего BGP

Используйте следующую команду, чтобы включить ранее отключенного BGP-соседа:

Команда	Описание
no neighbor {*ip-address* | *X:X::X:X*} **shutdown**	Активирует работу соседнего BGP

7. Настройка внешнего узла с несколькими переходами

По умолчанию внешние одноранговые узлы должны находиться в сети с прямым подключением. Когда прямое физическое соединение невозможно или нежелательно, для настройки внешнего узла с несколькими переходами необходимо выполнить следующую задачу:

Команда	Описание
neighbor {*ip-address* | *X:X::X:X*} **ebgp-multihop** ttl	Настройка внешнего узла с несколькими переходами в качестве BGP-соседа

8. Настройка административной дистанции маршрутов BGP

Административная дистанция, или расстояние управления – это метрика, используемая в сетевой инфраструктуре для определения надежности или предпочтительности разных протоколов маршрутизации. Меньшее значение этой метрики указывает на более предпочтительный или надежный маршрут. Этот параметр помогает при определении наилучшего маршрута для передачи данных в сложных сетевых конфигурациях с несколькими возможными маршрутами.

BGP использует три различных расстояния управления: внешнее, внутреннее и локальное. Маршрутам, полученным от внешнего BGP, будет назначено внешнее расстояние; маршруты, полученные из внутреннего BGP, будут иметь внутреннее расстояние, локальным маршрутам назначается локальное расстояние. Используйте следующую команду для настройки административной дистанции маршрутов BGP:

Команда	Описание
distance bgp {*external-distance*| *internal-distance* |*local-distance*}	Настраивает административную дистанцию

Изменение расстояний при настройке административной дистанции маршрута BGP опасно и обычно не рекомендуется. Внешнее расстояние должно быть короче, чем расстояние любого другого протокола динамической маршрутизации, а внутреннее расстояние должно быть длиннее, чем расстояние любого другого протокола динамической маршрутизации.

9. Настройка таймера BGP

Используйте следующую команду, чтобы настроить таймеры поддержки активности и времени удержания BGP для соседнего узла:

Команда	Описание
neighbor {*ip-address* | *X:X::X:X*} **timers** *keepalive holdtime*	Установка интервала таймера «поддержки активности» и «времени удержания» (отсчитывается в секундах) для назначенного узла или сообщества узлов

Используйте команду **no neighbour timers**, чтобы сбросить интервал таймера соседа или одноранговогo сообщества BGP до значения по умолчанию.

10. Сравнение MED маршрутов от разных AS

MED – это параметр, который следует учитывать при выборе наилучшего маршрута из нескольких путей. Предпочтительнее рассматривать маршрут с более низким значением MED, чем с более высоким.

По умолчанию в процессе выбора лучшего маршрута сравнение MED происходит только между маршрутами из одной и той же AS. Вы можете разрешить сравнение MED при выборе маршрутизации, независимо от того, из какой AS исходят маршруты. Для этого используйте следующую команду:

Команда	Описание
bgp always-compare-med	Позволяет выполнять сравнение MED между маршрутами из разных AS

11. Настройка аутентификации MD5 для соседа BGP

Чтобы обеспечить безопасную пересылку информации о маршрутизации между AS, выполните аутентификацию по паролю в соединении BGP с помощью опции MD5, предоставляемой TCP. Для этого выполните следующую команду:

Команда	Описание
neighbor *A.B.C.D* **password** *LINE*	Включает аутентификацию MD5 соседа BGP и устанавливает пароль

Вы можете запустить команду **no neighbor *A.B.C.D* password**, чтобы отменить аутентификацию MD5 для соседа BGP.

46.7.3 Мониторинг и поддержка BGP

Администратор может просмотреть или удалить таблицу маршрутизации BGP или содержимое других баз данных. Также может быть отображена подробная статистическая информация. Основные задачи следующие:

- удаление таблицы маршрутизации BGP и базы данных;
- отображение таблицы маршрутизации и информации о статистике системы;
- отслеживание информации BGP.

46.7.3.1 Удаление таблицы маршрутизации BGP и базы данных

Ниже перечислены задачи, связанные с быстрым удалением кэша, таблицы или базы данных BGP. Все команды, указанные в следующей таблице, выполняются в режиме EXEC.

Команда	Описание
clear ip bgp *	Удаляет все соединения BGP

clear ip bgp *as-number*	Удаляет соединения BGP назначенной автономной системы
clear ip bgp *address*	Удаляет соединения BGP назначенного соседа
clear ip bgp *address* soft {in | out}	Удаляет входящую или исходящую базу данных назначенного соседа
clear ip bgp *aggregates*	Удаляет маршруты, созданные в процессе агрегации
clear ip bgp *networks*	Удаляет маршруты, созданные в процессе пересылки
clear ip bgp *redistribute*	Удаляет маршруты, созданные командой **network**

46.7.3.2 Отображение таблицы маршрутизации и данных статистики

Приведенные ниже команды позволяют отобразить подробную статистическую информацию о таблице маршрутизации BGP или базе данных. Предоставленная информация может помочь в оценке использования ресурсов и в решении сетевых проблем. Также может быть отображена информация о достижимости узла.

Команда	Описание
show ip bgp	Отображает таблицу маршрутизации BGP в системе
show ip bgp prefix	Отображает маршруты, соответствующие указанному списку префиксов
show ip bgp community	Отображает статистическую информацию комьюнити
show ip bgp regexp *regular-expression*	Отображает маршруты, соответствующие указанному регулярному выражению
show ip bgp *network*	Отображает указанный маршрут BGP
show ip bgp neighbors *address*	Отображает информацию о соединениях TCP и BGP указанного соседа
show ip bgp neighbors [*address*] [**received-routes** | **routes** | **advertised-routes**]	Отображает маршруты, полученные от указанного соседа BGP
show ip bgp paths	Отображает информацию базы данных обо всех путях BGP
show ip bgp summary	Отображает состояния всех соединений BGP

46.7.3.3 Отслеживание информации BGP

Вы можете наблюдать за установлением соединения BGP и маршрутизацией передачи/приема, отслеживая информацию BGP. Это помогает выявлять неполадки и устранять проблемы. Команды для вывода отладочной информации BGP показаны в следующей таблице:

Команда	Описание
debug ip bgp	Отслеживает общую информацию BGP
debug ip bgp all	Отслеживает всю информацию BGP
debug ip bgp fsm	Отслеживает изменения состояний BGP
debug ip bgp keepalive	Отслеживает пакеты KeepAlive
debug ip bgp open	Отслеживает пакеты OPEN
debug ip bgp update	Отслеживает пакеты UPDATE

46.7.4 Примеры настройки BGP

46.7.4.1 Примеры использования карты маршрутов

В следующем примере показано, как использовать карту маршрутов для изменения атрибута входящего маршрута от соседа. Установите метрику всех маршрутов, приходящих от соседа 140.222.1.1 и соответствующих требованиям списка доступа ASPATH «aaa», равной 200; значение локального приоритета – 250. Такие маршруты будут приняты, все остальные – отклонены.

```
router bgp 100
 neighbor 140.222.1.1 route-map fix-weight in
 neighbor 140.222.1.1 remote-as 1
!
route-map fix-weight 10 permit
 match as-path aaa
 set local-preference 250
 set weight 200
!
ip as-path access-list aaa permit ^690$
ip as-path access-list aaa permit ^1800
```

В следующем примере первая запись карты маршрутов «freddy» установит метрику MED равной 127 для всех маршрутов, исходящих из автономной системы, у которых AS_PATH

начинается с 690. Вторая запись позволяет передавать маршруты, которые не соответствуют вышеуказанным условиям, соседу 1.1.1.1.

```
router bgp 100
 neighbor 1.1.1.1 route-map freddy out
!
ip as-path access-list abc permit ^690_
ip as-path access-list xyz permit .*
!
route-map freddy 10 permit
 match as-path abc
 set metric 127
!
route-map freddy 20 permit
 match as-path xyz
```

В следующем примере показано, как использовать **route-map** для изменения маршрутов при их перераспределении:

```
router bgp 100
 redistribute rip 1 route-map rip2bgp
!
route-map rip2bgp
 match ip address rip
 set local-preference 25
 set metric 127
 set weight 30000
 set ip next-hop 192.92.68.24
 set origin igp
!
ip access-list standard rip
 permit 131.108.0.0 255.255.0.0
 permit 160.89.0.0 255.255.0.0
```

```
permit 198.112.0.0 255.255.128.0
```

46.7.4.2 Пример конфигурации соседей

В следующем примере маршрутизатор BGP принадлежит AS109 и создает две сети. У данного роутера 3 соседа: первый сосед внешний (в разных AS); второй – внутренний (с тем же номером AS). Третий – тоже внешний.

```
router bgp 109
 network 131.108.0.0
 network 192.31.7.0
 neighbor 131.108.200.1 remote-as 167
 neighbor 131.108.234.2 remote-as 109
 neighbor 150.136.64.19 remote-as 99
```

46.7.4.3 Пример фильтрации маршрутов BGP на основе соседей

Маршруты, проходящие через AS_PATH, указанный в списке доступа «test1», будут иметь значение метрики 100. Только маршруты, проходящие через AS_PATH, указанный в списке доступа «test2», будут отправлены по направлению к 193.1.12.10, и аналогично, только те маршруты, которые проходят через список доступа «test3», будут приняты от 193.1.12.10:

```
router bgp 200
 neighbor 193.1.12.10 remote-as 100
 neighbor 193.1.12.10 filter-list test1 in weight 100
 neighbor 193.1.12.10 filter-list test2 out
 neighbor 193.1.12.10 filter-list test3 in
!
ip as-path access-list test1 permit ^109_
ip as-path access-list test2 permit ^200$
ip as-path access-list test2 permit ^100$
ip as-path access-list test3 deny ^690$
ip as-path access-list test3 permit .*
```

46.7.4.4 Примеры фильтрации маршрутов BGP на основе интерфейса

Ниже приведен пример настройки фильтрации маршрутов на основе интерфейса. В данной конфигурации фильтруются маршруты, проходящие через интерфейс vlan1 при помощи списка доступа «acl»:

```
router bgp 122
 filter vlan1 in access-list acl
```

В следующем примере используется список доступа «filter-network» для фильтрации сетевых номеров маршрутов, а также используется список доступа «filter-gateway» для фильтрации адресов шлюзов маршрутов, проходящих через интерфейс vlan1.

```
router bgp 100
 filter vlan1 in access-list filter-network gateway filter-gateway
```

В следующем примере используется список префиксов «filter-prefix» для фильтрации сетевых номеров маршрутов. Одновременно применяется список доступа «filter-gateway» для фильтрации адресов шлюзов маршрутов, проходящих через все интерфейсы.

```
router bgp 100
 filter * in prefix-list filter-prefix gateway filter-gateway
```

46.7.4.5 Примеры использования списка префиксов для настройки фильтрации маршрутов

В следующем примере маршрут по умолчанию 0.0.0.0/0 запрещен.

```
ip prefix-list abc deny 0.0.0.0/0
```

В следующем примере BGP разрешает маршруты, соответствующие префиксу 35.0.0.0/8:

```
ip prefix-list abc permit 35.0.0.0/8
```

В следующем примере процесс BGP принимает только префиксы длиной от /8 до /24:

```
router bgp 1
 network 101.20.20.0
 filter * in prefix max24
!
```

```
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
!
```

В следующей конфигурации маршрутизатор фильтрует маршруты со всех интерфейсов, принимая только маршруты с префиксом от 8 до 24:

```
router bgp 12
 filter * in prefix-list max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
!
```

В следующем примере BGP разрешает маршруты с длиной префикса не более 24 в сети 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

В следующем примере BGP запрещает маршруты с длиной префикса более 25 в сети 192/8:

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

В следующем примере BGP разрешает маршруты с длиной префикса более 8, но менее 24 во всем адресном пространстве:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

В следующем примере BGP запрещает все маршруты с длиной префикса более 25 во всем адресном пространстве:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

В этом примере запрещены маршруты из сети 10/8, поскольку если маска в сети класса A 10.0.0.0/8 меньше или равна 32 битам, все маршруты из этой сети будут запрещены:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

В следующем примере BGP запрещает маршруты с длиной маски более 25 в сети 204.70.1.24:

```
ip prefix-list abc deny 204.70.1.0/24 ge 25
```

В следующем примере BGP разрешает все маршруты:

```
ip prefix-list abc permit any
```

46.7.4.6 Пример агрегации маршрутов BGP

Пример ниже иллюстрирует, как создавать агрегированные маршруты в BGP. Это можно сделать путем перераспределения маршрутов или с использованием условной функции агрегации маршрутов.

В следующем примере команда «redistribute static» используется для перераспределения агрегированного маршрута 193.*.*.*:

```
ip route 193.0.0.0 255.0.0.0 null 0
!
router bgp 100
 redistribute static
```

Если в таблице маршрутизации есть хотя бы один маршрут в пределах назначенного диапазона, следующая конфигурация создаст маршрут агрегации в таблице маршрутизации BGP. Маршрут агрегации будет считаться исходящим от вашей AS и иметь атрибут «atomic», чтобы указать на возможность потери информации.

```
router bgp 100
 aggregate 193.0.0.0/8
```

В следующем примере создается агрегированный маршрут 193...* и запрещается передавать более конкретные маршруты всем соседям:

```
router bgp 100
 aggregate 193.0.0.0/8 summary-only
```

46.7.4.7 Пример настройки маршрутного рефлектора

Ниже приведен пример конфигурации отражателя маршрута. RTA, RTB, RTC, RTE принадлежат одной автономной системе AS200, RTA служит рефлектором, RTB и RTC являются его клиентами, а RTE – обычным соседом IBGP. RTD принадлежит AS100 и создает соединение EBGP с RTA. Конфигурация показана на рисунке 46-4:

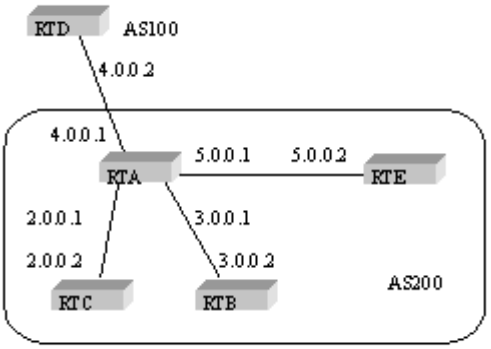

Рисунок 46-4 – Топология сети BGP

Настройка RTA:

```
interface vlan2
ip address 2.0.0.1 255.0.0.0
!
interface vlan3
ip address 3.0.0.1 255.0.0.0
!
interface vlan4
ip address 4.0.0.1 255.0.0.0
!
interface vlan5
ip address 5.0.0.1 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200   /*RTC IBGP*/
neighbor 2.0.0.1 route-reflector-client
neighbor 3.0.0.1 remote-as 200   /*RTB IBGP*/
neighbor 3.0.0.1 route-reflector-client
neighbor 5.0.0.1 remote-as 200   /*RTE IBGP*/
neighbor 4.0.0.2 remote-as 100   /*RTD EBGP*/
network 11.0.0.0/8
```

```
!
ip route 11.0.0.0 255.0.0.0 2.0.0.12
```

Настройка RTB:

```
interface vlan3
ip address 3.0.0.2 255.0.0.0
!
router bgp 200
neighbor 3.0.0.1 remote-as 200   /*RTA IBGP*/
network 13.0.0.0/8
!
ip route 13.0.0.0 255.0.0.0 3.0.0.12
```

Настройка RTC:

```
interface vlan2
ip address 2.0.0.2 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200   /*RTA IBGP*/
network 12.0.0.0/8
!
ip route 12.0.0.0 255.0.0.0 2.0.0.12
```

Настройка RTD:

```
interface vlan4
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200   /*RTA EBGP*/
network 14.0.0.0/8
```

```
!
ip route 14.0.0.0 255.0.0.0 4.0.0.12
```

Настройка RTE:

```
interface vlan5
ip address 5.0.0.2 255.0.0.0
!
router bgp 200
neighbor 5.0.0.1 remote-as 200   /*RTA IBGP*/
network 15.0.0.0/8
!
ip route 15.0.0.0 255.0.0.0 5.0.0.12
```

46.7.4.8 Пример конфедерации BGP

Ниже приведена конфигурация конфедерации. RTA, RTB, RTC создают соединения IBGP и принадлежат частной автономной системе 65010; RTE принадлежит другой частной автономной системе 65020; RTE и RTA устанавливают внутреннее EBGP-соединение конфедерации; AS65010 и AS65020 составляют конфедерацию, идентификатор которой – AS200; RTD принадлежит автономной системе AS100, RTD устанавливает соединение EBGP с автономной системой 200 через RTA.

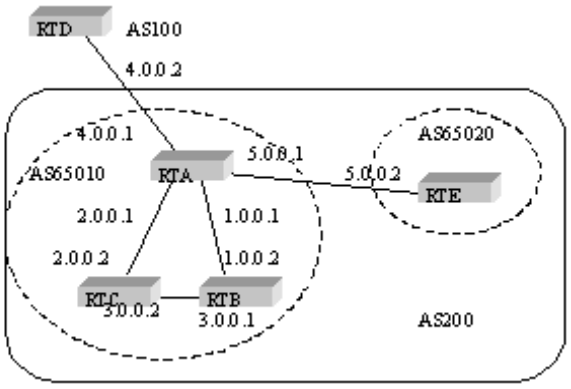

Рисунок 46-5 – Конфедерация BGP

Настройка RTA:

```
interface vlan1
ip address 1.0.0.1 255.0.0.0
!
interface vlan2
ip address 2.0.0.1 255.0.0.0
!
interface vlan4
ip address 4.0.0.1 255.0.0.0
!
interface vlan5
ip address 5.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.2 remote-as 65010  /*RTB IBGP*/
neighbor 2.0.0.2 remote-as 65010  /*RTC IBGP*/
neighbor 5.0.0.2 remote-as 65020  /*RTE EBGP*/
neighbor 4.0.0.2 remote-as 100    /*RTD EBGP*/
```

Настройка RTB:

```
interface vlan1
ip address 1.0.0.2 255.0.0.0
!
interface vlan3
ip address 3.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.1 remote-as 65010  /*RTA IBGP*/
```

```
neighbor 3.0.0.2 remote-as 65010  /*RTC IBGP*/
```

Настройка RTC:

```
interface vlan2
ip address 2.0.0.2 255.0.0.0
!
interface vlan3
ip address 3.0.0.2 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 2.0.0.1 remote-as 65010  /*RTA IBGP*/
neighbor 3.0.0.1 remote-as 65010  /*RTB IBGP*/
```

Настройка RTD:

```
interface vlan4
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200  /*RTA EBGP*/
```

Настройка RTE:

```
interface vlan5
ip address 5.0.0.2 255.0.0.0
!
router bgp 65020
bgp confederation identifier 200
bgp confederation peers 65010
neighbor 5.0.0.1 remote-as 65010  /*RTA EBGP*/
```

46.7.4.9 Пример карты маршрутов с атрибутом группы BGP

В этом разделе приведены три примера использования карты маршрутов с атрибутом комьюнити BGP.

В первом примере настройка «route-map set-community» применяется к исходящему обновлению соседа 171.69.232.50. Установите специальный атрибут «community» со значением «no-export» для маршрутов, проходящих через список доступа «aaa», в то время как другие маршруты будут транслироваться обычным образом. Этот специальный атрибут комьюнити автоматически не позволит узлам BGP в AS200 объявлять маршрут за пределами своей автономной системы.

```
router bgp 100
 neighbor 171.69.232.50 remote-as 200
 neighbor 171.69.232.50 send-community
 neighbor 171.69.232.50 route-map set-community out
!
 route-map set-community 10 permit
 match ip address aaa
 set community no-export
!
 route-map set-community 20 permit
```

Во втором примере «route-map set-community» используется для выходного обновления соседа 171.69.232.90. Все маршруты, исходящие из AS70, будут добавлять значение 200 в атрибут сообщества 200, все остальные маршруты будут объявляться обычным образом.

```
route-map bgp 200
 neighbor 171.69.232.90 remote-as 100
 neighbor 171.69.232.90 send-community
 neighbor 171.69.232.90 route-map set-community out
!
route-map set-community 10 permit
 match as-path test1
```

```
 set community-additive 200 200
!
route-map set-community 20 permit
 match as-path test2
!
ip as-path access-list test1 permit 70$
ip as-path access-list test2 permit .*
```

В третьем примере выборочно установите MED и значение локального приоритета маршрутов от соседа 171.69.232.55 в соответствии со значением атрибута сообщества маршрутов. Всем маршрутизаторам, соответствующим списку com1, будет присвоен номер MED 8000, это может включать маршруты со значением комьюнити «100 200 300» или «900 901». Эти маршруты могут иметь другие значения атрибутов.

Для всех маршрутов, соответствующих списку com2, будет установлено значение локального приоритета 500.

Всем остальным маршрутам будет присвоено значение локального приоритета 50. Таким образом, все остальные маршруты соседа 171.69.232.55 будут иметь приоритет 50.

```
router bgp 200
 neighbor 171.69.232.55 remote-as 100
 neighbor 171.69.232.55 route-map filter-on-community in
!
route-map filter-on-community 10 permit
 match community com1
 set metric 8000
!
route-map filter-on-community 20 permit
 match community com2
 set local-preference 500
!
route-map filter-on-community 30 permit
 set local-preference 50
!
```

```
ip community-list standard com1 permit 100 200 300
ip community-list standard com1 permit 900 901
!
ip community-list standard com2 permit 88
ip community-list standard com2 permit 90
!
```

46.8 PBR

46.8.1 Обзор

PBR (Policy Based Routing) – это сокращение от «маршрутизация на основе политик». PBR дает пользователю возможность маршрутизировать IP-пакеты в соответствии с какой-либо политикой, отличной от протокола динамической маршрутизации. В настоящее время поддерживаются политики на основе длины IP-пакета и на основе IP-адреса источника. Вы можете установить шлюз или исходный интерфейс для пакетов, соответствующих политике. PBR может поддерживать балансировку нагрузки.

Правила выбора следующего перехода у PBR следующие:

- Если настроен параметр **set ip next-hop** и шлюз доступен, будет использоваться шлюз. Если настроено несколько шлюзов, используется первый доступный шлюз. Если используется ключевое слово **load-balance**, между этими шлюзами применяется балансировка нагрузки.
- Если настроен параметр **set interface**, а исходящий интерфейс является маршрутизируемым (протокол интерфейса включен и IP-адрес настроен), используется исходящий интерфейс. Если настроено несколько исходящих интерфейсов, будет использоваться первый маршрутизируемый интерфейс. Если используется ключевое слово **load-balance**, между этими интерфейсами применяется балансировка нагрузки. Если настроены и **set ip next-hop**, и **set interface**, сначала используется **set ip next-hop**.
- **set ip default next-hop** или **set default interface** не будут использоваться до тех пор, пока поиск маршрутизации не завершится неудачей.

В следующих случаях политика маршрутизации не применяется:

- если адрес назначения пакета является локальным;
- если пакет является многоадресным сообщением;
- если пакет является локальным прямым широковещательным пакетом.

46.8.2 Настройка PBR

Задачи настройки

- Создание стандартного списка доступа (опционально)
- Создание карты маршрутизации
- Применение карты маршрутизации на интерфейсе

46.8.2.1 Создание стандартного списка доступа

Для создания списка доступа выполните следующую команду:

Команда	Описание
ip access-list standard net1	Создает стандартный список доступа с именем «net1»

46.8.2.2 Создание карты маршрутизации

Карта маршрутизации определяет набор критериев совпадения и действий, которые будут применены к пакетам трафика, соответствующим этим критериям. Для создания карты маршрутизации выполните следующие команды:

Команда	Описание
route-map pbr	Вход в режим настройки карты маршрутизации
match ip address *access-list* **match length** *min_length max_length*	Настраивает политику сопоставления
set ip [**default**] **next-hop** *A.B.C.D* **set** [**default**] **interface** *interface_name*	Настраивает адрес или порт следующего перехода IP-пакета

46.8.2.3 Применение карты маршрутизации на интерфейсе

Чтобы включить PBR на интерфейсе, выполните следующие действия:

Команда	Описание
interface *interface_name*	Вход в режим настройки интерфейса
ip policy route-map *route-map_name*	Применяет PBR к интерфейсу

46.8.2.4 Мониторинг и поддержка PBR

Для отображения информации о работе PBR выполните следующую команду:

Команда	Описание
debug ip policy	Отображает результаты применения политики маршрутизации

46.8.3 Пример настройки PBR

Настройка коммутатора:

```
!
interface Vlan1
ip address 10.1.1.3 255.255.255.0
no ip directed-broadcast
ip policy route-map pbr
!
interface Vlan2
ip address 13.1.1.3 255.255.255.0
no ip directed-broadcast
!
interface Vlan3
ip address 14.1.1.3 255.255.255.0
no ip directed-broadcast
!
ip access-list standard net1
permit 10.1.1.2 255.255.255.255
!
ip access-list standard net2
permit 10.1.1.4 255.255.255.255
!
ip access-list standard net3
permit 10.1.1.21 255.255.255.255
!
route-map pbr 10 permit
match ip address net1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
```

```
match ip address net2
set ip next-hop 14.1.1.99
!
route-map pbr 30 permit
match ip address net3
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
!
route-map pbr 40 permit
set ip default next-hop 13.1.1.99
```

Политика маршрутизации включена на интерфейсе vlan1. Для пакетов, исходящих от 10.1.1.2, следующим переходом является 13.1.1.99, если 13.1.1.99 доступен. Если 13.1.1.99 недоступен, используется базовая маршрутизация. Для пакетов от 10.1.1.21 используется карта маршрутизации pbr 30. Поскольку применено ключевое слово «load-balance», в качестве следующего перехода будут использоваться как 13.1.1.99, так и 14.1.1.99 (при условии, что в таблице маршрутизации есть маршруты к 13.1.1.99 и 14.1.1.99).

46.9 Настройка высокого приоритета протокола маршрутизации коммутатора

При тестировании маршрутизирующих протоколов можно улучшить приоритет обработки пакетов протокола на центральном процессоре с помощью механизма FP (Fast Path). Это позволяет гарантировать, что пакеты протокола маршрутизации могут быть обработаны, даже если система перегружена фоновым трафиком (например, IP-пакеты, которые должны быть перенаправлены). Выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
switch routing-protocol-highpriority	Включает повышение приоритета пересылки пакетов маршрутизации на ЦП

47. Маршрутизация IP-подсетей на аппаратном уровне

47.1 Введение

Механизм маршрутизации IP-подсетей на аппаратном уровне аналогичен быстрой обработке пакетов IP Fast Exchange.

Когда данная функция выключена, перед пересылкой сообщения, содержащего IP-адрес A, к следующему узлу, коммутатор сначала проверяет, существует ли запись с адресом A в аппаратном кэше IP. Если запись существует, сообщение будет пересылаться через аппаратное обеспечение. Если запись не существует, сообщение отправляется в ЦПУ и обрабатывается программным обеспечением.

Элементы IP-маршрутизации в оборудовании включают в себя подсеть назначения, маску, IP-адрес следующего узла, интерфейс и так далее. Когда включена маршрутизация IP-подсетей на аппаратном уровне, после неудачного сопоставления в кэше IP, система проверяет элементы подсетевой маршрутизации в оборудовании. Если совпадающий элемент найден, сообщение направляется напрямую через IP-адрес следующего узла и интерфейс, указанные в найденном элементе. Если элемент подсетевой маршрутизации в оборудовании не найден, сообщение отправляется в CPU для обработки.

47.2 Настройка маршрутизации IP-подсетей на аппаратном уровне

Для настройки функции выполните следующие команды:

Команда	Описание
[**no**] **ip exf**	Включает или отключает аппаратную маршрутизацию
[**no**] **ip exf down-up-threshold** *rate*	Устанавливает пороговое значение для маршрутов, обрабатываемых программным обеспечением (в процентах). Значение по умолчанию – 90

47.3 Пример настройки

Во время настройки маршрутов следует обратить внимание на следующие моменты:

- При прямом подключении (direct-connecting routing), следующим переходом является ЦПУ. Если следующий переход – это интерфейс маршрутизации, а не IP-адрес, то настраивайте как в случае прямого подключения.
- Если ARP-запись для IP-адреса следующего перехода отсутствует, система отправит ARP-запрос и временно укажет следующий маршрут как ЦПУ. После получения ARP-ответа система обновит переход на указанный пользователем IP-адрес. Если интерфейс VLAN, на котором находится следующий переход, отличается от настроенного интерфейса во время ARP-ответа, следующий переход маршрута будет указан как ЦПУ. Пользователю следует исправить конфигурацию.
- Если интерфейс следующего перехода или протокол интерфейса не существуют, запись не будет добавлена в таблицу маршрутизации на аппаратном уровне.

Предположим, что коммутатор настроен при помощи следующей команды:

ip exf down-up-threshold 80

Данная команда указывает, что, когда количество маршрутов, обрабатываемых программным обеспечением, превысит 80% верхнего предела маршрутов на аппаратном уровне, коммутатор автоматически отключит функцию аппаратной маршрутизации. Когда количество маршрутов, обрабатываемых программным обеспечением, снизится до значения меньше 80% верхнего предела маршрутов на аппаратном уровне, функция аппаратной маршрутизации подсетей снова будет включена.

48. IP-PBR

48.1 Введение

IP-PBR реализует функции программного обеспечения PBR посредством аппаратного обеспечения микросхемы коммутатора.

PBR означает маршрутизацию на основе политик. Это позволяет пользователям полагаться на определенную политику, а не на протокол маршрутизации. Программное обеспечение PBR поддерживает несколько политик и правил, а также балансировку нагрузки. Вы можете назначить IP-адрес или порт следующего перехода для тех пакетов, которые соответствуют политике. PBR поддерживает балансировку нагрузки и применяет несколько IP-адресов или портов следующего перехода к пакетам, поддерживаемым политикой.

IP-PBR позволяет определить специальные правила, по которым пакеты могут быть перенаправлены на конкретный выходной интерфейс или следующий переход на основе определенных условий. Важным аспектом является наличие ARP-записи для указанного следующего перехода, так как благодаря ей IP-PBR считает этот переход действительным и применяет соответствующее правило. Когда пакет соответствует условиям IP-PBR, коммутатор аппаратно непосредственно перенаправляет этот пакет на указанный следующий переход, обеспечивая высокую производительность без нагрузки на ЦПУ. Пакеты, перенаправляемые с использованием IP-PBR, имеют наивысший приоритет, и только неподходящие под правила IP-PBR пакеты направляются на ЦПУ.

IP-PBR поддерживает политики на основе списка контроля доступа по IP (IP ACL) и политики с использованием следующего IP-адреса. При наличии нескольких следующих переходов, будет выбран первый активный переход. IP-PBR также поддерживает аппаратную эквивалентную маршрутизацию, которая реализуется через микросхему коммутатора. Для использования аппаратной эквивалентной маршрутизации не требуется дополнительной настройки.

IP-PBR поддерживает следующие команды маршрутизации на основе политики:

route-map *WORD*

match ip address *WORD*

set ip next-hop *X.X.X.X* [**load-balance**]

ip policy route-map *WORD*

Механизм IP-PBR несколько отличается от механизма маршрутизации с использованием политик на маршрутизаторе.

IP-PBR выбирает эффективный следующий узел (выход) и отбрасывает пакеты, если нет допустимого следующего узла. В то время как маршрутизация с использованием политик на маршрутизаторе также выбирает эффективный следующий узел, но возможна потеря пакетов, если этот следующий узел не имеет информации ARP.

Когда установлены несколько последовательностей, одно из различий между IP-PBR и программной маршрутизацией с использованием политик заключается в том, что последняя всегда выбирает маршруты с более высоким приоритетом, независимо от того, перекрываются ли IP-адреса, соответствующие высокоприоритетным и низкоприоритетным последовательностям, и действительны ли эти маршруты. В то время как IP-PBR выбирает маршруты с низким приоритетом, когда маршруты с высоким приоритетом становятся недействительными.

48.2 Настройка IP-PBR

48.2.1 Глобальное включение или отключение IP-PBR

Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
ip pbr	Включает IP-PBR
no ip pbr	Восстанавливает настройки по умолчанию

По умолчанию функция IP-PBR отключена.

48.2.2 Создание списка доступа

Для создания ACL выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
ip access-list standard *net1*	Вход в режим настройки ACL и создание стандартного списка с именем «net1»

48.2.3 Создание карты маршрутизации

Для создания карты маршрутизации выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание

route-map *pbr*	Вход в режим настройки карты маршрутизации
match ip address *access-list*	Настраивает политику сопоставления
set ip next-hop *A.B.C.D*	Настраивает адрес следующего перехода IP-пакета

48.2.4 Применение политики на интерфейсе

Чтобы применить политику маршрутизации к порту приема IP-пакетов, выполните следующие команды:

Команда	Описание
interface *interface_name*	Вход в режим настройки интерфейса
ip policy route-map *route-map_name*	Применяет политику маршрутизации к порту

48.3 Мониторинг и поддержка IP-PBR

Выполните следующие команды в режиме управления:

Команда	Описание
show ip pbr	Отображает информацию о конфигурации и состоянии IP-PBR
show ip pbr policy	Отображает информацию о политике маршрутизации IP-PBR
show ip pbr exf	Отображает информацию об эквивалентной маршрутизации IP-PBR
debug ip pbr	Включает или отключает отладочную информацию IP-PBR

Отображение информации о том, что IP-PBR не запущен:

```
switch#show ip pbr

IP policy based route state: disabled


No pbr apply item

No equiv exf apply item
```

Отображение данных, относящихся к работе IP-PBR:

```
switch#show ip pbr
IP policy based route state: enabled

No equiv exf apply item

VLAN3 use route-map ddd, and has 1 entry active.
-----------------
Entry sequence 10, permit
  Match ip access-list:
    ac1
  Set Outgoing nexthop
    90.0.0.3
```

Отображение информации о политике маршрутизации IP-PBR:

```
switch#show ip pbr policy
IP policy based route state: enabled

VLAN3 use route-map ddd, and has 1 entry active.
-----------------
Entry sequence 10, permit
  Match ip access-list:
    ac1
  Set Outgoing nexthop
    90.0.0.3
```

Отображение информации об эквивалентной маршрутизации:

```
switch#show ip pbr exf
IP policy based route state: enabled

Equiv EXF has 1 entry active.
-----------------
Entry sequence 1, handle c1f95b0
  Dest ip: 1.1.0.0/16
    90.0.0.3
    192.168.213.161
```

48.4 Пример настройки IP-PBR

Настройка на коммутаторе:

```
!
ip pbr
!
interface vlan1
ip address 10.1.1.3 255.255.255.0
```

```
no ip directed-broadcast
ip policy route-map pbr
!
ip access-list standard ac1
permit 10.1.1.21 255.255.255.255
!
ip access-list standard ac2
permit 10.1.1.2 255.255.255.255
!
route-map pbr 10 permit
match ip address ac1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
match ip address ac2
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
!
```

Описание конфигурации

Коммутатор должен применять политику маршрутизации к пакетам, полученным из VLAN1. Что касается пакетов, чьи исходные IP-адреса равны 10.1.1.21, их следующий переход – 13.1.1.99. Пакеты, исходные IP-адреса которых равны 10.1.1.2, применяются к карте маршрутов pbr 20. Поскольку **set ip next-hop** имеет параметр **load-balance**, микросхема коммутатора автоматически выберет 13.1.1.99 или 14.1.1.99 в качестве выхода в соответствии с IP-адресом назначения.

49. Multi-VRF CE

49.1 Введение

Виртуальная частная сеть (VPN) обеспечивает безопасный метод для нескольких клиентских сетей совместно использовать полосу пропускания, предоставляемую интернет-провайдером (ISP). Как правило, одна VPN объединяет несколько клиентских сетей, которые разделяют общую таблицу маршрутизации на маршрутизаторах ISP. Каждая клиентская сеть подключается к интерфейсу устройства ISP, и устройство ISP связывает

каждый интерфейс с таблицей маршрутизации VPN. Такая таблица называется VRF (VPN Routing/Forwarding table).

VRF обычно развертывается на граничном устройстве провайдера (PE), как MPLS VRF VPN. PE поддерживает несколько VPN, и каждый VPN имеет своё независимое пространство IP-адресов, которые могут перекрываться. VPN разных клиентов подключаются к разным интерфейсам PE, и PE различает таблицы маршрутизации на основе входного порта пакета.

Multi-VRF CE устраняет необходимость в подключении нескольких клиентских сетей с PE к клиентскому граничному узлу CE и требует только физическое соединение CE и PE. Таким образом, экономятся ресурсы портов на PE. CE также поддерживает таблицу маршрутизации VRF для каждой VPN. Пакеты из клиентской сети сначала пересылаются на CE, а затем передаются на PE после прохождения через сеть ISP.

Коммутатор, который служит MCE, соединяет разные клиентские сети через разные порты, а затем связывает эти порты с таблицей маршрутизации VPN. Коммутатор поддерживает настройки VRF только на порту VLAN.

MCE обычно развертывается на границе крупномасштабной VPN-сети MPLS-VRF. Три функции: Multi-VRF CE, переключение меток MPLS и функция уровня управления MPLS – независимы. На рисунке 49-1 показана VPN-сеть MPLS-VRF.

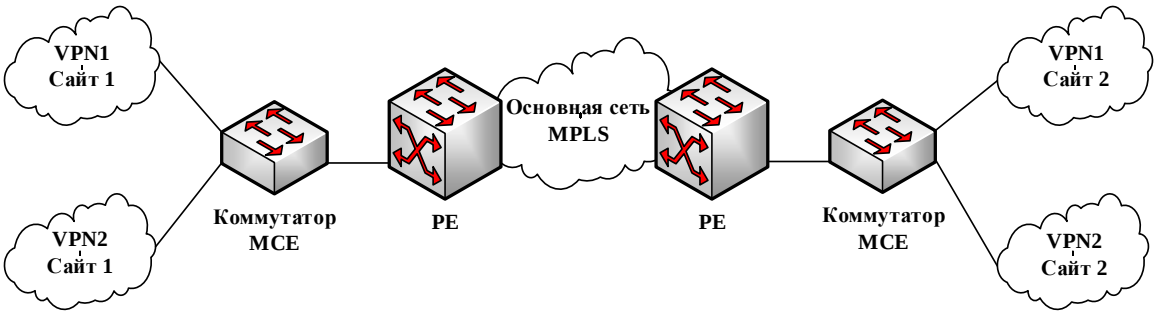

Рисунок 49-1 – MCE в сети VPN MPLS-VRF

49.1.1 Создание маршрутов с CE

Коммутатор CE Multi-VRF может создавать маршруты через CE, используя несколько протоколов динамической маршрутизации. CE могут быть маршрутизаторами или коммутаторами Ethernet. Поддерживаемые протоколы маршрутизации включают OSPF, RIP и BEIGRP. Коммутатор MCE также поддерживает настройку статической маршрутизации.

Коммутатору MCE обычно нужны разные порты VLAN для подключения CE, принадлежащих разным VPN. Порты VLAN, используемые для подключения VPN, должны быть связаны с VRF. CE не обязательно должен поддерживать VRF.

49.1.2 Создание маршрутов с PE

Коммутатор MCE может подключать один или несколько PE, но как MCE, так и подключенные PE должны иметь настроенные VRF. MCE предоставит PE маршруты, которые он узнает от CE, а также узнает маршруты удаленных клиентских сетей от PE.

Маршрут VRF может быть установлен между MCE и PE с помощью протоколов динамической маршрутизации, таких как BGP, OSPF, RIP и BEIGRP. Также, маршрут VRF может быть установлен статически.

Обычно MCE и PE принадлежат разным автономным системам. Следовательно, метод установления маршрута VRF между MCE и PE с помощью EBGP является ключевым.

49.2 Настройка Multi-VRF CE

49.2.1 Настройка VRF по умолчанию

Функция	Настройки по умолчанию
VRF	Конфигурации нет. Все маршруты добавляются в таблицу маршрутизации по умолчанию
VPN-расширяемость VRF	Идентификация RD отсутствует. Цели маршрутизации ввода/вывода (RT) не существует
Максимальное количество маршрутов VRF	10240
VRF-порт	Н/Д. Ни один из портов VLAN не связан с VRF, а маршруты портов добавляются в таблицу маршрутизации по умолчанию
IP экспресс-пересылка	Аппаратная IP-маршрутизация не включена

49.2.2 Настройка MCE

Задачи настройки

- Настройка VRF
- Настройка VPN-маршрута
- Настройка маршрута BGP между PE и CE
- Проверка соединения VRF между PE и CE

49.2.2.1 Настройка VRF

Для настройки одного или нескольких экземпляров VRF выполните следующие команды:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации
Switch_config# **ip vrf** *vrf-name*	Создает VRF и входит в режим настройки VRF. *vrf-name*: имя VRF длиной до 31 символа
Switch_config_vrf# **rd** *route-distinguisher*	Устанавливает отличительный признак маршрута VRF. *route-distinguisher*: обозначает отличительный признак маршрута. Он состоит из ID домена AS и случайных чисел или IP и случайных чисел
Switch_config_vrf# **route-target** {**export** | **import** | **both**} *route-target-extened-community*	Создает расширенные атрибуты VPN для объектов VRF ввода/вывода. *route-target-extended-community*: состоит из ID домена AS и случайных чисел или IP и случайных чисел
Switch_config_vrf# **exit**	Выход из режима настройки VRF
Switch_config# **interface** *intf-name*	Вход в режим настройки интерфейса. *intf-name*: обозначает имя интерфейса
Switch_config_intf# **ip vrf forwarding** *vrf-name*	Связывает интерфейс L3 с VRF. *vrf -name*: означает имя VRF
Switch_config_intf# **exit**	Выход из режима настройки интерфейса
Switch_config# **ip exf**	Включает аппаратную IP-маршрутизацию
Switch_config# **show ip vrf** [**brief** | **detail** | **interface**] *vrf-name*	Отображает информацию VRF
Switch_config# **no ip vrf** *vrf-name*	Удаляет настроенный VRF и связь между VRF и интерфейсом L3. *vrf-name*: означает имя VRF
Switch_config_intf# **no ip vrf forwarding** *vrf-name*	Удаляет связь между интерфейсом L3 и VRF

49.2.2.2 Настройка VPN-маршрута

Маршрут между MCE и клиентским устройством может быть установлен посредством настройки BGP, OSPF, RIP, BEIGRP или статической маршрутизации. Ниже в качестве примера приведена настройка OSPF, которая аналогична настройкам других маршрутов.

Когда на MCE настроен маршрут для подключения к клиентской сети, необходимо указать атрибуты VRF протокола маршрутизации. VRF не требуется настраивать на клиентском устройстве.

Команда	Описание
Switch# **config**	Вход в режим настройки коммутатора
Switch_config# **router ospf** *process-id* **vrf** *vrf-name*	Запускает маршрут OSPF-VRF и входит в режим настройки
Switch_config_ospf# **network** *network-number network-mask* **area** *area-id*	Определяет сеть, маску и идентификатор области OSPF
Switch_config_ospf# **redistribute bgp** *ASN*	Перенаправляет назначенную сеть BGP в сеть OSPF
Switch_config_ospf# **exit**	Выход из режима настройки OSPF
Switch_config# **show ip ospf**	Отображает информацию о протоколе OSPF
Switch_config# **no router ospf** *process-id*	Удаляет конфигурацию маршрутизации OSPF-VRF

49.2.2.3 Настройка маршрута BGP между PE и CE

Выполните следующие команды настройки:

Команда	Описание
Switch# **config**	Вход в режим глобальной конфигурации коммутатора
Switch_config# **router bgp** *autonomous-system-number*	Запускает протокол BGP, указывая номер автономной системы, и переходит в режим настройки BGP
Switch_config_bgp# **bgp log-neighbor-changes**	Включает журналирование (логирование) изменений состояния соседей BGP
Switch_config_bgp# **address-family ipv4 vrf** *vrf-name*	Вход в режим настройки семейства адресов VRF
Switch_config_bgp_af# **redistribute ospf** *ospf-process-id*	Пересылает информацию о маршрутизации OSPF в сеть BGP
Switch_config_bgp_af# **network** *network-number/prefix-length*	Настраивает номер сети и длину маски, распространяемые через BGP
Switch_config_bgp_af# **neighbor** *address* **remote-as** *ASN*	Настраивает соседа BGP и номер автономной системы соседа
Switch_config_bgp_af# **exit-address-family**	Выход из режима настройки семейства адресов
Switch_config_bgp# **exit**	Выход из режима настройки BGP
Switch_config# **show ip bgp vpnv4** [**all** | **rd** | **vrf**]	Отображает информацию о маршрутизации BGP-VRF
Switch_config# **no router bgp** *ASN*	Удаляет конфигурацию маршрутизации BGP

49.2.2.4 Проверка соединения VRF между PE и CE

Используйте команду PING с опцией VRF, чтобы подтвердить подключение PE и CE через VRF.

Команда	Описание
Switch# **ping -vrf** *vrf-name ip-address*	Проводит операцию PING по адресам в VRF

49.3 Пример настройки MCE

На рисунке 49-2 показана простая сеть VRF. И S1, и S2 являются коммутаторами CE Multi-VRF. S11, S12 и S13 принадлежат VPN1, S21 и S22 принадлежат VPN2, и все они являются клиентскими устройствами. Маршрут OSPF должен быть настроен между CE и клиентским устройством, а маршрут BGP настроен между CE и PE.

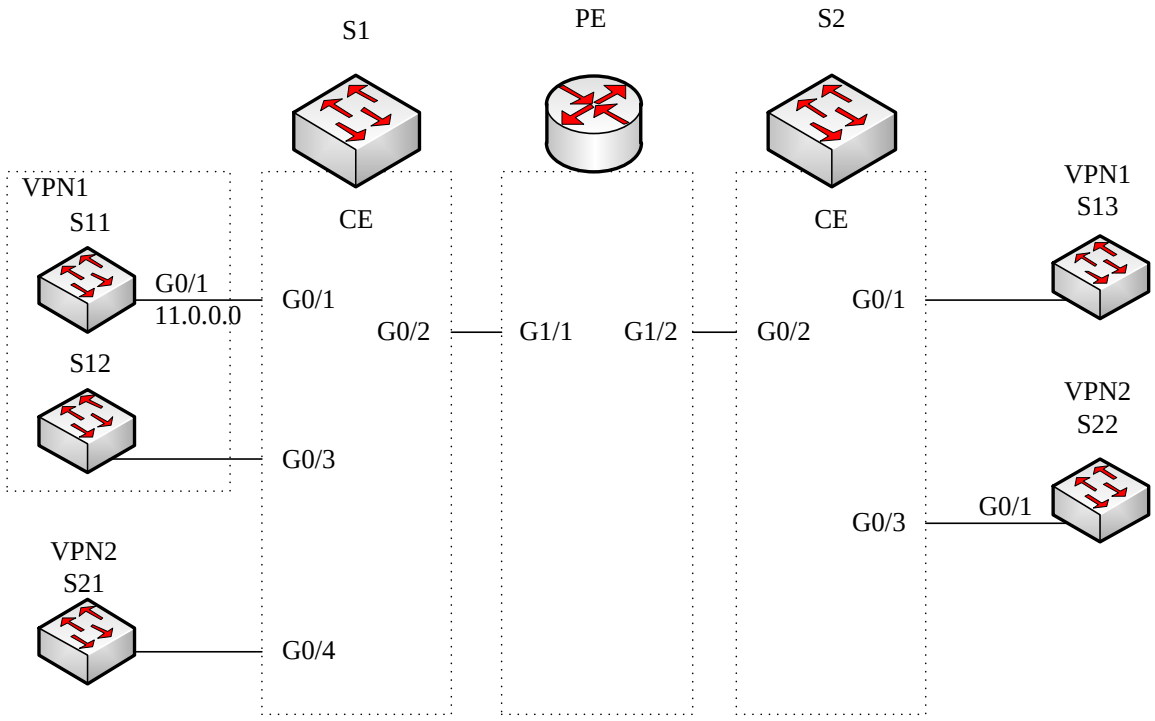

Рисунок 49-2 – Топология сети

49.3.1 Настройка S11

Установите атрибуты VLAN физического интерфейса, соединяющего CE:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 11

Switch_config_g0/1# exit

Установите IP-адрес и интерфейс VLAN:

Switch_config# interface VLAN11

Switch_config_v11# ip address 11.0.0.2 255.0.0.0

Switch_config_v11# exit

Установите протокол маршрутизации между CE и устройством клиента:

Switch_config# router ospf 101

Switch_config_ospf_101# network 11.0.0.0 255.0.0.0 area 0

Switch_config_ospf_101# exit

49.3.2 Настройка MCE-S1

Настройте VRF на устройстве Multi-VRF CE:

Switch# config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 100:1

Switch_config_vrf_vpn1# route-target export 100:1

Switch_config_vrf_vpn1# route-target import 100:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 100:2

Switch_config_vrf_vpn2# route-target export 100:2

Switch_config_vrf_vpn2# route-target import 100:2

Switch_config_vrf_vpn2# exit

Настройте порт обратной связи и физический порт и используйте адрес порта loopback в качестве идентификатора маршрутизатора протокола BGP:

Switch_config# interface loopback 0

Switch_config_l0# ip address 101.0.0.1 255.255.255.255

Switch_config_l0# exit

S1 подключается к S11 через порт G0/1, к S21 – через порт G0/4 и к PE – через порт G0/2:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 11

Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/4

Switch_config_g0/4# switchport pvid 15

Switch_config_g0/4# exit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# exit

Установите порт VLAN L3 коммутатора, привяжите VRF к порту VLAN и установите IP-адрес. S1 подключает PE через два логических порта: VLAN21 и VLAN22. Два порта, VLAN11 и VLAN15, соединяют VPN1 и VPN2 соответственно:

Switch_config# interface VLAN11

Switch_config_v11# ip vrf forwarding vpn1

Switch_config_v11# ip address 11.0.0.1 255.0.0.0

Switch_config_v11# exit

Switch_config# interface VLAN15

Switch_config_v15# ip vrf forwarding vpn2

Switch_config_v15# ip address 15.0.0.1 255.0.0.0

Switch_config_v15# exit

Switch_config# interface VLAN21

Switch_config_v21# ip vrf forwarding vpn1

Switch_config_v21# ip address 21.0.0.2 255.0.0.0

Switch_config_v21# exit

Switch_config# interface VLAN22

Switch_config_v22# ip vrf forwarding vpn2

Switch_config_v22# ip address 22.0.0.2 255.0.0.0

Switch_config_v22# exit

Настройте маршрут OSPF между CE и клиентским устройством:

Switch_config# router ospf 1 vrf vpn1

Switch_config_ospf_1# network 11.0.0.0 255.0.0.0 area 0

Switch_config_ospf_1# redistribute bgp 100

Switch_config_ospf_1#exit

Switch_config# router ospf 2 vrf vpn2

Switch_config_ospf_2# network 15.0.0.0 255.0.0.0 area 0

Switch_config_ospf_2# redistribute bgp 100

Switch_config_ospf_2#exit

Настройте маршрут EBGP между PE и CE:

Switch_config# router bgp 100

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# redistribute ospf 1

Switch_config_bgp_vpn1# neighbor 21.0.0.1 remote-as 200

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# redistribute ospf 2

Switch_config_bgp_vpn2# neighbor 22.0.0.1 remote-as 200

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

Создайте VLAN:

Switch_config# vlan 1,11-12,21-22

Включите аппаратную маршрутизацию:

Switch_config# ip exf

49.3.3 Настройка PE

Настройте VRF на PE:

Switch# config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 200:1

Switch_config_vrf_vpn1# route-target export 200:1

Switch_config_vrf_vpn1# route-target import 200:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 200:2

Switch_config_vrf_vpn2# route-target export 200:2

Switch_config_vrf_vpn2# route-target import 200:2

Switch_config_vrf_vpn2# exit

Установите интерфейс обратной связи в качестве идентификатора маршрутизатора:

Switch_config# interface loopback 0

Switch_config_l0# ip address 102.0.0.1 255.255.255.255

```
Switch_config_l0# exit
```

Установите физический интерфейс, который соединяет PE и CE: G1/1 и G1/2 соединяют S1 и S2 соответственно:

```
Switch_config# interface gigaEthernet 1/1
Switch_config_g1/1# switchport mode trunk
Switch_config_g1/1# interface gigaEthernet 1/2
Switch_config_g1/2# switchport mode trunk
Switch_config_g1/2# exit
```

Установите интерфейс L3 VLAN PE, который соединяет S1:

```
Switch_config# interface VLAN21
Switch_config_v21# ip vrf forwarding vpn1
Switch_config_v21# ip address 21.0.0.1 255.0.0.0
Switch_config_v21# exit

Switch_config# interface VLAN22
Switch_config_v22# ip vrf forwarding vpn2
Switch_config_v22# ip address 22.0.0.1 255.0.0.0
Switch_config_v22# exit
```

Установите интерфейс L3 VLAN PE, который соединяет S2:

```
Switch_config# interface VLAN31
Switch_config_v31# ip vrf forwarding vpn1
Switch_config_v31# ip address 31.0.0.1 255.0.0.0
Switch_config_v31# exit

Switch_config# interface VLAN32
Switch_config_v32# ip vrf forwarding vpn2
Switch_config_v32# ip address 32.0.0.1 255.0.0.0
```

Switch_config_v32# exit

Настройте EBGP PE:

Switch_config# router bgp 200

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# neighbor 21.0.0.2 remote-as 100

Switch_config_bgp_vpn1# neighbor 31.0.0.2 remote-as 300

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# neighbor 22.0.0.2 remote-as 100

Switch_config_bgp_vpn2# neighbor 32.0.0.2 remote-as 300

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

Настройте VLAN и включите аппаратную маршрутизацию:

Switch_config# vlan 1,21-22,31-32

Switch_config# ip exf

49.3.4 Настройка MCE-S2

Настройте VRF:

Switch# config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 300:1

Switch_config_vrf_vpn1# route-target export 300:1

Switch_config_vrf_vpn1# route-target import 300:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 300:2

Switch_config_vrf_vpn2# route-target export 300:2

Switch_config_vrf_vpn2# route-target import 300:2

Switch_config_vrf_vpn2# exit

Настройте порт обратной связи и физический порт и используйте адрес порта loopback в качестве идентификатора маршрутизатора протокола BGP:

Switch_config# interface loopback 0

Switch_config_l0# ip address 103.0.0.1 255.255.255.255

Switch_config_l0# exit

S2 подключается к S13 через порт G0/1, к S22 – через порт G0/3 и к PE – через порт G0/2:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 41

Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/3

Switch_config_g0/3# switchport pvid 46

Switch_config_g0/3# exit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# exit

Установите порт VLAN L3 коммутатора, привяжите VRF к порту VLAN и установите IP-адрес. S2 подключает PE через два логических порта: VLAN31 и VLAN32. Два порта, VLAN41 и VLAN46, соединяют VPN1 и VPN2 соответственно:

Switch_config# interface VLAN41

Switch_config_v41# ip vrf forwarding vpn1

Switch_config_v41# ip address 41.0.0.1 255.0.0.0

Switch_config_v41# exit

Switch_config# interface VLAN46

Switch_config_v46# ip vrf forwarding vpn2

Switch_config_v46# ip address 46.0.0.1 255.0.0.0

Switch_config_v46# exit

Switch_config# interface VLAN31

Switch_config_v31# ip vrf forwarding vpn1

Switch_config_v31# ip address 31.0.0.2 255.0.0.0

Switch_config_v31# exit

Switch_config# interface VLAN32

Switch_config_v32# ip vrf forwarding vpn2

Switch_config_v32# ip address 32.0.0.2 255.0.0.0

Switch_config_v32# exit

Настройте маршрут OSPF между CE и клиентским устройством:

Switch_config# router ospf 1 vrf vpn1

Switch_config_ospf_1# network 41.0.0.0 255.0.0.0 area 0

Switch_config_ospf_1# redistribute bgp 300

Switch_config_ospf_1#exit

Switch_config# router ospf 2 vrf vpn2

Switch_config_ospf_2# network 46.0.0.0 255.0.0.0 area 0

Switch_config_ospf_2# redistribute bgp 300

Switch_config_ospf_2# exit

Настройте маршрут EBGP между PE и CE:

Switch_config# router bgp 300

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# redistribute ospf 1

Switch_config_bgp_vpn1# neighbor 31.0.0.1 remote-as 200

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# redistribute ospf 2

Switch_config_bgp_vpn2# neighbor 32.0.0.1 remote-as 200

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

Создайте VLAN:

Switch_config# vlan 1,31-32,41,46

Включите аппаратную маршрутизацию:

Switch_config# ip exf

49.3.5 Настройка S22

Установите атрибуты VLAN физического интерфейса CE и соедините S22 и S2 через интерфейс G0/1:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 46

Switch_config_g0/1# exit

Установите IP-адрес и интерфейс VLAN:

```
Switch_config# interface VLAN46
Switch_config_v46# ip address 46.0.0.2 255.0.0.0
Switch_config_v46# exit
```

Настройте протокол маршрутизации между CE и устройством клиента:

```
Switch_config# router ospf 103
Switch_config_ospf_103# network 46.0.0.0 255.0.0.0 area 0
Switch_config_ospf_103# exit
```

49.3.6 Проверка VRF-соединения

Запустите команду **ping** на S1, чтобы проверить подключение VPN1 между S1 и S11:

```
Switch# ping -vrf vpn1 11.0.0.2
!!!!!
--- 11.0.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

Подтвердите соединение между S1 и PE:

```
Switch# ping -vrf vpn1 21.0.0.1
!!!!!
--- 21.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

50. VRRP

50.1 Обзор

Протокол резервирования виртуального маршрутизатора VRRP гарантирует безотказную работу отдельного узла при статической маршрутизации по умолчанию. VRRP позволяет избежать недостатков статически заданных шлюзов. Например, группа OLT может работать совместно как виртуальный OLT при помощи VRRP. Виртуальный OLT обладает

виртуальным IP-адресом и виртуальным MAC-адресом для внешних соединений. VRRP выбирает один из OLT в группе в качестве главного (master), отвечающего за пересылку пакетов. Когда у главного OLT возникают проблемы, резервный незамедлительно принимает на себя его задачи, не меняя адрес шлюза по умолчанию. Весь процесс переключения непрозрачен для терминальной системы. Этот механизм может обеспечить быстрое и эффективное решение проблем, как только они возникают.

50.2 Настройка VRRP

Задачи настройки

- Включение/отключение VRRP на интерфейсе
- Настройка режима аутентификации VRRP
- Настройка вытеснения на основе приоритета VRRP
- Настройка MAC-адреса пакета протокола VRRP
- Настройка приоритета VRRP
- Настройка временных параметров VRRP
- Настройка отслеживаемого объекта VRRP
- Мониторинг и поддержка VRRP

50.2.1 Настройка виртуального IP-адреса VRRP

Выполните следующие команды в режиме настройки интерфейса VLAN:

Команда	Описание
vrrp [*vrid*] **associate** *virtual-address address-mask*	Настраивает виртуальный IP-адрес VRRP на интерфейсе
no vrrp [*vrid*] **associate** [*virtual-address address-mask*]	Удаляет виртуальный IP-адрес VRRP на интерфейсе

Виртуальный OLT включается после настройки виртуального адреса VRRP. Виртуальный адрес и основной IP-адрес порта должны находиться в одном сегменте сети. В противном случае виртуальный OLT остается в состоянии «INIT». Когда виртуальный IP-адрес и IP-адрес порта совпадают, система автоматически повышает приоритет виртуального маршрутизатора до 255.

50.2.2 Настройка режима аутентификации VRRP

Выполните следующие команды в режиме настройки интерфейса VLAN.

Команда	Описание
vrrp [*vrid*] **authentication** *WORD*	Настраивает текстовый режим аутентификации VRRP
no vrrp [*vrid*] **authentication**	Возвращает режим аутентификации VRRP к настройкам по умолчанию

В режиме простой текстовой аутентификации строка символов аутентификации находится в сообщении в виде открытого кода и пересылается по сети. Получатель проверяет строку символов аутентификации в сообщении, чтобы увидеть, соответствует ли она локально настроенной строке. Строка аутентификации должна содержать не более восьми символов.

По умолчанию аутентификация VRRP отсутствует.

50.2.3 Настройка описания VRRP

Выполните следующие команды в режиме настройки интерфейса VLAN:

Команда	Описание
vrrp [*vrid*] **description** *WORD*	Настраивает описание VRRP
no vrrp [*vrid*] **description**	Удаляет информацию описания VRRP

Описание VRRP – это информация которая используется для указания использования локального VRRP. По умолчанию VRRP не имеет описания.

50.2.4 Настройка вытеснения на основе приоритета VRRP

Выполните следующие команды в режиме настройки интерфейса VLAN:

Команда	Описание
vrrp [*vrid*] **preempt** [**delay** *second*]	Настраивает приоритетное вытеснение VRRP
no vrrp [*vrid*] **preempt** [**delay**]	Возвращает режим по умолчанию

Режим вытеснения на основе приоритета действует только для резервного OLT. После того как резервный OLT получит VRRP-сообщение от главного OLT, он проверит его приоритет. Если уровень приоритета главного OLT ниже, чем локально настроенный уровень резервного OLT, то, в случае, если установлен режим вытеснения, резервный OLT перейдет в состояние главного и отправит в сеть уведомление. Если же режим вытеснения на основе приоритета не включен, резервный OLT остается в своем прежнем статусе.

По умолчанию настроен невытесняющий режим.

50.2.5 Настройка MAC-адреса пакета протокола VRRP

Выполните следующие команды в режиме настройки интерфейса VLAN:

Команда	Описание
vrrp [*vrid*] **source-mac-use-system**	Настраивает группу VRRP для пересылки пакетов с MAC-адресом системы
no vrrp [*vrid*] **source-mac-use-system**	Настраивает группу VRRP для пересылки пакетов с MAC-адресом протокола

По умолчанию, при переадресации пакетов протокола VRRP используется MAC-адрес протокола в качестве адреса отправителя. Однако, после выполнения указанной команды, в пакетах протокола VRRP в качестве адреса отправителя будет использоваться системный MAC-адрес.

50.2.6 Настройка приоритета VRRP

Выполните следующие команды в режиме настройки интерфейса VLAN:

Команда	Описание
vrrp [*vrid*] **priority** *value* (1~254)	Настраивает приоритет VRRP
no vrrp [*vrid*] **priority**	Возобновляет режим приоритета VRRP по умолчанию

Если виртуальный адрес и адрес порта совпадают, VRRP автоматически увеличит свое значение приоритета до 255. После изменения виртуального адреса или адреса порта значение приоритета автоматически возвращается к исходному значению.

Значение по умолчанию – 100.

50.2.7 Настройка временных параметров VRRP

Выполните следующие команды в режиме настройки интерфейса VLAN:

Команда	Описание
vrrp [*vrid*] **timer advertise** {*value* | **dsec** *value* | **csec** *value*}	Настраивает значение частоты отправки рекламных сообщений VRRP
no vrrp [*vrid*] **timer advertise**	Возвращает значение частоты отправки рекламных сообщений VRRP к значению по умолчанию
no vrrp [*vrid*] **timer learn**	Устанавливает часы VRRP в режим обучения

Значение «часов» (clock value) представляет собой время, которое требуется виртуальному маршрутизатору OLT для восстановления после возникновения проблемы. Когда маршрутизаторы работают в режиме VRRP, они периодически отправляют рекламные сообщения друг другу для информирования о своем состоянии и приоритете. Таймер **timer advertise** устанавливает, с какой периодичностью эти сообщения отправляются. Когда главный маршрутизатор OLT выходит из строя, резервный OLT заменит его и станет главным после интервала, равного 3***timer advertise** + интервал **skew_time**. Если значение частоты отправки рекламных сообщений VRRP слишком велико, это означает, что проблему нельзя устранить немедленно.

Поэтому рекомендуется использовать значение по умолчанию для параметра **timer advertise**.

Значение по умолчанию составляет 1 секунду.

50.2.8 Настройка отслеживаемого объекта VRRP

Выполните следующие команды в режиме настройки интерфейса VLAN:

Команда	Описание
vrrp [*vrid*] **track interface** *intf-id value*	Настраивает отслеживание интерфейса VRRP
no vrrp [*vrid*] **track interface** *intf-id*	Возвращает настройки по умолчанию
vrrp [*vrid*] **track ip** *ip-address value*	Настраивает отслеживание состояния статической маршрутизации на назначенный адрес
no vrrp [*vrid*] **track ip** *ip-address*	Возвращает настройки по умолчанию

Приоритеты в группе VRRP могут быть автоматически скорректированы в зависимости от изменения состояния связи. Если основная линия связи становится недоступной, протокол VRRP позволяет переключить трафик на резервную линию, тем самым обеспечивая непрерывность сервиса. Изменение относится к доступности конечной точки связи, которая использует маршрутизацию VRRP через OLT, а не к доступности самого устройства OLT. Это значит, что, если путь к конечному узлу, проходящий через VRRP-маршрутизируемый OLT, становится недоступным, VRRP позволяет переключиться на резервный маршрут, даже если сам OLT по-прежнему функционирует нормально.

VRRP поддерживает отслеживание двух объектов: во-первых, мониторинг состояния интерфейса: Если отслеживаемый порт переходит в состояние «down», VRRP автоматически понижает приоритет данного маршрутизатора. Это означает, что если основной маршрутизатор теряет связь, то его приоритет уменьшается, и резервный маршрутизатор может взять на себя роль основного. Во-вторых, мониторинг состояния статического маршрута назначенного узла: Если отслеживаемый статический маршрут становится недоступным, VRRP также автоматически понижает приоритет маршрутизатора. Это гарантирует, что в случае проблем с маршрутизацией к определённому узлу, трафик может быть перенаправлен на альтернативный маршрут.

Для мониторинга статического маршрута используется функция BFD (Bidirectional Forwarding Detection), которая обеспечивает быстрое обнаружение сбоев в сети и позволяет VRRP оперативно реагировать на изменения состояния маршрутов.

50.2.9 Мониторинг и поддержка VRRP

Выполните следующие команды в режиме EXEC:

Команда	Описание
show vrrp {**brief** | [**interface** *vlan_intf*] [**detail**]}	Отображает информацию VRRP
debug vrrp [**interface** *intf-id vrid*] {**errors** | **events** | **packets** | **all**}	Включает сбор отладочной информации для пакетов и событий VRRP
no debug vrrp	Отключает сбор отладочной информации для пакетов и событий VRRP

Отображение информации VRRP:

```
Switch_config# show vrrp interface vlan 1 detail
VLAN1 - Group 1
  VRRP State is Master
  Virtual IP address : 192.168.20.110/24
  Virtual Mac address : 0000.5e00.0101
  Current Priority : 100   (Config 100)
  VRRP timer : Advertise 1.0 s (default)   master_down 3.6 s
  VRRP current timer : Advertise 1.0 s master_down 0.0 s preempt after 0.0 s
  Authentication string is not set
  Preempt is set  (delay : 0  s)
  Learn Advertise Interval is not set
  Master Router IP : 192.168.20.118, priority : 100, advertisment :  1.0 s
```

50.3 Пример настройки VRRP

Топология сети показана на рисунке 50-1.

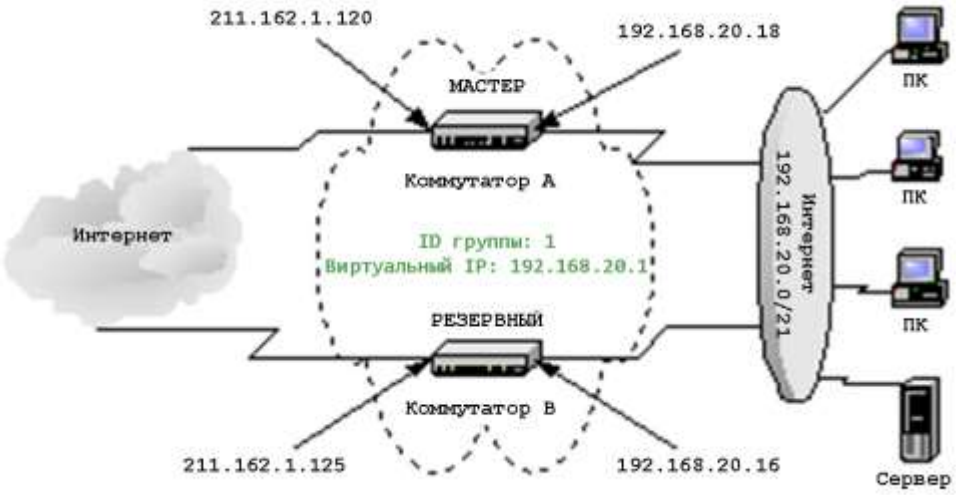

Рисунок 50-1 – Топология сети

Настройка коммутатора А

1. Настройте адрес для интерфейса частной сети.

   Switch_config_v1# ip address 192.168.20.18 255.255.255.0

2. Настройте адрес для интерфейса общедоступной сети.

   Switch_config_v2# ip address 211.162.1.120 255.255.255.0

3. Настройте группу виртуальных коммутаторов 1 на интерфейсе частной сети. Виртуальный адрес – 192.168.20.1. Значение приоритета – 120.

   Switch_config_v1# vrrp 1 associate 192.168.20.1 255.255.255.0

   Switch_config_v1# vrrp 1 priority 120

4. Отображение информации о виртуальном OLT.

   Switch_config# show vrrp detail

   VLAN1 - Group 1

   VRRP State is Master

   Virtual IP address : 192.168.20.1/24

   Virtual Mac address : 0000.5e00.0101

   Current Priority : 120 (Config 120)

   VRRP timer : Advertise 1.0 s (default) master_down 3.6 s

   VRRP current timer : Advertise 1.0 s master_down 0.0 s preempt after 0.0 s

   Authentication string is not set

Preempt is set (delay : 0 s)

Learn Advertise Interval is not set

Master Router IP : 192.168.20.18, priority : 100, advertisment : 1.0 s

Настройка коммутатора B

1. Настройте адрес для интерфейса частной сети.

Switch_config_v1# ip address 192.168.20.16 255.255.255.0

2. Настройте адрес для интерфейса общедоступной сети.

Switch_config_v2# ip address 211.162.1.125 255.255.255.0

3. Настройте группу виртуальных коммутаторов 1 на интерфейсе частной сети. Виртуальный адрес – 192.168.20.1. Значение приоритета – 120.

Switch_config_v1# vrrp 1 associate 192.168.20.1 255.255.255.0

Switch_config_v1# vrrp 1 priority 120

4. Отображение информации о виртуальном OLT.

Switch_config# show vrrp detail

Switch_config# show vrrp interface vlan 1 detail

VLAN1 - Group 1

VRRP State is Backup

Virtual IP address : 192.168.20.1/24

Virtual Mac address : 0000.5e00.0101

Current Priority : 100 (Config 100)

VRRP timer : Advertise 1.0 s (default) master_down 3.6 s

VRRP current timer : Advertise 0.0 s master_down 3.0 s preempt after 0.0 s

Authentication string is not set

Preempt is set (delay : 0 s)

Learn Advertise Interval is not set

Master Router IP : 192.168.20.18, priority : 120, advertisement : 1.0 s

Настройка ПК и сервера частной сети

Настройте шлюз по умолчанию для каждого компьютера и сервера в частной сети на 192.168.20.1.

51. Многоадресная рассылка

51.1 Обзор

В данном разделе описывается, как настроить протокол многоадресной маршрутизации. Традиционная IP-передача позволяет одному хосту взаимодействовать только с одним хостом (одноадресная связь) или со всеми хостами (широковещательная связь). Технология многоадресной рассылки позволяет одному хосту отправлять сообщения нескольким хостам. Эти хосты называются членами группы.

Адрес назначения сообщения, отправленного члену группы, представляет собой адрес класса D (224.0.0.0~239.255.255.255). Многоадресное сообщение передается как UDP. Он не обеспечивает надежную передачу и контроль ошибок, как TCP.

В приложении многоадресной рассылки всегда присутствуют отправитель и получатель. Отправитель может отправить многоадресное сообщение, не присоединяясь к группе. Однако получатель должен присоединиться к группе, прежде чем он сможет получать адресованные ей сообщения.

Отношения между членами группы динамичны. Организатор может присоединиться к группе или покинуть ее в любое время. Ограничений по местонахождению и количеству участников группы нет. При необходимости хост может быть членом нескольких групп. Следовательно, состояние группы и количество ее членов меняется со временем.

Маршрутизатор может поддерживать таблицу маршрутизации для пересылки многоадресных сообщений, выполняя протокол многоадресной маршрутизации, такой как PIM-DM и PIM-SM. Маршрутизатор изучает состояние членов группы в сегменте сети с прямым подключением через IGMP. Хост может присоединиться к назначенной группе IGMP, отправив IGMP-сообщение.

Технология многоадресной IP-адресации подходит для мультимедийных приложений типа «один-ко-множеству».

Понятие «маршрутизатор», упоминаемое в данной главе, – это коммутаторы уровня 3, использующие протоколы маршрутизации, маршрутизаторы в общей сетевой среде и другие устройства, использующие протоколы маршрутизации.

51.1.1 Реализация многоадресной маршрутизации

В программном обеспечении коммутатора многоадресная маршрутизация включает следующие правила:

- IGMP работает между маршрутизатором и хостом в локальной сети и используется для отслеживания отношений между членами группы.
- PIM-DM/PIM-SM – протоколы динамической многоадресной маршрутизации. Они работают между коммутаторами и реализуют многоадресную пересылку путем создания таблицы многоадресной маршрутизации.

На рисунке 51-1 показаны протоколы, используемые в приложениях многоадресной IP-адресации:

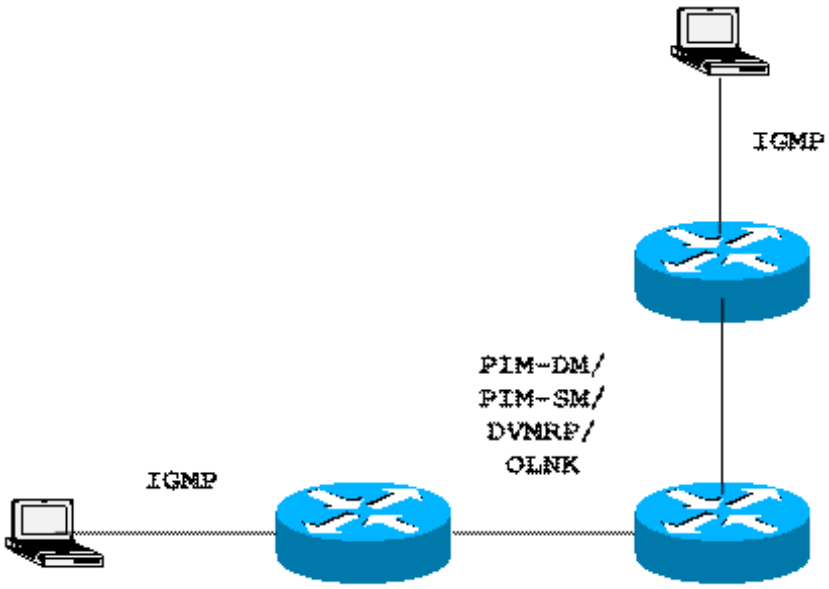

Рисунок 51-1 – Мультикастовые протоколы

51.1.2 Список задач по настройке многоадресной маршрутизации

51.1.2.1 Задачи основной настройки многоадресной рассылки

- Запуск многоадресной маршрутизации (обязательно)
- Настройка порога TTL (необязательно)
- Настройка границы многоадресной передачи (необязательно)
- Настройка помощника многоадресной рассылки (необязательно)
- Настройка тупикового многоадресного маршрута (необязательно)
- Мониторинг и поддержка многоадресного маршрута (необязательно)

51.1.2.2 Задачи настройки IGMP

- Изменение текущей версии IGMP
- Настройка интервала запросов IGMP
- Настройка интервала проверки запросчика IGMP
- Настройка максимального времени ответа IGMP
- Настройка интервала опроса последнего члена группы IGMP

- Статическая конфигурация IGMP
- Настройка списка немедленного выхода из группы IGMP

51.1.2.3 Задачи настройки PIM-DM

- Настройка таймера
- Обозначение версии PIM-DM
- Настройка обновления состояния
- Настройка списка фильтрации
- Установка приоритета DR
- Очистка (S, G)-информации

51.1.2.4 Задачи настройки PIM-SM

- Настройка C-RP
- Настройка C-BSR
- Настройка порога SPT
- Настройка SSM
- Настройка управляемого домена
- Отображение и очистка локальных записей маршрутизации PIM-SM

51.2 Основные настройки многоадресной маршрутизации

51.2.1 Запуск многоадресной маршрутизации

Чтобы разрешить программному обеспечению коммутатора пересылать многоадресные сообщения, необходимо запустить многоадресную маршрутизацию. Выполните следующую команду в режиме глобальной конфигурации, чтобы запустить пересылку многоадресных сообщений:

Команда	Описание
ip multicast-routing	Запускает многоадресную маршрутизацию

51.2.2 Запуск функции многоадресной рассылки на порту

Когда на порту работает протокол многоадресной маршрутизации, на порту активируется IGMP. Протоколы многоадресной маршрутизации включают PIM-DM и PIM-SM. На одном порту может работать только один протокол. Когда маршрутизатор соединяет несколько

доменов многоадресной рассылки, на разных портах могут работать разные многоадресные протоколы.

Тем не менее, программное обеспечение коммутатора может работать как пограничный маршрутизатор многоадресной рассылки (MBR). Если возможно, не запускайте одновременно несколько протоколов многоадресной маршрутизации на одном коммутаторе, поскольку это может серьезно повлиять на работу некоторых из них. Например, при одновременном запуске PIM-DM (поддерживает только записи (S, G)) и BIDIR PIM-SM (поддерживает только записи (*, G)) возможны конфликты и несогласованность данных. Также может произойти повторное построение деревьев, что приведет к неэффективному использованию сетевых ресурсов и увеличению задержек в доставке информации.

51.2.2.1 Запуск PIM-DM

Выполните следующую команду, чтобы запустить PIM-DM на порту, а затем активируйте функцию плотного режима многоадресной рассылки:

Команда	Описание
ip pim-dm	Указывает порт, на котором работает PIM-DM, а затем активирует процесс многоадресной маршрутизации PIM-DM в режиме Настройки интерфейса

51.2.2.2 Запуск PIM-SM

Чтобы запустить PIM-SM на порту и активировать многоадресную рассылку в разреженном режиме, выполните следующую операцию:

Команда	Описание
ip pim-sm	Указывает порт, на котором должен работать PIM-SM, а затем активирует процесс групповой маршрутизации PIM-SM в режиме настройки интерфейса

51.2.3 Настройка порога TTL

Запустите команду **ip multicast ttl-threshold**, чтобы настроить порог TTL многоадресного сообщения, которому разрешено проходить через порт. Запустите команду **no ip multicast ttl-threshold**, чтобы использовать пороговое значение по умолчанию 1.

Команда	Описание
ip multicast ttl-threshold *ttl-value*	Настраивает порог TTL на порту

Пример

В следующем примере показано, как администратор настраивает порог TTL для порта:

```
interface vlan1
ip multicast ttl-threshold 200
```

51.2.4 Настройка границы многоадресной IP-передачи

Запустите команду **ip multicast boundary**, чтобы настроить границу многоадресной рассылки для порта. Запустите команду **no ip multicast boundary**, чтобы отменить настроенную границу. Команды, используемые во второй конфигурации, заменят команды, используемые в первой конфигурации.

Команда	Описание
ip multicast boundary *access-list*	Настраивает границу многоадресной рассылки для порта

Пример

В следующем примере показано, как настроить диапазон адресов, в котором порт может управлять многоадресной рассылкой:

```
interface vlan1
ip multicast boundary acl
!
ip access-list standard acl
permit 192.168.20.97 255.255.255.0
```

51.2.5 Настройка помощника многоадресной передачи

Запустите команду **ip multicast helper-map**, чтобы использовать маршрут многоадресной рассылки для соединения двух широковещательных сетей в многоадресной сети. Запустите команду **no ip multicast helper-map**, чтобы отменить команду.

На первом переходе маршрутизатор подключен к исходной широковещательной сети:

Команда	Описание
interface *type number*	Вход в режим настройки интерфейса
ip multicast helper-map broadcast *group-address access-list*	Настраивает помощник многоадресной рассылки для преобразования широковещательного сообщения в многоадресное

ip directed-broadcast	Разрешает направленную трансляцию
ip forward-protocol [*port*]	Настраивает номер порта, позволяющего пересылать сообщение

На маршрутизаторе последнего перехода, подключающемся к широковещательной сети назначения, выполните следующие операции:

Команда	Описание
interface *type number*	Вход в режим настройки интерфейса
ip directed-broadcast	Разрешает направленную трансляцию
ip multicast helper-map *group-address broadcast-address access-list*	Настраивает помощник многоадресной рассылки для преобразования многоадресного сообщения в широковещательное сообщение
ip forward-protocol [*port*]	Настраивает номер порта, позволяющего пересылать сообщение

Пример

В следующем примере показано, как настроить помощник многоадресной рассылки.

Выполните команду **ip directed-broadcast** на порту vlan1 маршрутизатора первого перехода для обработки направленного сообщения. Настройка **ip multicast helper-map broadcast 230.0.0.1 testacl1** позволяет преобразовать широковещательное сообщение UDP с номером порта 4000, отправленное с исходного адреса 192.168.20.97/24, в многоадресное сообщение с адресом назначения 230.0.0.1.

Выполните команду **ip directed-broadcast** на порту vlan1 маршрутизатора последнего перехода для обработки направленного сообщения. Настройка **ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2**, позволяет преобразовать многоадресное сообщение с номером порта 4000 и адресом назначения 230.0.0.1, отправленное с исходного адреса 192.168.20.97/24, в широковещательное сообщение с адресом назначения 172.10.255.255.

В маршрутизаторе первого перехода, подключающемся к исходной широковещательной сети, выполните следующие операции:

```
interface vlan1
ip directed-broadcast
ip multicast helper-map broadcast 230.0.0.1 testacl1
ip pim-dm
!
ip access-list extended testacl1
 permit udp 192.168.20.97 255.255.255.0 any
```

```
!
ip forward-protocol udp 4000
```

В маршрутизаторе последнего перехода, подключающемся к широковещательной сети назначения, выполните следующие операции:

```
interface vlan2
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim-dm
!
ip access-list extended testacl2
  permit udp 192.168.20.97 255.255.255.0 any
!
ip forward-protocol udp 4000
```

51.2.6 Настройка тупикового многоадресного маршрута

Запустите команды **ip igmp helper-address** и **ip pim-dm neighbor-filter**, чтобы настроить многоадресный маршрут типа Stub.

На порту, к которому подключены stub-маршрутизатор и хост, выполните следующие операции:

Команда	Описание
interface *type number*	Вход в режим настройки интерфейса
ip igmp helper-address *destination-address*	Настраивает команду **ip igmp helper-address** для пересылки многоадресного сообщения на центральный маршрутизатор

На порту, к которому подключены центральный маршрутизатор и stub-маршрутизатор, выполните следующие операции:

Команда	Описание
interface *type number*	Вход в режим настройки интерфейса
ip pim-dm neighbor-filter *access-list*	Фильтрует все сообщения PIM на stub-маршрутизаторе

51.2.7 Мониторинг и поддержка многоадресного маршрута

1. Очистка мультикаст-кэша и таблицы маршрутизации

Если специальные кэши или таблица маршрутизации недействительны, необходимо очистить их содержимое. Выполните следующие команды в режиме управления:

Команда	Описание
clear ip igmp group [*type number*] [*group-address* | *<cr>*]	Очищает элементы кэша IGMP
clear ip mroute [* | *group-address* | *source-address*]	Очищает элементы в таблице многоадресной маршрутизации

2. Отображение таблицы многоадресной маршрутизации и статистической информации системы.

Подробная информация о таблице многоадресной IP-маршрутизации, кэше или базе данных помогает оценить, как используются ресурсы, и решить сетевые проблемы.

Выполните следующие команды в режиме управления, чтобы отобразить статистическую информацию о многоадресном маршруте:

Команда	Описание
show ip igmp groups [*type number* | *group-address*] [**detail**]	Отображает информацию о группе многоадресной рассылки в кэше IGMP
show ip igmp interface [*type number*]	Отображает информацию о конфигурации IGMP на интерфейсе
show ip mroute mfc	Отображает кэш многоадресной пересылки
show ip rpf [**pim-dm** | **pim-sm**] *source-address*	Отображает информацию RPF

51.3 IGMP

51.3.1 Обзор

IGMP (Internet Group Management Protocol) – это протокол, используемый для управления членами групп многоадресной рассылки. IGMP – асимметричный протокол, включающий сторону хоста и сторону коммутатора. На стороне хоста протокол IGMP регулирует, как хост, будучи участником группы многоадресной рассылки, сообщает, к какой группе он принадлежит, и как отвечает на запросы от коммутатора. На стороне маршрутизатора протокол IGMP регулирует, как коммутатор узнает идентификатор члена группы многоадресной рассылки в локальной сети и как изменяет сохраненную информацию о членах группы многоадресной рассылки в соответствии с сообщениями отчета от хоста.

Поскольку данные коммутаторы поддерживают протокол IGMP-Router, протоколу многоадресной маршрутизации может быть предоставлена информация о членах группы многоадресной рассылки в текущей сети, и коммутатор решает, пересылать ли многоадресное сообщение. Чтобы коммутатор поддерживал процесс многоадресной рассылки IP-сообщений, необходимо настроить протокол многоадресной маршрутизации и протокол IGMP-Router. В настоящее время коммутаторы поддерживают IGMP версии 3.

Для IGMP не существует независимых команд запуска. Функция протокола IGMP-Router запускается через протокол многоадресной маршрутизации.

51.3.2 Настройка IGMP

Команды настройки атрибутов IGMP-Router в основном являются командами настройки параметров IGMP. Ниже приводится описание этих команд.

51.3.2.1 Изменение текущей версии IGMP

На данный момент протокол IGMP имеет три формальные версии. Соответствующие RFC: RFC1112, RFC2236 и RFC3376. IGMP V1 поддерживает только функцию записи участников группы многоадресной рассылки. IGMP V2 может запрашивать назначенного участника группы многоадресной рассылки, генерирует сообщение о выходе, когда хост IGMP покидает группу, и сокращает задержку при изменении статуса участника группы. IGMP V3 имеет дополнительные функции для обновления и поддержания идентификаторов членов группы многоадресной рассылки, которые соответствуют адресам исходных хостов. Протокол IGMP-Router V3 полностью совместим с хост-стороной IGMP V1 и IGMP V2. Наше программное обеспечение поддерживает протоколы IGMP трех версий.

Вы можете настроить функцию IGMP-Router на разных интерфейсах (протокол многоадресной маршрутизации, настроенный на разных интерфейсах, может запускать функцию IGMP-Router), и на разных интерфейсах можно запускать разные версии IGMP.

Обратите внимание, что коммутатор многоадресной рассылки может запустить функцию IGMP-Router только на одном из портов, подключающихся к одной сети.

Запустите следующую команду в режиме настройки интерфейса, чтобы изменить версию протокола IGMP на порту:

Команда	Описание
ip igmp version *version_number*	Изменяет версию IGMP, работающую на текущем порту

51.3.2.2 Настройка интервала запросов IGMP

Независимо от номера версии текущего протокола IGMP-Router, многоадресный коммутатор может отправлять сообщение общего запроса IGMP каждый определенный раз на порт, на котором запущена функция IGMP. Адрес передачи – 224.0.0.1. Целью

многоадресного коммутатора является получение отчетного сообщения от хоста IGMP и, следовательно, знание того, к какой группе многоадресной рассылки принадлежит каждый хост IGMP в сети. Интервал отправки сообщения общего запроса называется интервалом запроса IGMP. Если для параметра «IGMP Query Interval» установлено большое значение, коммутатор не сможет сразу получить информацию о том, к какой группе многоадресной рассылки принадлежит текущий хост IGMP. Если для параметра «IGMP Query Interval» установлено небольшое значение, поток сообщений IGMP в текущей сети будет увеличиваться.

Запустите следующую команду в режиме настройки интерфейса, чтобы изменить интервал запросов IGMP на порту:

Команда	Описание
ip igmp query-interval *time*	Изменяет интервал запросов IGMP на текущем интерфейсе (единица измерения – секунды)

51.3.2.3 Настройка интервала проверки запросчика IGMP

Что касается версии 2 и версии 3 протокола IGMP-Router, то если в той же сети существует другой коммутатор, поддерживающий протокол IGMP-Router, вам необходимо выбрать запросчик(querier). Запросчиком называют коммутатор, который может отправлять сообщение запроса. Фактически это порт коммутатора, на котором включен протокол IGMP-Router. Обычно в одной сети есть только один запросчик, то есть только один коммутатор отправляет сообщение запроса IGMP. В IGMP версии 1 нет процедуры выбора запросчика, и протокол многоадресной маршрутизации решает, какой коммутатор будет генерировать запросы.

IGMP-Router V2 и IGMP-Router V3 имеют одинаковый механизм выбора запрашивающего, то есть коммутатор с минимальным IP-адресом является запросчиком в сети. Коммутатору, который не является запрашивающим, необходимо поддерживать счетчик времени для отслеживания наличия запрашивающего. Если время истекает, то устройство, которое не является текущим запросчиком, становится им вместо предыдущего запросчика. Однако оно продолжит выполнять эту функцию только до тех пор, пока не получит запрос IGMP от другого устройства с IP-адресом, меньшим, чем у него. Для IGMP-Router V2 вы можете настроить интервалы проверки запросчика с помощью следующей команды:

Команда	Описание
ip igmp querier-timeout *time*	Настраивает интервал проверки запросчика (единица измерения – секунда)

Для IGMP-Router V1 интервал проверки запросчика бесполезен. Для IGMP-Router V3 интервал настроить невозможно, поскольку он определяется самим протоколом. Таким образом, приведенные выше команды настройки действительны только для IGMP-Router V2.

51.3.2.4 Настройка максимального времени ответа IGMP

Для IGMP-Router V2 и IGMP-Router V3 специальное поле данных в передаваемом сообщении IGMP General Query регулирует максимальное время ответа хоста IGMP. То есть хост IGMP должен отправить ответное сообщение до истечения регламентированного максимального времени ответа, указывая на то, что сообщение общего запроса получено. Если максимальное время ответа установлено на большое значение, смена членов многоадресной группы задерживается. Если максимальное время ответа установлено на небольшое значение, поток сообщений IGMP в текущей сети будет увеличен.

Максимальное время ответа IGMP должно быть короче интервала запроса IGMP. Если значение максимального времени ответа больше интервала запроса, система автоматически установит максимальное время ответа равным интервалу запроса – 1.

Для IGMP-Router V2 и IGMP-Router V3 выполните следующую команду в режиме настройки интерфейса, чтобы установить максимальное время ответа IGMP:

Команда	Описание
ip igmp query-max-response-time *time*	Настраивает максимальное время ответа IGMP (единица измерения – секунды)

51.3.2.5 Настройка интервала запросов IGMP для последнего члена группы

Когда в IGMP-Router V2 и V3 отправляется запрос для конкретной мультикаст-группы, интервал запроса, установленный для последнего участника этой группы, используется как максимальное время ожидания ответа от устройств.

Это означает, что устройство, участвующее в мультикаст-группе (IGMP-хост), должно отправить свой ответ до истечения максимального времени ожидания, установленного для последнего участника группы. Это позволяет указать, что запрос для конкретной мультикаст-группы был получен. Если хост определяет, что ему не нужно отвечать на запрос, он может не отправлять ответ после установленного интервала. В таком случае коммутатор, управляющий мультикаст-группой, должен обновить информацию о членах группы.

Если интервал запроса, установленный для последнего участника группы, большой, это может привести к задержкам при изменении состава группы. Если интервал маленький, это может увеличить количество обмена сообщениями IGMP в текущей сети.

Для IGMP-Router V2 и V3 выполните следующую команду в режиме настройки интерфейса, чтобы установить интервал запросов IGMP для последнего участника группы:

Команда	Описание
ip igmp last-member-query-interval *time*	Настраивает интервал запроса IGMP последнего члена группы (единица измерения – мс)

Данная команда неактуальна для IGMP-Router V1.

51.3.2.6 Статическая конфигурация IGMP

Помимо функций, регулируемых протоколом IGMP-Router, коммутаторы данной серии поддерживают настройку статической группы многоадресной рассылки на порту. Для хоста IGMP отношения с членами группы многоадресной рассылки могут различаться. Предположим, что хост IGMP принадлежит только группе многоадресной рассылки group1, получая от нее и отправляя в нее многоадресные сообщения. По истечении определенного периода времени он может принадлежать также к группе group2, принимать от нее и отправлять в нее многоадресные сообщения. По истечении другого периода времени хост IGMP может не принадлежать ни к одной из групп многоадресной рассылки. Поэтому информация о назначении группы многоадресной рассылки варьируется.

В отличие от вышеупомянутой динамической группы многоадресной рассылки, если порт настроен как принадлежащий к статической группе, протокол многоадресной маршрутизации затем принимает порт как тот, который всегда получает и отправляет многоадресные сообщения в пределах этой группы. Для лучшей совместимости с IGMP-Router V3 статическую группу многоадресной рассылки можно настроить на получение многоадресных сообщений с назначенного адреса источника, то есть при получении сообщения добавляется функция фильтра источника.

Запустите следующую команду в режиме настройки интерфейса, чтобы указать статическую многоадресную группу для порта:

Команда	Описание
ip igmp static-group { * | *group-address*} {**include** *source-address* | *<cr>* }	Настраивает атрибут статической группы многоадресной рассылки для порта

51.3.2.7 Настройка списка немедленного выхода из группы IGMP

Если IGMP V2 запущен на порту коммутатора и сеть, к которой подключается этот порт, имеет только один хост IGMP, вы можете реализовать функцию немедленного выхода для хоста, настроив список немедленного выхода из группы IGMP. Согласно правилам IGMP V2, когда хост покидает определенную группу, он отправляет сообщение Leave всем коммутаторам многоадресной рассылки. После получения сообщения Leave коммутаторы многоадресной рассылки отправляют сообщение, специфичное для группы, чтобы подтвердить, существует ли на порту какое-либо многоадресное сообщение, которое хост должен получить из группы или отправить в нее. Если настроена функция «Немедленный выход», между хостом IGMP и коммутатором многоадресной рассылки не требуется обмен сообщениями. Изменение идентификаторов членов группы не будет задерживаться.

Команда может быть настроена как в режиме глобальной конфигурации, так и в режиме настройки интерфейса. Приоритет команды, настроенной в глобальном режиме, выше, чем у команды, настроенной в режиме интерфейса. Если команда сначала настроена в глобальном режиме, команда, настроенная в режиме

интерфейса, будет проигнорирована. Если команда сначала настроена в режиме настройки интерфейса, команда, настроенная глобально, удалит настройки, выполненные на интерфейсе.

Для IGMP-Router V2 выполните следующую команду в режиме интерфейса, чтобы настроить список немедленного выхода из группы IGMP:

Команда	Описание
ip igmp immediate-leave group-list *list-name*	Указывает список доступа, реализующий функцию немедленного выхода из группы многоадресной рассылки для хоста IGMP
ip access-list standard *list-name*	Создает стандартный список IP-доступа с именем *list-name*
permit *source-address*	Настраивает IP-адрес для хоста IGMP, который будет реализовывать функцию немедленного выхода в режиме настройки стандартного списка доступа

51.3.3 Примеры настройки функций IGMP

1. Пример изменения версии IGMP

Протокол IGMP-Router последней версии совместим с хостом IGMP младшей версии, но не может быть совместим с протоколом IGMP-Router более ранней версии. Поэтому, если в текущей сети есть коммутаторы, использующие протокол IGMP-Router более ранней версии, вам необходимо изменить протокол IGMP-Router последней версии на протокол самой ранней версии, работающий в том же сегменте сети.

Предположим, администратор знает, что коммутаторы, работающие под управлением IGMP-Router V1 и IGMP-Router V2, существуют в сети, к которой подключается локальный коммутатор. Администратору необходимо изменить версию протокола IGMP-Router с версии 2 на версию 1 на порту коммутатора, на котором работает IGMP-Router V2.

```
interface vlan 1
ip igmp version 1
```

2. Пример настройки интервала запроса IGMP

В следующем примере показано, как изменить интервал запроса IGMP до 50 секунд на интерфейсе vlan 1:

```
interface vlan 1
ip igmp query-interval 50
```

3. Пример настройки интервала проверки запросчика IGMP

В следующем примере показано, как изменить интервал проверки запросчика на 100 секунд для интерфейса vlan 1:

```
interface vlan 1
ip igmp querier-timeout 100
```

4. Пример настройки максимального времени ответа IGMP

В следующем примере показано, как изменить максимальное время ответа IGMP до 15 секунд на интерфейсе vlan 1:

```
interface vlan 1
ip igmp query-max-response-time 15
```

5. Пример настройки интервала запроса IGMP для последнего члена группы

В следующем примере показано, как изменить интервал запроса IGMP последнего члена группы на 2000 мс на интерфейсе vlan 1:

```
interface vlan 1
ip igmp last-member-query-interval 2000
```

6. Пример статической конфигурации IGMP

Команда настройки статической группы многоадресной рассылки может определять различные классы статических групп, принимая разные параметры. В следующих примерах показаны результаты выполнения различных параметров команды.

```
interface vlan 1
ip igmp static-group *
```

Предыдущая команда настраивает все статические группы многоадресной рассылки на интерфейсе vlan 1. Протокол многоадресной маршрутизации будет транслировать все многоадресные IP-сообщения на интерфейс vlan 1.

```
interface vlan 1
ip igmp static-group 224.1.1.7
```

Предыдущая команда настраивает статическую многоадресную группу 224.1.1.7 на интерфейсе vlan 1, то есть интерфейс принадлежит группе многоадресной рассылки 224.1.1.7. Протокол многоадресной маршрутизации будет отправлять все многоадресные IP-сообщения, целью назначения которых является группа многоадресной рассылки 224.1.1.7, на интерфейс vlan 1.

```
interface vlan 1
ip igmp static-group 224.1.1.7 include 192.168.20.168
```

Предыдущая команда настраивает статическую группу многоадресной рассылки 224.1.1.7 на интерфейсе vlan 1 и определяет фильтр источника для этой группы как 192.168.20.168.

То есть интерфейс принадлежит к группе многоадресной рассылки 224.1.1.7, но он получает многоадресные IP-сообщения только с адреса 192.168.20.168. Протокол многоадресной маршрутизации будет отправлять все многоадресные IP-сообщения, полученные от 192.168.20.168 и целью назначения которых является группа 224.1.1.7, на интерфейс vlan 1.

Выполните следующую команду в режиме настройки интерфейса, чтобы принимать мультикастовый трафик для группы 224.1.1.7 только если он исходит с IP-адреса 192.168.20.169:

```
ip igmp static-group 224.1.1.7 include 192.168.20.169
```

Предыдущую команду можно выполнять много раз, чтобы определить разные адреса источника.

В группе многоадресной рассылки нельзя одновременно настроить информацию о группе как для конкретного источника данных, так и для всех источников данных. Если выполнить команду для настройки информации о группе с указанием всех источников, то команда, выполненная позже для настройки информации с указанием конкретного источника, будет проигнорирована. Например, если выполнить команду **ip igmp static-group 224.1.1.7 include 192.168.20.168** после выполнения команды **ip igmp static-group 224.1.1.7**, то команда **ip igmp static-group 224.1.1.7 include 192.168.20.168** будет проигнорирована.

---

7. Пример настройки списка участников IGMP с немедленным выходом

В следующем примере показано, как настроить список доступа для реализации функции немедленного выхода на интерфейсе vlan 1 и добавить IP-адрес 192.168.20.168 хоста IGMP в список доступа. Конфигурация гарантирует, что хост IGMP с IP-адресом 192.168.20.168 реализует функцию немедленного выхода.

```
interface vlan 1
 ip igmp immediate-leave imme-leave
!
ip access-list standard imme-leave
 permit 192.168.20.168
```

51.4 PIM-DM

51.4.1 Введение

PIM-DM (Protocol Independent Multicast Dense Mode) – это протокол многоадресной маршрутизации в плотном режиме. По умолчанию, когда источник многоадресной рассылки начинает отправлять мультикастовые данные, их получают все сетевые узлы в домене, так как PIM-DM пересылает многоадресные пакеты в режиме ограниченной широковещательной рассылки. Когда источник рассылки начинает отправлять данные, коммутаторы рядом с ним пересылают многоадресные пакеты на все активированные интерфейсы PIM, кроме интерфейса RPF (Reverse Path Forwarding). Таким образом, все сетевые узлы в домене PIM-DM могут получать эти многоадресные пакеты. Чтобы завершить многоадресную пересылку, коммутаторам вместе необходимо создать соответствующий элемент многоадресной маршрутизации (S, G) для группы G и ее источника S. Элемент маршрутизации (S, G) включает в себя адрес источника многоадресной рассылки, адрес группы многоадресной рассылки, входной интерфейс, список выходных интерфейсов, таймер и метку.

Если в определенном сегменте сети нет члена группы многоадресной рассылки, PIM-DM отправит информацию об «обрезании» (Pruning) лишних ветвей широковещательного дерева, отключит интерфейс пересылки, соединяющий сегмент сети, а затем установит состояние Pruning. Оно длится соответственно таймеру тайм-аута. По истечении времени таймера состояние снова меняется на пересылку (Forwarding), и многоадресные данные могут пересылаться по ранее пресеченным ветвям. Кроме того, состояние Pruning содержит информацию об источнике многоадресной рассылки и группе многоадресной рассылки. Когда член группы многоадресной рассылки появляется в обрезанной области, PIM-DM активно отправляет сообщение о присоединении в верхнее поле, не дожидаясь истечения таймера, переводя состояние Pruning в состояние Forwarding.

Пока источник S все еще транслирует данные в группу G, коммутатор первого перехода будет периодически отправлять обновляющую информацию элемента маршрутизации (S, G) в нижнее исходное широковещательное дерево для завершения обновления. Механизм обновления состояния PIM-DM может обновлять состояние нисходящего канала, гарантируя, что сокращение широковещательного дерева не истечет по тайм-ауту.

В сети с множественным доступом, помимо выбора DR, PIM-DM также вводит следующие механизмы:

- механизм подтверждения для выбора уникального отправителя, чтобы предотвратить повторную пересылку многоадресного пакета;
- механизм ограничения добавления/обрезания для уменьшения избыточной информации о добавлении/обрезании;
- механизм запрета режима Pruning для предотвращения неправильных действий по обрезанию широковещательного дерева.

В домене PIM-DM маршрутизаторы, на которых работает PIM-DM, периодически отправляют информацию Hello для достижения следующих целей:

- обнаружение соседних маршрутизаторов PIM;
- оценка конечных сетей и конечных маршрутизаторов;
- выбор назначенного маршрутизатора (DR) в сети с множественным доступом.

Чтобы быть совместимым с IGMP v1, PIM-DM отвечает за выбор DR. Когда все соседние маршрутизаторы PIM поддерживают настройку приоритета на интерфейсе, в качестве DR выбирается маршрутизатор с более высоким приоритетом. Если приоритет одинаковый, в качестве DR выбирается маршрутизатор с максимальным значением IP-интерфейса. Если приоритет не отображается в сообщении Hello нескольких маршрутизаторов, в качестве DR выбирается маршрутизатор, интерфейс которого имеет наибольшее значение IP.

PIM-DM v2 коммутаторов данной серии поддерживает список фильтрации соседей, CIDR, VLSM и IGMP v1-v3.

51.4.2 Настройка PIM-DM

51.4.2.1 Настройка таймера

Протокол маршрутизации использует несколько таймеров для определения частоты передачи сообщения Hello и управляющего сообщения обновления состояния. Интервал передачи сообщения Hello влияет на возможность корректного создания отношений соседства.

Выполните следующие команды в режиме глобальной конфигурации, чтобы установить таймер:

Команда	Описание
ip pim-dm hello-interval	Устанавливает интервал (единица измерения – секунда) для отправки сообщения Hello от интерфейса и соседа
ip pim-dm state-refresh origination-interval	Для коммутатора первого перехода, напрямую подключенного к источнику, интервал отправки сообщения обновления состояния действителен только для конфигураций восходящих портов. Для следующих коммутаторов интервал – это период получения и обработки сообщения об обновлении состояния

51.4.2.2 Обозначение номера версии

Поскольку PIM v1 устарел, по умолчанию поддерживается PIM v2.

Команда	Описание
ip pim-dm version *version*	Настраивает версию PIM-DM на логическом порту коммутатора

51.4.2.3 Настройка обновления состояния

Управляющая информация о состоянии PIM-DM по умолчанию пересылается в режиме управления. Команды настройки в режиме интерфейса эффективны только для восходящих портов, когда коммутатор первого перехода, напрямую подключенный к источнику, периодически отправляет обновленное сообщение о текущем состоянии. Для следующих коммутаторов интервал – это период получения и обработки сообщения о состоянии.

Команда	Описание
no ip pim-dm state-refresh disable	Позволяет отправлять и получать на порту сообщения обновления состояния
ip pim-dm state-refresh origination-interval	Настраивает интервал для отправки и получения на порту сообщения обновления состояния

51.4.2.4 Настройка списка фильтрации

PIM-DM не устанавливает список фильтрации по умолчанию. Указанный список фильтрации включает в себя список фильтрации соседей и список фильтрации границ многоадресной рассылки. Список фильтрации необходимо настроить в режиме настройки интерфейса.

Чтобы запретить коммутатору или коммутаторам в сегменте сети участвовать в согласовании PIM-DM, необходимо настроить список фильтрации соседей. Чтобы запретить или разрешить некоторым группам проходить через локальный регион, необходимо настроить список фильтрации границ многоадресной рассылки.

Команда	Описание
ip pim-dm neighbor-filter	Настраивает список фильтрации соседей
ip multicast boundary	Настраивает список фильтрации границ многоадресной рассылки

51.4.2.5 Установка приоритета DR

Для совместимости с IGMP v1 требуется выбор DR. По умолчанию приоритет DR установлен на 1. Когда все соседние маршрутизаторы PIM на интерфейсе поддерживают приоритет DR, маршрутизатор с более высоким приоритетом выбирается в качестве DR. Если приоритет одинаковый, в качестве DR выбирается соседний маршрутизатор с максимальным значением IP-интерфейса. Если приоритет не отображается в сообщении Hello нескольких маршрутизаторов, в качестве DR выбирается маршрутизатор, интерфейс которого имеет наибольшее значение IP.

Запустите следующую команду в режиме настройки интерфейса:

Команда	Описание
ip pim-dm dr-priority	Настраивает приоритет локального DR на назначенном порту

51.4.2.6 Очистка элемента (S, G)

Периодически элемент (S, G) в локальной MRT или статистическое значение числа многоадресных сообщений, пересылаемых через элемент (S, G) необходимо очищать. Для этого выполните следующие команды в режиме управления:

Команда	Описание
clear ip mroute pim-dm {* | *group* [*source*]}	Очищает элемент (S, G) в локальной MRT. Операция заключается в удалении всех или части элементов локальной таблицы многоадресной маршрутизации. Это может повлиять на пересылку многоадресных сообщений. Команда используется для удаления только элементов (S, G), созданных протоколом многоадресной маршрутизации PIM-DM на восходящих портах
clear ip pim-dm interface	Сбрасывает значение статистики многоадресного сообщения, пересылаемого (S, G) на порт PIM-DM. Команда используется для сброса только элементов (S, G), созданных протоколом многоадресной маршрутизации PIM-DM на восходящих портах

51.5 PIM-SM

51.5.1 Введение

Протокол многоадресной маршрутизации в разреженном режиме PIM-SM (Protocol Independent Multicast Sparse Mode) позволяет использовать таблицу маршрутизации для многоадресных данных, независимо от применяемого протокола для одноадресной маршрутизации, такого как RIP, OSPF, IS-IS, BGP и другие. PIM не зависит от протокола одноадресной маршрутизации, при условии, что в таблице многоадресной маршрутизации могут быть сгенерированы соответствующие записи.

PIM использует механизм RPF (Reverse Path Forwarding) для пересылки многоадресных-пакетов. Когда такой пакет поступает на устройство, выполняется проверка RPF: если RPF-проверка проходит, то создается соответствующая запись в таблице многоадресной

маршрутизации и пакет пересылается; если RPF-проверка не проходит, то пакет отбрасывается.

51.5.2 Настройка PIM-SM

51.5.2.1 Глобальное включение многоадресной рассылки

Команда:

ip multicast-routing

no ip multicast-routing

Если вы хотите использовать протокол PIM-SM, запустите команду в режиме глобальной конфигурации:

switch_config# ip multicast-routing

Для отображения настройки используйте команду **show running**. Результат будет выглядеть следующим образом:

!

ip multicast-routing

!

Если вы не хотите использовать протокол pim-sm, запустите команду в режиме глобальной конфигурации:

switch_config# no ip multicast-routing

51.5.2.2 Запуск PIM-SM

После глобального включения функции многоадресной маршрутизации необходимо настроить интерфейс, поддерживающий PIM-SM, для отправки и получения пакетов протокола на соответствующем порту. Для каждого порта маршрутизации протокол многоадресной рассылки является эксклюзивным. То есть, если на порту включены другие протоколы многоадресной рассылки, настроить PIM-SM невозможно.

Предварительные условия для того, чтобы PIM-SM вступил в силу на интерфейсе:

- на порту настроен основной IP-адрес;
- протокол на порту включен;
- PIM-SM настроен на порту.

Пример настройки:

```
switch_config# interface v8
switch_config_v8#ip address 172.17.21.173 255.255.255.0
switch_config_v8#ip pim-sm
```

После настройки используйте команду **show running** для отображения результата:

```
!
interface VLAN8
ip address 172.17.21.173 255.255.255.0
no ip directed-broadcast
ip pim-sm
!
```

Для отображения состояния PIM-SM на интерфейсе, используйте команду **show ip pim-sm interface**:

```
switch# show ip pim-sm interface
Intf     Address         Ver/   Nbr    Hello  DR     DR
                         Mode   Count  Intvl  Prior  Addr
v8     172.17.21.173     V2/S   0      30     1      172.17.21.173
```

Если вы хотите отключить PIM-SM на интерфейсе, используйте форму команды с префиксом **no**:

```
switch_config# interface v8
switch_config_v8#no ip pim-sm
```

51.5.2.3 Настройка списка фильтрации соседей

PIM-SM поддерживает взаимодействие с соседями через обмен информацией «Hello». Эта информация используется для обнаружения соседей и согласования соответствующих параметров.

Когда маршрутизатор PIM-SM периодически посылает Hello-пакеты всем PIM-узлам (на мультикаст-адрес 224.0.0.13), он устанавливает соседские отношения, принимая Hello-пакеты и согласовывая параметры. Если маршрутизатор получает Hello-пакет до того, как

сам отправит свой, он будет считать, что соседний маршрутизатор уже есть. Если же маршрутизатор не получает Hello-пакет, он будет считать, что соседа не существует.

Настройка фильтра соседей позволяет проверять и отфильтровывать соседей для пакетов типа «Hello» на соответствующем интерфейсе. Если фильтр соседей удален или только что запрещенный сосед был снова разрешен, информация о соседе будет обновлена только в период следующего обмена Hello-сообщениями.

Шаги по настройке списка фильтрации соседей:

1. Настройка основного IP-адреса на интерфейсе;
2. Включение протокола на интерфейсе;
3. Настройка PIM-SM на интерфейсе;
4. Настройка стандартного списка доступа PIM-SM на интерфейсе для фильтрации соседей.

Пример настройки:

```
switch_config#interface v9
switch_config_v9#ip address 172.20.21.172 255.255.255.0
switch_config_v9#ip pim-sm
switch_config_v9#ip pim-sm nbr-filter nbr_permit
switch_config_v9#exit
switch_config#ip access-list standard nbr_permit
switch_config_std_nacl#permit 172.20.21.174 255.255.255.0
```

Результат настройки: включение пакетов Hello из сегмента 172.20.21.0/24 и установленное отношение соседства.

```
R172_config_std_nacl#show ip pim-s nei
PIM-SMv2 Neighbor Table
Neighbor        Interface          Uptime/Expires     DR
Address                                               Prior
172.20.21.173     v9          00:15:24/00:01:30   1(DR)
```

Измените конфигурацию следующим образом, и интерфейс v9 разрешит передачу пакетов приветствия только с адреса 172.20.21.174.

```
S172_config_std_nacl#permit 172.20.21.174 255.255.255.255
```

Отладочная информация следующая:

```
2023-1-1 00:16:26 PIM-SM: rcvd hello from 172.20.21.173, filter by acl
```

Предыдущий установленный сосед будет постепенно стареть до истечения времени:

```
S172#show ip pim-s nei
PIM-SMv2 Neighbor Table
Neighbor        Interface          Uptime/Expires     DR
Address                                               Prior
172.20.21.173   v9          00:17:21/00:00:03   1(DR)
```

51.5.2.4 Выбор DR

DR – это избранный маршрутизатор, который выбирают в сценариях с несколькими маршрутизаторами на одном сегменте сети. Выбор идет на основе приоритета и IP-адреса, которые указаны в пакете Hello каждого маршрутизатора.

Роль DR включает в себя:

1. Ответ на информацию IGMP(v1) от хоста. Если хост напрямую соединяется с двумя или более маршрутизаторами PIM-SM через Ethernet, только DR информирует и перенаправляет пакеты (*, G) join. Если DR и победитель операции «assert» на получающей стороне сталкиваются, выигрывает первый.

2. DR генерирует первоначальные регистрационные пакеты на источнике многоадресной рассылки и регистрирует их на RP (Rendezvous Point). Если найден новый сосед, DR отвечает за пересылку запомненных локальных пакетов BSM. Чтобы увеличить шансы локального коммутатора стать DR, повысьте локальный приоритет DR или значение IP-адреса в условиях одинакового приоритета DR.

Шаги по настройке приоритета DR:

1. Настройка основного IP-адреса на интерфейсе;
2. Включение протокола порта;
3. Настройка PIM-SM на интерфейсе;
4. Настройка **ip pim-sm dr-priority** на интерфейсе.

51.5.2.5 Настройка кандидата на роль RP

Если вам нужно настроить коммутатор в качестве кандидата на роль RP, выполните следующие четыре операции:

1. Настройте IP-адрес для порта маршрутизации, который должен быть кандидатом на роль RP;

2. Включите PIM-SM на порту;

3. Настройте PIM-SM в режиме глобальной конфигурации при помощи команды **router pim-sm**.

4. В режиме глобальной настройки PIM-SM выполните команду **c-rp ***** с необходимыми параметрами.

Пример настройки:

```
switch_config#interface loopback1
switch_config_l1#ip addr 1.1.1.1 255.255.255.0
switch_config_l1#ip pim-sm
switch_config#router pim-sm
switch_config_ps#c-rp lo1 list rp-range
switch_config_ps#exit
switch_config#ip access-list stand rp-range
switch_config_std_nacl#permit 225.1.1.0 255.255.255.0
switch_config_std_nacl#permit 226.1.1.0 255.255.255.0
```

Приведенная выше конфигурация указывает, что адрес кандидата на роль RP – 1.1.1.1, а поддерживаемые диапазоны групп – 225.1.1.0/24 и 226.1.1.0/24.

Используя команду **show**, вы можете посмотреть локальную конфигурацию CRP и его рабочее состояние.

```
switch_config#show ip pim-sm bsr
PIMv2 BSR information:
Candidate-RP: 1.1.1.1(Loopback1)
Interval of Advertisements: 60 seconds
Next Advertisement will be sent in 00:00:55
switch_config#
```

Если вы хотите отменить для коммутатора функцию кандидата на роль RP, выполните настройку в режиме конфигурации PIM-SM. Используйте форму команды **no**, чтобы очистить соответствующие настройки:

```
switch_config#router pim-sm
switch_config_ps#no c-rp loopback1
```

После очистки соответствующей конфигурации отобразите текущий статус CRP коммутатора с помощью команды **show**:

```
switch_config_ps#exit
```

```
switch_config#show ip pim-sm bsr
PIMv2 BSR information:
switch_config#
```

Кроме того, вы можете просмотреть соответствующую информацию о текущем состоянии конфигурации PIM-SM с помощью команды **show running-config**.

51.5.2.6 Настройка кандидата на роль BSR

Если вам нужно настроить коммутатор в качестве кандидата на роль BSR, выполните следующие четыре операции:

1. Настройте IP-адрес для порта маршрутизации, который должен быть кандидатом на роль BSR;

2. Включите PIM-SM на порту;

3. Настройте PIM-SM в режиме глобальной конфигурации при помощи команды **router pim-sm**.

4. В режиме глобальной настройки PIM-SM выполните команду **c-bsr ***** с необходимыми параметрами.

Пример настройки:

```
switch_config#interface loopback1
switch_config_l1#ip addr 1.1.1.1 255.255.255.0
switch_config_l1#ip pim-sm
switch_config#router pim-sm
switch_config_ps#c-bsr loopback1 30 200
```

Приведенная выше конфигурация указывает, что после того, как кандидат BSR выбран в качестве EBSR, длина хэша равна 30; приоритет данного кандидата BSR для участия в выборах равен 200.

С помощью команды **show** вы можете отобразить локальную конфигурацию кандидата BSR и рабочий статус:

```
switch_config_ps#show ip pim bsr
PIMv2 BSR information:
I am a Candidate-BSR:Loopback1 in sz 224.0.0.0/4.
CBSR-STM state (0-c,1-p,2-e):1.
switch_config_ps#
```

Наблюдайте за переключением состояний CBSR. Следующий пример показывает, что коммутатор был выбран в качестве EBSR:

```
switch_config_ps#show ip pim bsr
PIMv2 BSR information:
I am BSR in sz 224.0.0.0/4
  CBSR-STM state (0-c,1-p,2-e):2.
  Address of BSR:      1.1.1.1
  BSR Priority:        200
  Hash Mask Length:    30
  Uptime:              02:54:12
  BSR will expires in 00:00:51
switch_config_ps#
```

Если вы хотите отменить для коммутатора функцию кандидата на роль BSR, выполните настройку в режиме конфигурации PIM-SM. Используйте форму команды **no**, чтобы очистить соответствующие настройки:

```
switch_config#router pim-sm
switch_config_ps#no c-bsr loopback1
```

После очистки соответствующей конфигурации отобразите текущий статус CBSR коммутатора с помощью команды **show**:

```
switch_config_ps#show ip pim bsr
PIMv2 BSR information:
I am NCBSR in sz 224.0.0.0/4
NCBSR-STM state(0-NI,1-AA,2-AP):1
switch_config_ps#
```

Кроме того, вы можете просмотреть соответствующую информацию о текущем состоянии конфигурации PIM-SM с помощью команды **show running-config**.

51.5.2.7 Настройка порога SPT

Когда данные пересылаются на коммутаторе, он должен решить, нужно ли переключиться с режима RPT (Reverse Path Tree) на режим SPT (Shortest Path Tree). Для принятия этого решения используется параметр порогового значения spt-threshold. По умолчанию переключение с режима RPT на режим SPT происходит, когда получатель принимает первый пакет данных. Мы также можем установить пороговое значение для переключения

с режима RPT на режим SPT, измеряемое в килобайтах в секунду. Если происходит переключение с режима RPT на режим SPT, оно обычно не отменяется.

```
switch_config#router pim-sm
switch_config_ps#spt-threshold 1000
```

51.5.2.8 Настройка SSM

SSM (Source-Specific Multicast) – это модель мультимедийной рассылки, которая ориентирована на источник данных и получателя и предоставляет более точный и контролируемый способ управления потоками многоадресных данных.

SSM-модель требует поддержки IGMPv3 и активации IGMPv3 на устройствах PIM-SM, на которых находятся получатели данных. Для активации SSM-модели в PIM-SM, необходимо включить функции PIM-SM и SSM на системе. При развертывании PIM-SM рекомендуется включить PIM-SM на всех неграничных интерфейсах.

Во время передачи информации от источника многоадресной рассылки к получателю выбирается либо PIM-SSM, либо PIM-SM в зависимости от того, существует ли заданная мультимедийная группа получателя (S, G) в группе, заданной для PIM-SSM. То есть, когда интерфейсы используют PIM-SM, они будут учитывать, что данные мультимедийной группы находятся в пределах диапазона, определенного для модели PIM-SSM.

Перед настройкой основных функций PIM-SSM необходимо настроить маршрут для одноадресной передачи данных, чтобы обеспечить взаимодействие внутреннего сетевого уровня и наличие доступных маршрутов.

Шаги для настройки PIM-SSM включают в себя активацию PIM-SM на интерфейсе, вход в режим настройки PIM-SM и указание диапазона адресов SSM группы, а также, при необходимости, других функций PIM-SM.

Пример настройки

```
switch_config#interface v8
switch_config_v8#ip addr 1.1.1.1 255.255.255.0
switch_config_v8#ip pim-sm
switch_config_v8#exit
switch_config#router pim-sm
switch_config_ps#ssm rang grp_range
switch_config_ps#exit
switch_config#ip access-list standard grp-range
switch_config_std_nacl#permit 233.1.0.0 255.255.0.0
```

switch_config_std_nacl#

Если SSM отменен, отключите связанную с ним конфигурацию, указав «no» в режиме настройки PIM-SM.

51.5.2.9 Настройка управляемого домена

В механизме без управления доменами многоадресной рассылки PIM-SM один домен PIM-SM имеет только один эксклюзивный BSR. Вся сеть контролируется этим BSR. Однако для более удобного управления сетью PIM-SM можно разделить на несколько управляемых доменов: каждый управляемый домен поддерживает свой собственный BSR и обслуживает мультимедийные группы в определенном диапазоне. Глобальный домен также поддерживает один BSR, который обслуживает все остальные мультимедийные группы.

В механизме управления доменами граница каждого управляемого домена состоит из ZBR (граничное устройство управления) и каждый управляемый домен поддерживает свой собственный BSR, который обслуживает мультимедийные группы в определенном диапазоне. Пакеты протокола мультимедийной рассылки, относящиеся к этому диапазону, не могут пересекать границу управляемого домена.

В сети, применяющей механизм управления доменами, выбор BSR для разных мультимедийных групп осуществляется через C-BSR. C-RP в сети только пересылает информационные пакеты на соответствующий BSR, и BSR суммирует эти пакеты в RP-SET (Rendezvous Point Set) и информирует все устройства в пределах управляемого домена об этом.

Если вы хотите найти RP многоадресной группы, найдите соответствующий управляемый домен с наибольшим префиксом и маской подсети, затем найдите соответствующий RP-SET в этом управляемом домене на основе префикса и маски подсети группы, после чего вычислите RP.

Шаги для настройки управления доменами включают в себя настройку диапазона локальных управляемых мультимедийных групп на граничном устройстве управления ZBR и настройку резервного BSR внутри управляемого домена.

Пример настройки

1. На устройстве ZBR настройте диапазон адресов управляемого домена:

   Sa_config_v9#ip pim-sm admin-scope 225.1.1.0 255.255.255.0

2. Настройте границы группы и порт резервного BSR на доменном устройстве PIM-SM:

   Sb_config#interface loopback1

   Sb_config_l1#ip addr 1.1.1.1 255.255.255.0

   Sb_config_l1#ip pim-sm

   Sb_config#router pim-sm

Sb_config_ps#c-bsr admin-scope 225.1.1.0 255.255.255.0 30 200

Sb_config_ps#c-bsr loopback1 32 250

Значения 30 и 32 задают длину маски хэша, а 200 и 250 – приоритет резервного BSR. Если есть несоответствие, то используется значение, заданное при настройке резервного BSR, а не при настройке управляемого домена.

51.5.2.10 Настройка адреса источника зарегистрированных пакетов

По умолчанию, когда функция регистрации пакетов данных многоадресной рассылки активирована на назначенном маршрутизаторе DR, его адрес становится исходным адресом для всех зарегистрированных пакетов. Однако мы имеем возможность выбрать любой активный интерфейс с PIM-SM на этом устройстве и использовать его адрес в качестве исходного адреса для зарегистрированных пакетов.

Пример настройки

Sb_config#interface loopback1

Sb_config_l1#ip addr 1.1.1.1 255.255.255.0

Sb_config_l1#ip pim-sm

Sb_config#router pim-sm

Sb_config_ps# reg-src loopback1

В этом примере основной адрес интерфейса loopback1 назначается в качестве адреса источника зарегистрированных пакетов.

51.5.2.11 Настройка Anycast-RP

У отдельного RP большая нагрузка в домене PIM-SM. Чтобы снизить эту нагрузку, можно назначить несколько одинаковых RP. Источник многоадресной рассылки и получатель будут пересылать зарегистрированные пакеты и запросы на присоединение, базируясь на самом свежем RP.

Если в системе не использован модуль MSDP (Multicast Source Discovery Protocol), адрес соседа Anycast-RP и адрес порта, выступающего в роли RP, должны быть явно указаны при настройке Anycast-RP. При этом, соседний адрес и адрес порта, функционирующего как RP, не могут быть одинаковыми.

51.5.2.12 Отображение локальных записей маршрутизации PIM-SM

Если вы хотите отобразить информацию о многоадресной маршрутизации PIM-SM, вы можете использовать команду **show ip mroute pim-sm** в режиме управления:

Команда	Описание

show ip mroute pim-sm [*group-address*] [*source-address*]	Отображает информацию о многоадресной маршрутизации PIM-SM. *group-address* – адрес группы; *source-address* – адрес источника

Пример настройки

switch# show ip mroute pim-sm

IP PIM-SM Multicast Routing Table:

(source, group) RP Uptimer/Expires Flags

(*, 225.1.1.10), 9.1.1.1, 00:15:14/00:02:37,JOIN|IGMP

Upstream interface: VLAN5, RPF nbr 192.168.100.143

Downstream interface list:

VLAN2, 00:13:23/00:02:37

(192.166.1.253, 225.1.1.10), 00:15:14/00:02:46 JOIN|IGMP

Upstream interface: VLAN5, RPF nbr 192.168.100.143

Downstream interface list:

VLAN2, 00:15:14/00:02:46

51.5.2.13 Очистка записей маршрутизации PIM-SM

Если необходимо очистить информацию о многоадресной маршрутизации, сохраненную в таблице маршрутизатора PIM-SM, используйте следующую команду в режиме управления:

Команда	Описание
clear ip mroute pim-sm [***** | *group-address*] [*source-address*]	При возникновении ошибок очищает информацию многоадресной маршрутизации, сохраненную на устройстве. ***** – удаляет все многоадресные маршруты, созданные PIM-SM; *group-address* – удаляет многоадресную маршрутизацию связанной группы; *source-address* – удаляет многоадресный маршрут соответствующего источника

Примеры настройки

1. В примере показано, как очистить в MRT все маршруты, созданные PIM-SM на локальном восходящем порту.

```
switch# clear ip mroute pim-sm *
```

2. В примере показано, как очистить в MRT все маршруты, созданные PIM-SM на локальном восходящем порту, групповой адрес которых равен 239.1.1.1.

```
switch# clear ip mroute pim-sm 239.1.1.1
```

3. В примере показано, как удалить записи о маршруте многоадресного трафика до группы 239.1.1.1 через RP 192.168.20.131 из таблицы многоадресной маршрутизации.

```
switch# clear ip mroute pim-sm 239.1.1.1 192.168.20.131
```

51.5.2.14 Отслеживание отладочной информации PIM-SM

Если вы хотите отслеживать пакеты PIM-SM и информацию о его состоянии, вы можете использовать команду **debug ip pim-sm** в режиме управления:

Команда	Описание
debug ip pim-sm [**hello**|**jp**|**register**|**assert**|**bsr**|**timer**] [**packet**]	Отслеживает изменения состояния маршрутизатора PIM-SM, а также отправку и получение пакетов.

Примеры настройки

1. Отслеживание взаимодействия пакетов приветствия:

```
switch# debug ip pim-sm hello
2023-4-21 16:44:00 PIM-SM: VLAN5, Rcv Hello Msg, Source = 192.168.100.143,
Destination = 224.0.0.13, len = 34
2023-4-21 16:44:07 PIM-SM: VLAN5, Send Hello Msg, Destination = 224.0.0.13, len =
34
2023-4-21 16:44:08 PIM-SM: VLAN2, Send Hello Msg, Destination = 224.0.0.13, len =
34
2023-4-21 16:44:10 PIM-SM: VLAN2, Rcv Hello Msg, Source = 192.168.21.144,
Destination = 224.0.0.13, len = 34
```

2. Отслеживание взаимодействия пакетов присоединения/выхода и изменения статуса:

```
switch#debug ip pim-sm jp
switch#PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 224.2.127.254
SM state = PS_ST_JP_NI, ev = PS_EV_JP_JOIN.
PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 224.2.127.254
SM state = PS_ST_JP_J, ev = PS_EV_JP_PRUNE.
PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 239.255.255.250
SM state = PS_ST_JP_NI, ev = PS_EV_JP_JOIN.
PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 239.255.255.250
SM state = PS_ST_JP_J, ev = PS_EV_JP_PRUNE.
2023-4-21 16:48:52 PIM-SM: VLAN5, Rcv J/P Msg, Source = 192.168.100.143,
Destination = 224.0.0.13, len = 42
PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 225.1.1.10
SM state = PS_ST_JP_NI, ev = PS_EV_JP_JOIN.
```

3. Отслеживание взаимодействия зарегистрированных пакетов и изменения статуса.

```
S142#debug ip pim-sm register
S142#2003-4-21 16:52:19 Line protocol on Interface VLAN5, changed state to up
2003-4-21 16:52:29 PIM-SM: VLAN5, Rcv Register Msg, Source = 192.168.100.143,
Destination = 192.166.100.142, len = 57
2023-4-21 16:52:29 PIM-SM: VLAN5 Rcv Register Msg, Source = 192.168.100.143,
Destination = 192.166.100.142, len = 57
```

51.5.3 Примеры настройки

51.5.3.1 Типовая топология PIM-SM

На рисунке 51-2 изображена простая стандартная топология PIM-SM.

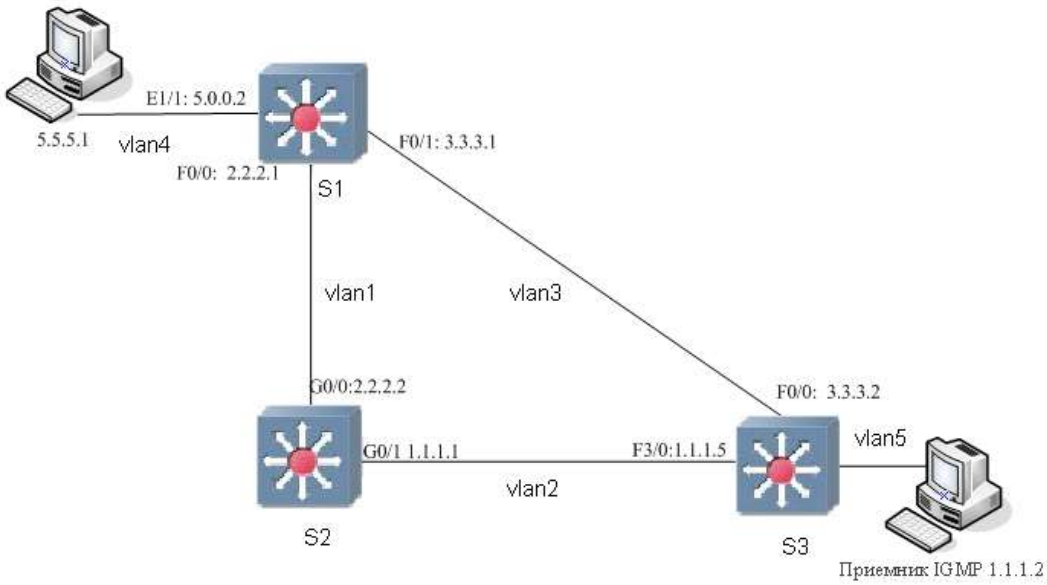

Рисунок 51-2 – Простая топология PIM-SM

1. Включите функцию многоадресной пересылки на всех маршрутизаторах:

   switch_config#ip multicast-routing

2. Настройте протокол PIM-SM на всех портах для многоадресной пересылки:

Настройка на примере коммутатора S1:

   S1_config_v4#ip pim-sm

   S1_config_v3#ip pim-sm

   S1_config_v1#ip pim-sm

3. Настройте RP.

3.1 Для динамического RP достаточно настроить только на тот маршрутизатор, который отвечает за C-BSR и C-RP. Настраивать C-BSR и C-RP на одной машине не обязательно.

В данном примере для функционирования в качестве C-BSR и C-RP выбран маршрутизатор S2. Первоначально необходимо настроить IP-адрес.

   S2_config_l0#ip add 6.6.6.6 255.255.255.0

   S2_config_l0# ip pim-s

S2_config#router pim-sm

S2_config_ps#c-bsr loopback0

S2_config_ps#c-rp loopback0

3.2 Для статического RP необходимо указать доступный RP-адрес на каждом PIM-маршрутизаторе. Порт с RP-адресом должен быть настроен с помощью PIM-SM:

Настройка на S2 следующая:

S2_config_l0#ip add 6.6.6.6 255.255.255.0

S2_config_l0# ip pim-s

S2_config_ps#static-rp 6.6.6.6

Only need to configure on S1 and S3:

S1_config_ps#static-rp 6.6.6.6

S3_config_ps#static-rp 6.6.6.6

4. Чтобы включить функцию SSM, весь домен PIM должен быть согласованным:

Модель SSM нуждается в поддержке IGMPv3, поэтому убедитесь, что функция IGMPv3 включена на устройстве PIM-SM, подключенном к приемнику. Модель SSM реализуется через подмножество функций PIM-SM. Таким образом, система имеет возможности SSM при включении функции PIM-SM. При развертывании домена PIM-SM рекомендуется включить PIM-SM на всех неграничных интерфейсах.

В зависимости от того, находится ли многоадресная группа, на которую подписался получатель (S, G), в диапазоне многоадресных групп, заданных моделью PIM-SSM, или PIM-SM, будет выбрана соответствующая модель. Если на интерфейсах включена поддержка PIM-SM, то многоадресная группа, находящаяся в определенном диапазоне, будет работать с моделью PIM-SSM.

Перед настройкой основных функций PIM-SSM необходимо настроить одноадресную маршрутизацию, чтобы обеспечить совместимость сетевого уровня и доступность маршрутов.

Этапы настройки PIM-SSM следующие:

- Включите PIM-SM на порту.
- Войдите в режим настройки PIM-SM и укажите диапазон адресов группы SSM.
- Настройте другие функции PIM-SM (необязательно).

Пример настройки

switch_config#interface vlan8

switch_config_v8#ip addr 1.1.1.1 255.255.255.0

```
switch_config_v8#ip pim-sm
switch_config_v8#exit
switch_config#router pim-sm
switch_config_ps#ssm rang grp_range
switch_config_ps#exit
switch_config#ip access-list standard grp-range
switch_config_std_nacl#permit 233.1.0.0 255.255.0.0
switch_config_std_nacl#
```

Диапазон группы SSM в приведенной выше конфигурации – это не значение по умолчанию 232.0.0.0/8, а настроенное 233.1.0.0/16. Если вы хотите отменить конфигурацию, связанную с SSM, можно использовать форму «no» команды.

В качестве примера возьмем следующую топологию: на рисунке 51-3 коммутатор S2 – это RP, а S3 – DR в сегменте сети 1.1.1.0.

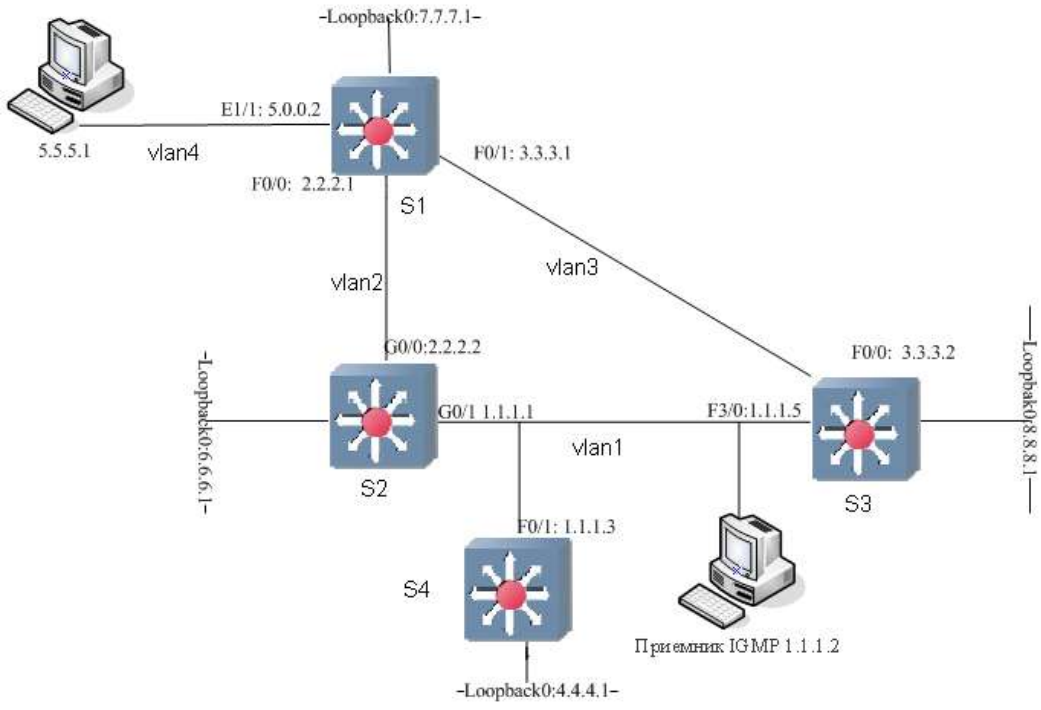

Рисунок 51-3 –Топология SSM

Чтобы использовать функцию SSM для пересылки многоадресного трафика в диапазоне 233.1.0.0/16, необходимо настроить каждый маршрутизатор во всем домене PIM-SM. В данном примере это узлы S1, S2, S3 и S4.

switch_config#router pim-sm

switch_config_ps#ssm rang grp_range

switch_config_ps#exit

switch_config#ip access-list standard grp-range

switch_config_std_nacl#permit 233.1.0.0 255.255.0.0

Приемник IGMP с IP-адресом 1.1.1.2 отправляет отчет IGMP v3. Когда в этом отчете указана группа (5.5.5.1, 233.1.0.1), маршрутизатор S3 (DR) в данной локальной сети присоединяется к источнику (5.5.5.1) напрямую, а не к RP. Это означает, что всякий раз, когда маршрутизатор S1 получает пакет с адресом (5.5.5.1, 233.1.0.1), он напрямую пересылает пакет по уже установленному дереву SPT, без необходимости регистрироваться у RP. Это улучшает эффективность, так как сокращаются расходы на регистрацию и для пересылки используется SPT-дерево.

Если отчет, отправленный приемником IGMP 1.1.1.2, имеет вид (*, 233.1.0.1), он не обрабатывается, потому что этот групповой адрес находится в диапазоне SSM, и обрабатываются только отчеты от указанного источника.

51.5.3.2 Смешение мультипротокольной многоадресной рассылки

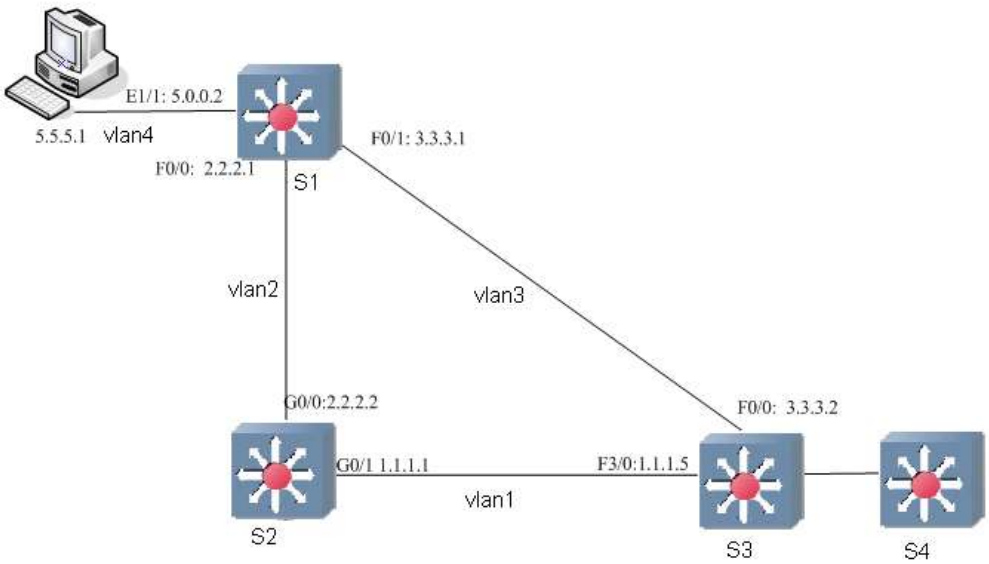

Рисунок 51-4 –Мультипротокольная рассылка

В схеме, изображенной на рисунке 51-4, настройка IP PIM-SM выполняется на VLAN1 и VLAN3 маршрутизатора S3, в то время как IP PIM-DM настраивается на VLAN4 маршрутизатора S1. Маршрутизатор S3 выполняет функцию граничного маршрутизатора (PMBR) между доменами PIM-SM и PIM-DM.

Важно отметить, что S3 создает записи (** RP) для каждого RP. Весь трафик групп, использующих адрес RP в домене PIM-SM, направляется по записи (** RP) к S3 и затем пересылается к S4. Поэтому при использовании смешанной конфигурации (когда одновременно используются PIM-SM и PIM-DM), нельзя одновременно использовать функцию SSM.

52. Настройка IPv6

Настройка IPv6-адреса действительна только на интерфейсе VLAN, а не на физическом интерфейсе.

По умолчанию протокол IPv6 отключен. Если протокол необходимо использовать на интерфейсе VLAN, его следует сначала включить в режиме настройки интерфейса VLAN. Для этого необходимо настроить адрес IPv6. Если на интерфейсе VLAN установлен хотя бы один адрес IPv6, интерфейс может обрабатывать соответствующие пакеты и обмениваться данными с другими устройствами IPv6.

52.1 Включение IPv6

52.1.1 Настройка IPv6-адреса

Адрес IPv6 используется для определения адреса назначения, на который могут быть отправлены IPv6-пакеты. Существует три типа адресов IPv6:

Тип	Формат	Описание
Одноадресный	2001:0:0:0:0DB8:800:200C:417A/64	**2001:0:0:0:0DB8:800:200C:417A** обозначает адрес для одноадресной рассылки, а **64** – длину префикса этого адреса
Многоадресный	FF01:0:0:0:0:0:0:101	Все адреса многоадресной рассылки начинаются с **FF**
Любой	2002:0:0:0:0DB8:800:200C:417A/64	Формат этого адреса такой же, как и у одноадресного. Разные интерфейсы VLAN могут иметь один и тот же адрес, независимо от того, является ли он одноадресным / широковещательным / многоадресным

Дополнительные сведения об адресе IPv6 см. в RFC 4291.

Чтобы включить IPv6, необходимо установить юникастовый адрес в режиме настройки интерфейса VLAN. Адрес должен представлять собой один или несколько адресов следующего типа:

- локальный адрес канала IPv6;
- глобальный IPv6-адрес.

Чтобы установить локальный адрес канала IPv6, в режиме настройки интерфейса VLAN выполните следующие команды:

Команда	Описание
ipv6 enable	Устанавливает локальный адрес автоматически
ipv6 address fe80::x link-local	Устанавливает локальный адрес вручную

- Локальный адрес канала должен начинаться с fe80. Длина префикса по умолчанию составляет 64 бита. При ручных настройках можно указать только значения последних 64 бит.
- На интерфейсе VLAN можно установить только один локальный адрес.
- После включения протокола IPv6 с помощью команды **ipv6 address link-local**, он действует только на локальном канале (в пределах подсети).

52.2 Настройка служб IPv6

После включения IPv6 можно настроить все службы, предоставляемые IPv6 для контроля и управления каналом. Задачи настройки следующие:

1. Установка MTU IPv6;
2. Установка частоты передачи пакета ICMPv6;
3. Настройка уведомлений о недоступности целевого узла IPv6;
4. Настройка ACL IPv6.

52.2.1 Установка MTU IPv6

Все интерфейсы имеют MTU IPv6 по умолчанию. Если длина пакета IPv6 превышает MTU, маршрутизатор фрагментирует этот пакет.

Чтобы установить MTU на определенном интерфейсе, выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
ipv6 mtu *bytes*	Устанавливает MTU на интерфейсе IPv6

52.2.2 Настройка перенаправления IPv6

Иногда маршрут, выбранный хостом, оказывается не самым оптимальным. В этом случае, когда коммутатор получит пакет по этому маршруту, он передаст в соответствии с таблицей маршрутизации пакет с интерфейса, на котором пакет получен, и перенаправит его другому маршрутизатору, принадлежащему тому же сегменту сети, в котором находится хост. При этом перенаправление пакета происходит не через сам коммутатор, а напрямую к другому маршрутизатору. Этот процесс требует от исходного хоста заменить изначальный маршрут на более прямой, который указан в пакете перенаправления.

IPv6-перенаправление по умолчанию включено. Однако, если на интерфейсе настроен протокол горячего резервирования маршрутизатора, IPv6-перенаправление автоматически отключается. Если протокол горячего резервирования маршрутизатора отменен, функция IPv6-перенаправления не включится снова автоматически.

Для включения перенаправления IPv6 выполните следующую команду:

Команда	Описание
ipv6 redirects	Позволяет IPv6 передавать пакеты перенаправления

52.2.3 Настройка уведомлений о недоступности целевого узла IPv6.

В большинстве случаев система автоматически будет отправлять сообщения об ошибке обратно к отправителю пакетов, которые не могут быть доставлены до указанного адреса или узла. Это помогает отправителю понять, что целевой узел недоступен, и принять соответствующие меры. Пользователи могут выключить эту функцию. Если она выключена, система не будет передавать такие пакеты ICMP.

Чтобы включить эту функцию, выполните следующую команду:

Команда	Описание
ipv6 unreachables	Включает отправку сообщений о недоступности целевого узла обратно к отправителю недоставленных пакетов IPv6

52.2.4 Настройка ACL IPv6

Пользователи могут использовать ACL для управления приемом и передачей пакетов на интерфейсе VLAN. Если вы введете имя ACL на интерфейсе VLAN в режиме глобальной конфигурации и укажете направление фильтрации, пакеты IPv6 будут фильтроваться на этом интерфейсе VLAN.

Чтобы отфильтровать пакеты IPv6, выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
ipv6 access-group *WORD* {**in** | **out**}	Фильтрует входящие/исходящие пакеты IPv6 на интерфейсе VLAN

53. Настройка ND

53.1 Обзор

Узел (хост и маршрутизатор) использует протокол обнаружения соседей ND (Neighbor Discovery protocol) для определения адресов канального уровня подключенных соседей и быстрого удаления недействительного кэша. Хост также использует соседа для обнаружения соседних маршрутизаторов, пересылающих пакеты. Кроме того, узел использует механизм ND для точного отслеживания того, какие соседи доступны или недоступны, а также для проверки измененного адреса канального уровня. Когда у маршрутизатора или на пути к маршрутизатору возникают проблемы, хост обязательно ищет другой работающий маршрутизатор или другой путь.

IPv6 ND выполняет функции, аналогичные функциям протоколов ARP, ICMP Router Discovery и ICMP Redirect в IPv4. В IPv4 нет аналогичного механизма и протокола для обнаружения недоступности соседей.

IPv6 ND поддерживает различные типы сетей, включая точка-точка (P2P), мультикаст, сети с несколькими активными узлами (NBMA), сети с общим каналом, а также изменяемый размер MTU и асимметричную доступность. Механизм ND выполняет следующие функции:

1. **Поиск маршрутизаторов**: алгоритм нахождения маршрутизаторов в сети для обеспечения связи с другими сегментами сети.
2. **Поиск префиксов**: алгоритм определения набора адресных префиксов, которые указывают, какие адреса активны в текущем сегменте сети.
3. **Поиск параметров**: алгоритм получения информации о параметрах, связанных с текущим сегментом сети, таких как MTU и другие настройки.
4. **Автоматическая установка адресов**: алгоритм автоматического назначения узлом IP-адреса для своего интерфейса.
5. **Разрешение адресов**: алгоритм определения MAC-адреса узла, когда известен его IP-адрес.
6. **Определение следующего перехода**: алгоритм, позволяющий узлу определить, какой IP-адрес (будь то маршрутизатор или конечный узел) следует использовать в качестве следующего перехода для доставки пакета к целевому узлу.
7. **Проверка недоступных соседей**: алгоритм определения недоступности соседа. В случае, если этот сосед – маршрутизатор, поиск и выбор нового соседнего маршрутизатора для использования по умолчанию.
8. **Проверка повторяющихся адресов**: алгоритм, гарантирующий, что выбранный узлом адрес не используется другим узлом в сети.

9. **Перенаправление**: алгоритм уведомления хоста о наилучшем следующем переходе для доставки пакета.

53.1.1 Разрешение адресов

Разрешение адресов – это процедура определения адреса канального уровня через IP-адрес узла. Обмен пакетами осуществляется посредством запроса ND и уведомления ND.

- Настройка статического кэша ND

  В большинстве случаев используется динамическое разрешение адресов, и статическая настройка кэша ND не требуется. При необходимости вы можете создать статический кэш ND в глобальном режиме, и система будет использовать его для перевода IP-адреса в MAC-адрес. В следующей таблице показано, как настроить сопоставление статического IP-адреса и адреса канального уровня.

Запустите следующую команду в режиме глобальной конфигурации:

Команда	Описание
ipv6 neighbor *ipv6address* **vlan** *vlanid* **hardware-address**	Создает статический кэш ND и преобразует адрес IPv6 в адрес канального уровня

54. OSPFv3

54.1 Обзор

OSPFv3 – это протокол маршрутизации IGP, разработанный рабочей группой OSPF IETF для сети IPv6. OSPFv3 поддерживает подсеть IPv6, метку внешней маршрутной информации и аутентификацию пакетов.

OSPFv3 и OSPFv2 имеют много общего:

- идентификатор маршрутизатора и идентификатор области являются 32-битными;
- одинаковые типы пакетов: Hello, DD, LSR, LSU и LSAck;
- наличие одного и того же механизма обнаружения соседей и построения соседских отношений;
- Наличие одинакового механизма расширения и устаревания LSA.

Основные различия OSPFv3 и OSPFv2 показаны ниже:

- OSPFv3 работает на основе канала, а OSPFv2 – на основе сегмента сети.
- OSPFv3 может запускать несколько экземпляров по одному и тому же каналу.
- OSPFv3 маркирует своего соседа по идентификатору маршрутизатора, а OSPFv2 – по IP.
- OSPFv3 определяет 7 классов LSA.

В следующей таблице показаны некоторые ключевые функции реализации OSPFv3:

Функция	Описание
Тупиковый домен	Поддержка области типа Stub
Перераспределение маршрутов	Означает, что маршруты, полученные или созданные любым протоколом маршрутизации, могут быть перенаправлены в домены других протоколов маршрутизации. В автономном домене это означает, что OSPFv3 может вводить изученные маршруты RIP. Маршруты, изученные OSPFv3, также можно экспортировать в RIP. Между автономными доменами OSPFv3 может импортировать маршруты, изученные BGP; Маршруты OSPFv3 также можно экспортировать в BGP
Параметры интерфейса маршрутизации	Ниже приведены настраиваемые параметры интерфейса: стоимость вывода, интервал повторной передачи, задержка передачи на интерфейсе, приоритет маршрутизатора, интервал определения завершения работы маршрутизатора, интервал приветствия и ключ аутентификации
Виртуальный канал	Поддерживает виртуальное соединение

54.2 Настройка OSPFv3

OSPFv3 требует переключения данных маршрутизации между внутридоменным маршрутизатором, ABR и ASBR. Чтобы упростить настройки, можно оставить их работать с параметрами по умолчанию без какой-либо аутентификации. Если необходимо изменить определенные настройки, вы должны гарантировать, что параметры на всех маршрутизаторах будут идентичны.

Чтобы настроить OSPFv3, необходимо выполнить следующие задачи. За исключением активации OSPFv3, приведенные ниже настройки не являются обязательными.

Включение OSPFv3

- Настройка параметров интерфейса OSPFv3
- Настройка OSPFv3 в разных физических сетях
- Настройка параметров домена OSPFv3
- Настройка домена NSSA OSPFv3.
- Настройка суммирования маршрутов в домене OSPFv3
- Настройка суммирования пересылаемых маршрутов
- Генерация маршрута по умолчанию
- Выбор идентификатора маршрута на интерфейсе обратной связи
- Установка таймера алгоритма маршрутизации
- Мониторинг и поддержка OSPFv3

54.2.1 Включение OSPFv3

Прежде чем активировать OSPFv3, необходимо включить функцию пересылки пакетов IPv6.

Для включения OSPFv3 необходимо создать процесс маршрутизации OSPFv3, указать идентификатор маршрутизатора этого процесса и включить OSPFv3 на интерфейсе. Выполните следующие команды в режиме глобальной конфигурации:

Команда	Описание
router ospfv3 *process-id*	Активирует OSPFv3 и входит в режим настройки маршрутизатора
router-id *router-id*	Устанавливает идентификатор маршрутизатора, на котором работает OSPFv3

Запустите следующую команду в режиме настройки интерфейса:

Команда	Описание
ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]	Включает OSPFv3 на интерфейсе

Если процесс OSPFv3 не был создан до включения OSPFv3 на интерфейсе, он будет создан автоматически.

54.2.2 Настройка параметров интерфейса OSPFv3

Во время реализации OSPFv3 соответствующие параметры на интерфейсе могут быть изменены в соответствии с фактическими требованиями. Необязательно менять каждый параметр, но следует убедиться, что параметры одинаковы на всех маршрутизаторах в подключенных сетях.

Выполните следующие команды в режиме настройки интерфейса:

Команда	Описание
ipv6 ospf cost *cost*	Устанавливает стоимость пакета, передаваемого из интерфейса OSPFv3
ipv6 ospf retransmit-interval *seconds*	Устанавливает интервал повторной передачи LSA между соседями
ipv6 ospf transmit-delay *seconds*	Устанавливает время задержки для передачи LSA на интерфейсе OSPFv3

ipv6 ospf priority *number*	Устанавливает приоритет маршрутизатора OSPFv3 для выбора DR
ipv6 ospf hello-interval *seconds*	Устанавливает интервал передачи пакетов Hello для интерфейса OSPFv3
ipv6 ospf dead-interval *seconds*	Означает, что в течение регламентированного интервала, если пакеты OSPFv3 не получены от соседнего маршрутизатора, этот соседний маршрутизатор считается отключенным

54.2.3 Настройка OSPFv3 в разных физических сетях

OSPFv3 делит физическую сетевую среду на следующие три типа:

- широковещательные сети (Ethernet, Token Ring, FDDI);
- нешироковещательные сети и сети множественного доступа (SMDS, Frame Relay, X.25);
- сети «точка-точка» (HDLC, PPP).

Сети X.25 и Frame Relay предоставляют дополнительные возможности широковещательной передачи. OSPF можно настроить для работы в широковещательных сетях с помощью map-команд. Информацию о команде **map** см. в описании команд x.25 и Frame Relay в Справочнике команд WAN.

54.2.4 Настройка типа сети OSPFv3

Независимо от того, какой тип физической среды используется в сети, ее можно настроить как широковещательную, нешироковещательную или сеть с множественным доступом. Вы можете настроить вашу сеть гибко, сделав ее нешироковещательной и со множественным доступом, либо как широковещательную, например, как сеть X.25, Frame Relay или SMDS. Кроме того, настройки соседних устройств будут упрощены.

Для настройки нешироковещательной сети и сети со множественным доступом предлагается рассматривать сеть так, будто каждые два маршрутизатора имеют виртуальное соединение или создать сеть полной взаимосвязи. Однако такую схему бывает трудно реализовать из-за высокой стоимости. Вместо этого можно настроить сеть как точка-многоточка, что позволяет маршрутизаторам, не являющимся соседними, передавать маршрутную информацию через виртуальное соединение.

Интерфейс OSPFv3 точка-многоточка может быть настроен как многоточка-точка, что позволяет устанавливать несколько маршрутов для хоста. Сеть типа «точка-многоточка» OSPFv3 по сравнению с нешироковещательной сетью и сетью множественного доступа или сетью точка-точка имеет следующие преимущества:

Сеть точка-многоточка легко настраивается и не требует выбора главного маршрутизатора (DR).

Она не требует сети полной взаимосвязи, что позволяет снизить стоимость создания.

Такие сети более надежны. Даже если виртуальный канал выйдет из строя, соединение можно будет поддерживать.

Тип сети маршрутизаторов – широковещательный.

54.2.5 Настройка параметров домена OSPFv3

Настраиваемые параметры домена включают в себя: аутентификацию, назначение тупиковой зоны и указание веса для суммарного маршрута по умолчанию. Аутентификация основана на защите паролем.

Тупиковая зона (stub area) означает, что внешние маршруты не могут быть распределены в эту область. Вместо этого ABR генерирует внешний маршрут по умолчанию, который входит в тупиковую зону, позволяя ей взаимодействовать с внешними сетями автономной системы. Чтобы использовать функции поддержки тупиковой зоны OSPF, следует использовать в ней маршрут по умолчанию. Чтобы дополнительно уменьшить количество LSA, отправляемых в тупиковую зону, можно запретить сборку маршрутов ABR, чтобы уменьшить отправку в нее сводных LSA (тип 3).

Чтобы настроить параметры домена, запустите следующую команду в режиме настройки маршрутизатора:

Команда	Описание
area *area-id* **stub** [no-summary]	Определяет тупиковую зону
area *area-id* **default-cost** *cost*	Устанавливает метрику для маршрута по умолчанию в тупиковой зоне

Что касается тех областей, которые не являются основными и не имеют прямого подключения к основным областям, или когда области разорваны, для установления логической связи между ними можно использовать виртуальное соединение OSPFv3. Чтобы создать виртуальный канал, вам необходимо выполнить настройку на обоих терминалах этого соединения. Если настроена только одна сторона, виртуальный канал работать не будет.

Для создания виртуального канала запустите следующую команду в режиме настройки маршрутизатора:

Команда	Описание
area *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*] [**hello-interval** *hello-value*] [**retransmit-interval** *retrans-value*] [**transmit-delay** *dly-value*]	Настраивает виртуальный канал

54.2.6 Настройка суммирования маршрутов в домене OSPFv3

С помощью этой функции ABR может транслировать сводный маршрут в другие регионы. В OSPFv3 каждая сеть передается в другие области. Если идентификаторы сетей идут последовательно, то можно настроить ABR так, чтобы он передавал суммарный маршрут другим областям. Суммарный маршрут может охватывать все сети в определенном диапазоне.

Запустите следующую команду в режиме настройки маршрутизатора, чтобы установить диапазон адресов:

Команда	Описание
area *area-id* **range** *ipv6-prefix /prefix-length*	Устанавливает диапазон адресов сводного маршрута

54.2.7 Настройка суммирования пересылаемых маршрутов

Когда маршруты распределяются из других областей маршрутизации в область маршрутизации OSPFv3, каждый маршрут передается отдельно как внешний LSA. Однако вы можете настроить сводный маршрут на маршрутизаторе, чтобы он охватывал диапазон адресов. Это позволяет уменьшить размер базы данных состояния связей OSPFv3 и сделать её более компактной.

Запустите следующую команду в режиме настройки маршрутизатора, чтобы установить сводный маршрут:

Команда	Описание
summary-prefix *ipv6-prefix /prefix-length*	Транслирует только один суммарный маршрут

54.2.8 Генерация маршрута по умолчанию

Можно указать маршрутизатору, работающему как ASBR, создавать маршрут по умолчанию для входа в область маршрутизации OSPFv3. Когда вы настраиваете маршрутизатор для распространения маршрутов в область OSPFv3, этот маршрутизатор автоматически становится ASBR. Однако изначально ASBR не создает маршрут по умолчанию для входа в область маршрутизации OSPFv3. В режиме настройки маршрутизатора используйте следующую команду, чтобы ASBR создавал маршрут по умолчанию:

Команда	Описание
default-information originate [**always**] [**route-map** *map-name*]	Указывает маршрутизатору ASBR создать маршрут по умолчанию, входящий в область маршрутизации OSPFv3

54.2.9 Выбор идентификатора маршрутизатора на интерфейсе Loopback

OSPFv3 использует наибольший адрес IPv6 в качестве идентификатора маршрутизатора. Если интерфейс IPv6, не работает или адрес IPv6 удален, процесс OSPF пересчитает идентификатор этого маршрутизатора и повторно передаст информацию о маршрутизации со всех интерфейсов.

Если на интерфейсе обратной связи (loopback) настроен IP-адрес, маршрутизатор сразу будет использовать этот адрес в качестве своего идентификатора. Поскольку интерфейс loopback никогда не отключается, таблица маршрутизации очень стабильна.

Маршрутизатор предпочтительно использует loopback-интерфейс в качестве идентификатора маршрутизатора, при этом в качестве идентификатора маршрутизатора выбирает самый большой IP-адрес среди всех loopback-интерфейсов. Если интерфейс обратной связи отсутствует, используется наибольший IPv6-адрес маршрутизатора. Вы не можете указать OSPFv3 использовать какой-либо конкретный интерфейс.

Выполните следующие команды в режиме глобальной конфигурации, чтобы настроить интерфейс обратной связи:

Команда	Описание
interface loopback *num*	Создает интерфейс loopback и входит в режим настройки интерфейса
ip address *ip-address mask*	Назначает IP-адрес для интерфейса

54.2.10 Установка таймера алгоритма маршрутизации

Вы можете настроить временную задержку между моментом получения OSPFv3 информации о топологических изменениях и началом расчета таблицы маршрутизации по алгоритму SPF. Также можно настроить интервал между двумя последовательными расчетами SPF. В режиме настройки маршрутизатора используйте следующие команды:

Команда	Описание
timers delay *delaytime*	Устанавливает задержку начала расчета маршрута после получения данных
timers hold *holdtime*	Устанавливает минимальный временной интервал между двумя последовательными расчетами SPF

54.2.11 Мониторинг и поддержка OSPFv3

Информация сетевой статистики, которая может быть отображена, включает содержимое таблицы IP-маршрутизации, кэширования и базы данных. Информация такого рода может помочь пользователям оценить использование сетевых ресурсов и решить сетевые проблемы.

Для отображения всех видов информации о статистике маршрутизации используются следующие команды:

Команда	Описание
show ipv6 ospf [*process-id*]	Отображает общую информацию о процессе маршрутизации OSPFv3
show ipv6 ospf [*process-id*] **database** **show ipv6 ospf** [*process-id*] **database** [**router**] [**adv-router** *router-id*] **show ipv6 ospf** [*process-id*] **database** [**network**] [**adv-router** *router-id*] **show ipv6 ospf** [*process-id*] **database** [**inter-prefix**] [**adv-router** *router-id*] **show ipv6 ospf** [*process-id*] **database** [**inter-router**] [**adv-router** *router-id*] **show ipv6 ospf** [*process-id*] **database** [**external**] [**adv-router** *router-id*] **show ipv6 ospf** [*process-id*] **database** [**link**] [**adv-router** *router-id*] **show ipv6 ospf** [*process-id*] **database** [**intra-prefix**] [**adv-router** *router-id*]	Отображает информацию о базе данных OSPFv3
show ipv6 ospf interface	Отображает информацию об интерфейсе OSPFv3
show ipv6 ospf neighbor	Отображает информацию о соседях OSPFv3
show ipv6 ospf route	Отображает информацию о маршрутизации OSPFv3
show ipv6 ospf topology	Отображает топологию OSPFv3
show ipv6 ospf virtual-links	Отображает виртуальные каналы OSPFv3
debug ipv6 ospf	Отслеживает все поведение OSPFv3
debug ipv6 ospf events	Отслеживает события OSPFv3
debug ipv6 ospf ifsm	Отслеживает изменения состояний интерфейса OSPFv3
debug ipv6 ospf lsa	Отслеживает связанное с LSA поведение OSPFv3
debug ipv6 ospf nfsm	Отслеживает изменения состояний соседей OSPFv3
debug ipv6 ospf nsm	Отслеживает информацию, о которой модуль управления уведомляет OSPFv3
debug ipv6 ospf packet	Отслеживает пакеты OSPFv3
debug ipv6 ospf route	Отслеживает информацию о маршрутизации OSPFv3

54.3 Примеры настройки OSPFv3

OSPFv3 требует информации о коммутации между многими внутренними маршрутизаторами, ABR и ASBR. При минимальных настройках маршрутизатор на базе OSPFv3 работает с условием, что все его параметры принимают значения по умолчанию и аутентификация отсутствует.

Ниже приведены три примера конфигурации.

В первом примере показаны команды для основных настроек OSPFv3.

Второй пример показывает, что на маршрутизаторе можно установить несколько процессов OSPFv3.

Третий пример показывает, как использовать OSPFv3 для изучения маршрутов.

В четвертом примере показано, как настроить виртуальный канал OSPFv3.

54.3.1 Пример базовой конфигурации OSPFv3

В следующем примере показаны простые настройки OSPFv3. В этом примере необходимо активировать процесс 90, подключить vlan 10 к области 0.0.0.0 и перенаправить OSPFv3 на RIPng.

```
ipv6 unicast-routing
!
interface vlan 10
  ipv6 address 2001::1/64
  ipv6 enable
  ipv6 ospf 90 area 0
  ipv6 ospf cost 1
!
router ospfv3 90
  router-id 1.1.1.1
  redistribute rip 1
!
router ripng 1
  redistribute ospf 90
```

54.3.2 Настройка нескольких процессов OSPFv3.

В следующем примере показано, как создаются два процесса OSPFv3.

```
ipv6 unicast-routing
!
interface vlan 10
  ipv6 address 2001::1/64
  ipv6 enable
  ipv6 ospf 109 area 0 instance 1
  ipv6 ospf 110 area 0 instance 2
!
!
interface vlan 11
  ipv6 address 2002::1/64
   ipv6 enable
  ipv6 ospf 109 area 1 instance 1
  ipv6 ospf 110 area 1 instance 2
!
!
router ospfv3 109
  router-id 1.1.1.1
  redistribute static
!
router ospfv3 110
  router-id 2.2.2.2
!
```

Каждый интерфейс может принадлежать многим процессам OSPFv3, но, если интерфейс принадлежит нескольким процессам, каждый процесс OSPFv3 должен соответствовать разным экземплярам.

54.3.3 Пример сложной конфигурации

В следующем примере показано, как настроить несколько маршрутизаторов в одной автономной системе OSPFv3. На рисунке 54-1 показана топология сети:

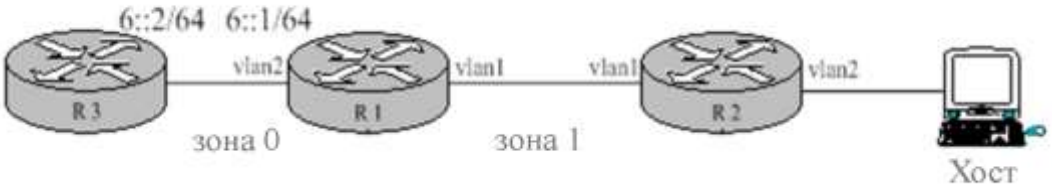

Рисунок 54-1 – Топология OSPFv3

Настройки на маршрутизаторе R1:

```
interface vlan 1
  ipv6 enable
ipv6 ospf 1 area 1
!
interface vlan 2
  ipv6 enable
ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
 router-id 1.1.1.1
redistribute static
!
```

Настройки на маршрутизаторе R2:

```
interface vlan 1
  ipv6 enable
ipv6 ospf 1 area 1
!
!
```

```
router ospfv3 1
 router-id 2.2.2.2
!
```

Просмотр таблицы маршрутизации R2:

```
R2#show ipv6 route
O     6::/64[1]
      [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
O     2001::/64[1]  (Forwarding route )
      [110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
C     fe80::/10[1]
      is directly connected, L,Null0
C     fe80::/64[1]
      is directly connected, C, VLAN1
C     fe80::2e0:fff:fe26:a8/128[1]
      is directly connected, L, VLAN1
C     ff00::/8[1]
      is directly connected, L,Null0
```

Из приведенных выше строк мы видим, что R2 научился переадресации маршрутов.

Настройка зоны 1 в качестве тупиковой области

Настройки на маршрутизаторе R1:

```
interface vlan 1
  ipv6 enable
ipv6 ospf 1 area 1
!
interface vlan 2
  ipv6 enable
ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
```

```
!
router ospfv3 1
 router-id 1.1.1.1
 area 1 stub
redistribute static
!
```

Настройки на маршрутизаторе R2:

```
interface vlan 1
  ipv6 enable
ipv6 ospf 1 area 1
!
!
router ospfv3 1
 router-id 2.2.2.2
 area 1 stub
!
```

Просмотр таблицы маршрутизации R2:

```
R2#show ipv6 route
O     ::/0[1]
      [110,11] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
O     6::/64[1]
      [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
C     fe80::/10[1]
      is directly connected, L,Null0
C     fe80::/64[1]
      is directly connected, C, VLAN1
C     fe80::2e0:fff:fe26:a8/128[1]
      is directly connected, L, VLAN1
C     ff00::/8[1]
      is directly connected, L,Null0
```

Можно считать, что ABR в тупиковой зоне в состоянии нормально генерировать маршрут по умолчанию и уведомлять другие маршрутизаторы в этой области без импорта в нее ASE LS.

54.3.4 Настройка виртуального канала

В следующем примере показано, как настроить виртуальный канал в одной автономной системе OSPFv3. На рисунке 54-2 показана топология сети:

Рисунок 54-2 – Топология OSPFv3

Настройки на маршрутизаторе R1:

```
interface vlan 1
ipv6 address 101::1/64
  ipv6 enable
ipv6 ospf 1 area 1
!
interface vlan 2
ipv6 address 6::1/64
  ipv6 enable
ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
 router-id 200.200.200.1
 area 1 virtual-link 200.200.200.2
 redistribute static
```

```
!
```

Настройки на маршрутизаторе R2:

```
interface vlan 1
ipv6 address 101::2/64
  ipv6 enable
ipv6 ospf 1 area 1
!
interface vlan 2
ipv6 address 888::8/64
  ipv6 enable
ipv6 ospf 1 area 2
!
!
router ospfv3 1
 router-id 200.200.200.2
 area 1 virtual-link 200.200.200.1
!
```

Просмотр состояния соседа OSPFv3:

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State          Dead Time   Interface  Instance ID
200.200.200.2     1   Full/DR        00:00:35    VLAN1      0
200.200.200.2     1   Full/ -        00:00:36    VLINK1     0

R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
OSPFv3 Process (1)
Neighbor ID     Pri   State          Dead Time   Interface  Instance ID
200.200.200.1     1   Full/Backup    00:00:36    VLAN1      0
200.200.200.1     1   Full/ -        00:00:37    VLINK1     0
```

Просмотр информации в таблицах маршрутизации:

R1#show ipv6 route

C 6::/64[1]

is directly connected, C,VLAN2

C 6::1/128[1]

is directly connected, L, VLAN2

C 101::/64[2]

is directly connected, C, VLAN1

C 101::1/128[2]

is directly connected, L, VLAN1

O 101::2/128[2]

[110,10] via fe80:4::2e0:fff:fe26:a8(on VLAN1)

O 888::/64[2]

[110,20] via fe80:4::2e0:fff:fe26:a8(on VLAN1)

S 2001::/64[1]

[1,0] via 6::2(on VLAN2)

C fe80::/10[2]

is directly connected, L,Null0

C fe80::/64[2]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:2d98/128[2]

is directly connected, L, VLAN1

C fe80::/64[1]

is directly connected, C, VLAN2

C fe80::2e0:fff:fe26:2d99/128[1]

is directly connected, L, VLAN2

C ff00::/8[2]

is directly connected, L,Null0

R2#show ipv6 route

O 6::/64[1]

[110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C 101::/64[1]

is directly connected, C, VLAN1

O 101::1/128[1]

[110,10] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C 101::2/128[1]

is directly connected, L, VLAN1

C 888::/64[1]

is directly connected, C, VLAN2

C 888::8/128[1]

is directly connected, L, VLAN2

O 2001::/64[1]

[110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C fe80::/10[1]

is directly connected, L,Null0

C fe80::/64[1]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:a8/128[1]

is directly connected, L, VLAN1

C fe80::/64[1]

is directly connected, C, VLAN2

C fe80::2e0:fff:fe26:a9/128[1]

is directly connected, L, VLAN2

C ff00::/8[1]

is directly connected, L,Null0

55. Настройка NTP

55.1 Обзор

Протокол сетевого времени (NTP) – это тип протокола, который можно использовать для синхронизации системного времени между распределенными серверами времени и клиентами. Он имеет высокоточную функцию коррекции времени и может предотвратить атаки вредоносных программ посредством зашифрованной аутентификации. Клиенты и

серверы обмениваются данными при помощи протокола пользовательских дейтаграмм (UDP) через порт 123.

55.2 Настройка оборудования в качестве NTP-сервера

Режим настройки: глобальный.

Команда	Описание
ntp master primary	Если оборудование не имеет NTP-сервера верхнего уровня, настраивает оборудование как исходный NTP-сервер (уровень = 1)
ntp master secondary	Если оборудование имеет NTP-сервер верхнего уровня, настраивает это оборудование в качестве вторичного NTP-сервера. Таким образом, оборудование не может предоставлять услугу синхронизации времени для клиентов NTP, если не настроена команда **ntp server** и синхронизация времени не достигнута на назначенных серверах

55.3 Настройка функции аутентификации NTP

Режим настройки: глобальный.

Команда	Описание
ntp authentication enable	Включает функцию аутентификации (по умолчанию отключена)
ntp authentication key *keyid* **md5** *password*	Настраивает идентификатор ключа аутентификации NTP md5 и соответствующие ключи
ntp authentication trusted-key *keyid*	Настраивает ключи, соответствующие идентификатору, в качестве доверенных ключей

55.4 Настройка ассоциации NTP

Режим настройки: глобальный.

Команда	Описание
ntp server *ip-address* [**version** *number* | **key** *keyid*]	Настраивает IP-адрес NTP-сервера; номер версии, номер ключа

ntp peer *ip-address* [**version** *number* | **key** *keyid*]	Устанавливает синхронизацию времени между текущим устройством и устройством, указанным по его IP-адресу, с возможностью указать версию протокола и ключ аутентификации, если это необходимо

Рекомендации по использованию:

1. Оборудование может предоставлять услуги синхронизации времени для клиентов NTP при условии, что оно само синхронизировано; в противном случае клиентское устройство, которое использует это оборудование в качестве своего сервера, не сможет достичь точной синхронизации.

2. Для проведения аутентификации NTP обе стороны должны одновременно включить функцию аутентификации NTP, настроить один и тот же идентификатор ключа и пароль, а также определить идентификатор ключа как доверенный; в противном случае синхронизация времени не удастся.

56. ACL IPv6

56.1 Фильтрация пакетов IPv6

Фильтрация IPv6-пакетов помогает контролировать передачу данных в сети. Этот контроль может ограничивать передачу данных и работу в сети для определенных пользователей или устройств. Для включения или отключения передачи пакетов через определенный порт предоставляется ACL (список контроля доступа). IPv6 ACL позволяет:

- ограничивать передачу пакетов через порт.
- ограничивать доступ к виртуальным терминальным линиям.
- ограничивать обновление маршрутов.

В данной главе описывается, как настраивать списки доступа IPv6 и как их применять.

IPv6 ACL представляет собой хорошо организованный набор правил, которые включают или отключают IPv6-адреса. Программное обеспечение коммутатора будет проверять адреса в соответствии с этими правилами ACL. Первое совпадение определяет, будет ли адрес принят или отклонен. После первого совпадения программное обеспечение прекращает проверку правил, поэтому последовательность условий имеет значение. Если нет ни одного совпадающего правила, адрес будет отклонен.

Для использования списка доступа необходимо:

- настроить ACL, указав его имя и условия;
- применить ACL к порту.

56.2 Настройка ACL IPv6

Используйте строку символов для настройки ACL IPv6.

Стандартный и расширенный ACL не могут быть одинаковыми.

Чтобы настроить ACL IPv6, выполните следующую команду в режиме глобальной конфигурации:

Команда	Описание
IPv6 access-list *name*	Создает список управления доступом IPv6 с именем *name*
{**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]	*protocol* – указание протокола, к которому применяется данное правило. *source-ipv6-prefix/prefix-length* – задание исходного IPv6-префикса и его длины, или можно использовать **any** для любого исходного адреса, или **host** *source-ipv6-address* для конкретного исходного адреса. [*operator* [*port-number*]] – опционально, можно указать оператор и номер порта для дополнительной фильтрации. *destination-ipv6-prefix/prefix-length* – задание целевого IPv6-префикса и его длины, или можно использовать any для любого целевого адреса, или **host** *destination-ipv6-address* для конкретного целевого адреса. [**dscp** *value*] – опционально, можно указать значение Differentiated Services Code Point (DSCP) для фильтрации на основе уровня обслуживания. [**flow-label** *value*] – опционально, можно указать значение метки потока для фильтрации на основе метки потока. [**fragments**] – опционально, разрешает фильтрацию фрагментированных пакетов. [**log**] [**log-input**] [**routing**] – опционально, различные параметры логирования событий, связанных с этим правилом. [**sequence** *value*] – опционально, задает порядковый номер для правила в списке.

	[**time-range** *name*] – опционально, можно связать правило с временным диапазоном
exit	Выход из режима настройки ACL

Если ACL настроен без указания порядкового номера (sequence value) для правил deny или permit, то новые правила будут автоматически добавляться в конец ACL. Другими словами, можно добавить правила в любую позицию внутри ACL, указав порядковый номер (sequence value) либо в начале, либо в конце правила deny или permit.

Также с помощью команд **no permit** и **no deny** можно удалить определенное правило из ACL, а командой **no sequence** можно удалить правило с определенным порядковым номером непосредственно.

При настройке списков контроля доступа, нужно помнить, что по умолчанию последним правилом в ACL является правило **deny ipv6 any any**. Иными словами, если вы устанавливаете какие-то правила в ACL и не указываете явно правило для запрета всего трафика (как **deny ipv6 any any**), то ACL будет автоматически запрещать все оставшиеся пакеты, которые не соответствуют ни одному из указанных вами правил, используя правило **deny ipv6 any any** в конце.

56.3 Применение ACL к портам

ACL может применяться к одному или нескольким портам. Выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
IPv6 access-group *name*	Применяет ACL к порту

При настройке стандартного входящего ACL проверяется адрес источника пакета после его получения. При расширенном списке ACL коммутатор маршрутизации также проверяет целевой адрес. Если ACL разрешает адрес, программное обеспечение продолжает обрабатывать пакет. Если ACL не разрешает адрес, программное обеспечение отбросит пакет и вернет ICMP-сообщение о недоступности узла.

Если назначенный список ACL отсутствует, прохождение всех пакетов будет разрешено.

56.4 Пример настройки ACL IPv6

В приведенном примере, сначала разрешается подключение к конкретному удаленному хосту с IPv6-адресом A:B:C:D::E (при помощи правила **permit any host A:B:C:D::E sequence 20**).

Затем запрещается подключение к порту SMTP средствами протокола TCP для любого исходного хоста, чей IPv6-префикс равен 255:255:255::/48 (при помощи правила **deny tcp any 255:255:255::/48 eq smtp sequence 10**).

Важно заметить, что порядок следования правил имеет значение: правило с порядковым номером 10 (запрет SMTP) идет перед правилом с порядковым номером 20 (разрешение доступа к конкретному хосту).

В конце примера команда **show ipv6 access-lists mylist** используется для отображения конфигурации ACL с именем «mylist», и вывод показывает последовательность правил в ACL, как описано выше.

```
Switch_config#ipv6 access-list  mylist
Switch_config_ipv6acl#permit any host A:B:C:D::E sequence 20
Switch_config_ipv6acl#deny tcp any 255:255:255::/48 eq 25 sequence 10
Switch_config_ipv6acl#ex
Switch_config#show ipv6 access-lists mylist
ipv6 access-list mylist
  deny tcp any 255:255:255::/48 eq smtp sequence 10
  permit ipv6 any host A:B:C:D::E sequence 20
```

57. Настройка защиты от IP-атак

57.1 Обзор

Чтобы обеспечить рациональное использование пропускной способности сети, в коммутаторах данной серии предусмотрена функция защиты от IP-атак, позволяющая предотвратить захват полосы пропускания сети вредоносным IP-трафиком. Для хостов, которые отправляют большое количество ICMP, IGMP или IP-пакетов в течение определенного периода времени, вводятся ограничения на коммуникацию и отключаются сетевые услуги. Эта настройка может предотвратить проблему перегрузки сети, вызванную вредоносными пакетами, занимающими значительную часть пропускной способности.

Когда количество пакетов IGMP, ICMP или IP, отправленных хостом в течение любого заданного интервала времени, превышает пороговое значение, мы предполагаем, что в сети произошла атака.

Вы можете выбрать типы защиты от атак (ICMP, IGMP или IP), порты приложения и параметры обнаружения атак. В задачи настройки входят:

- настройка типа защиты от IP-атак;
- настройка параметров обнаружения IP-атак.

57.2 Настройка параметров обнаружения IP-атак

Команда	Описание
ip verify log-enable	Включает/отключает системный журнал обнаружения атак
ip verify filter *time*	Когда источник атаки будет идентифицирован, останавливает для него обслуживание. Единица измерения – секунда, время по умолчанию – 180 секунд

57.3 Настройка типа обнаружения IP-атак

Команда	Описание
ip verify icmp ping-flood *value*	Ограничивает прием ping-пакетов. **value** означает порог обнаружения
ip verify icmp ping-sweep *time*	Ограничивает сканирование ping. **time** означает период обнаружения, единица измерения – секунда
ip verify tcp syn-flood *value*	Ограничивает прием TCP-пакетов синхронизации. **value** означает порог обнаружения
ip verify tcp syn-sweep *time*	Ограничивает сканирование TCP SYN-пакетов на порту. **time** означает период обнаружения, единица измерения – секунда
ip verify tcp fin-scan *time*	Ограничивает скрытое FIN-сканирование. **time** означает период обнаружения, единица измерения – секунда
ip verify tcp rst-flood *value*	Ограничивает прием пакетов RST. **value** означает порог обнаружения
ip verify udp udp-flood *value*	Ограничивает прием пакетов UDP. **value** означает порог обнаружения
ip verify udp udp-sweep *time*	Ограничивает сканирование UDP.

	time означает период обнаружения, единица измерения – секунда
ip verify attack Xmas-Tree *time*	Фильтрует атаки сканирования Xmas-Tree. **time** означает период обнаружения, единица измерения – секунда
ip verify attack Null-scan *time*	Фильтрует атаки типа Null-scan. **time** означает период обнаружения, единица измерения – секунда
ip verify attack Land	Фильтрует атаки Land
ip verify attack Smurf	Фильтрует атаки Smurf
ip verify attack WinNuke	Фильтрует атаки WinNuke
ip verify attack TearDrop	Фильтрует атаки TearDrop
ip verify attack Fraggle	Фильтрует атаки Fraggle

57.4 Включение функции защиты от IP-атак

Когда все параметры защиты от атак настроены, функцию можно активировать. Следует отметить, что функция предотвращения атак забирает определенные ресурсы процессора.

Команда	Описание
ip verify enable	Включает/отключает обнаружение атак

Если применена форма **no** этой команды, обнаружение атак отключается, а все заблокированные источники атак разблокируются.

57.5 Пример настройки защиты от IP-атак

Чтобы включить защиту от сканирования портов, можно настроить систему следующим образом: если какое-либо устройство в сети выполняет сканирование портов слишком часто (более одного раза в 15 секунд), это считается потенциальной атакой, и сетевые услуги будут временно заблокированы на 10 минут, чтобы предотвратить возможные злоумышленные действия.

```
ip verify icmp ping-sweep 15

ip verify tcp syn-sweep 15
```

ip verify udp udp-sweep 15

ip verify enable

ip verify log-enable

ip verify filter 600

58. Защита от IP-атак против непосредственно подключенных сегментов сети

58.1 Обзор

Чтобы злонамеренные атаки не отправляли большое количество пакетов сканирования на маршрут с прямым подключением, коммутатор создает программный кэш для недостижимых адресов в непосредственно подключенных сегментах сети, тем самым увеличивая загрузку ЦП. Функция предотвращения атак на IP-уровне позволяет справляться с такими атаками и снижать нагрузку на процессор.

Если количество неполных запросов ARP на VLAN коммутатора превышает определенное значение, то считается, что коммутатор подвергается атаке в результате сканирования сети. Когда количество недостижимых IP-пакетов в заданный промежуток времени превышает порог, то считается, что произошла атака, и записывается сообщение для предупреждения пользователя.

58.2 Настройка защиты

Пользователь может выбрать режим работы и параметры функции защиты от IP-атак на непосредственно подключенные сетевые сегменты. Задачи настройки включают в себя:

- настройку параметров обнаружения атак
- настройку типов обнаружения атак

Если вы используете команду **ip verify ip-sweep action rate-limit-attacker**, она перезапишет настройки, указанные в команде **ip verify ip-sweep action rate-limit**. Для того чтобы применить настройки из первой команды, вам нужно предварительно выполнить команду **no ip verify ip-sweep action rate-limit-attacker**. Параметры времени и количества пакетов будут унаследованы при перезаписи настроек.

58.2.1 Настройка параметров обнаружения атак

Команда	Описание
ip verify filter *time*	Когда источник атаки идентифицирован, обслуживание источника атаки прекращается. Единица настройки – секунды, время по умолчанию – 180 секунд

58.2.2 Настройка типов обнаружения атак

Команда	Описание
ip verify ip-sweep action rate-limit	Ограничивает количество IP-пакетов
ip verify ip-sweep action rate-limit *time packets*	Ограничивает количество IP-пакетов, настраивается ограниченный период времени и максимальное количество IP-пакетов, разрешенное в этот период
ip verify ip-sweep action rate-limit-attacker	Ограничивает только количество пакетов, определенных как IP-пакеты злоумышленника
ip verify ip-sweep action rate-limit-attacker *time packets*	Ограничивает количество пакетов, определенных как IP-пакеты злоумышленника. Настраивает ограниченный период времени и максимальное количество IP-пакетов, разрешенное для адреса источника за этот период
ip verify ip-sweep action no-cache	Запрещает создание кэша для неизвестных хостов, напрямую подключенных к сегменту сети

58.2.3 Включение защиты от IP-атак против непосредственно подключенных сегментов сети

Когда все параметры настроены, вы можете включить защиту. Следует отметить, что функция предотвращения атак занимает определенный объем процессорного пространства.

Команда	Описание
ip verify ip-sweep detect unknown-host	Включает/отключает функцию защиты от злонамеренного IP-сканирования сети с прямым подключением неизвестными хостами

Если применена форма **no** этой команды, обнаружение атак отключается, а все заблокированные источники атак разблокируются.

58.2.4 Пример настройки защиты от IP-атак против непосредственно подключенных сегментов сети

Для включения предотвращения атак на IP-сети, осуществляемых путем сканирования непосредственно подключенных сегментов сети, можно настроить следующие параметры: обнаруженному атакующему разрешено пересылать всего 200 IP-пакетов каждые две секунды, и кэш сведений о неизвестных устройствах в непосредственно подключенных сетевых сегментах блокируется. Кроме того, результаты тестирования сбрасываются каждые 10 минут.

ip verify filter 600

ip verify ip-sweep detect unknown-host

ip verify ip-sweep action no-cache

ip verify ip-sweep action rate-limit 2 200

Результаты обнаружения выглядят следующим образом:

Jan 1 00:07:14 Unknown-host (connected network sweep) attack detected

Jan 1 00:07:14 Action rate-limit-attacker is being used.

Jan 1 00:07:14 Action no-cache is being used.

Jan 1 00:07:14 Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1

Jan 1 00:07:14 [SLOT 2]Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1

Приведенный выше пример описывает ситуацию, когда включена защита от атак сканирования непосредственных сетевых сегментов, а также методы ограничения скорости и блокировки кэша. В данном случае, произошла атака, при которой сканировался сетевой сегмент с портом vlan 100, физическим портом g2/1 и IP-адресом 100.1.1.2. Требуется рассмотреть эту ситуацию как можно скорее и принять необходимые меры.

59. Временной диапазон

59.1 Введение

59.1.1 Обзор

Временной диапазон (Time Range), – это модуль, который контролирует время действия и время сбоя функции (например, расширенного списка контроля доступа по IP).

Временной диапазон может выполнять свои функции только в том случае, если он взаимодействует с другими модулями, поддерживающими функцию временного диапазона.

Временной диапазон Time Range состоит из отдельных временных диапазонов, или интервалов, которые бывают двух видов: абсолютные и периодические. Периодические временные диапазоны дополнительно подразделяются на изолированные и диапазоны с определенным началом и концом.

Вся система содержит множество временных диапазонов. Каждый отличается по своему имени (с учетом регистра). Любой временной диапазон может иметь не более одного абсолютного временного интервала, но множество периодических.

59.1.2 Абсолютный временной диапазон

Абсолютный временной диапазон – это временной диапазон, начинающийся и заканчивающийся конкретной датой и временем В абсолютном временном диапазоне без конкретной начальной даты и времени за точку отсчета принимается текущее время; абсолютный временной диапазон без конкретного времени окончания считается задействованным навсегда. Например, 08:08 8 8 2023 г. – 10:10 10 10 2025 г. – это абсолютный диапазон.

59.1.3 Периодический временной диапазон

У периодического временного диапазона нет конкретного времени начала и окончания, но есть определенный период действия, повторяющийся в соответствии с днями недели. Например, периодический диапазон начинается с 20:00–21:00 каждый вторник, четверг и воскресенье; или начинается с 09:00 каждого вторника до 18:00 каждого четверга. Или с 09:00 до 10:00 каждые выходные; с 23:00 до 07:00 ежедневно; и с 09:00 до 18:00 по будням.

59.1.4 Изолированный временной диапазон

Изолированный временной диапазон – это один из типов периодического диапазона. Время от его начала до окончания всегда меньше 24 часов. Например, 19:00–19:30 каждый понедельник – это изолированный временной диапазон; 20:00–21:00 каждый вторник, четверг и воскресенье – это изолированный временной диапазон; но время с 09:00 вторника до 18:00 каждого четверга – это не изолированный диапазон, а диапазон времени «от и до», описанный ниже.

59.1.5 Временной диапазон «от и до»

Временной диапазон «от и до» также является разновидностью периодического временного диапазона. При этом время начала и окончания должно составлять не менее 24 часов. Например, время с 09:00 вторника до 18:00 каждого четверга представляет собой диапазон времени «от и до».

59.1.6 Активация временного диапазона

Временной диапазон может одновременно содержать и абсолютный, и периодические интервалы. Состояние временного диапазона можно разделить на 4 ситуации в зависимости от того, настроен ли абсолютный/периодический диапазон.

Ситуация 1

Если временной диапазон не настроен ни как абсолютный, ни как периодический, то такой диапазон считается «пустым» (EMPTY). В этом случае данный диапазон не активен и не имеет определенных временных параметров.

Ситуация 2

Если в рамках временного диапазона абсолютный интервал отсутствует, но есть периодический, то временной диапазон будет активирован в течение всего периода, определенного периодическим интервалом.

Ситуация 3

Если в рамках временного диапазона периодический интервал отсутствует, но есть абсолютный, то временной диапазон будет активирован в течение всего времени, определенного абсолютным интервалом.

Ситуация 4

Если у временного диапазона настроены и абсолютный интервал, и периодические, то активирующее время для данного диапазона будет определено как область, в которой пересекаются все имеющиеся временные интервалы, включая абсолютный и периодические.

Дополнительные области активирующих временных интервалов считаются неактивирующими интервалами.

Если системное время находится в пределах активирующего временного интервала для данного временного диапазона, то этот диапазон считается активным.

Если временной диапазон имеет активный временной интервал, но системное время находится за пределами этого активного интервала, то временной диапазон считается неактивным.

Если временной диапазон вообще не имеет активного временного интервала, то он считается пустым.

Если временный диапазон меняется между состояниями «неактивный», «активный» и «пустой,» то он считается измененным. В противном случае он остается без изменений.

59.2 Настройка временного диапазона

Задачи настройки

- Добавление/удаление временного диапазона
- Добавление/удаление абсолютного временного диапазона
- Добавление/удаление периодического временного диапазона
- Применение временного диапазона
- Мониторинг конфигурации и состояния временного диапазона

59.2.1 Добавление/удаление временного диапазона

Вся система имеет множество временных диапазонов. Каждый временной диапазон различается по имени (с учетом регистра).

Выполните следующие команды, чтобы настроить временной диапазон:

Команда	Описание
time-range *name*	Добавляет временной диапазон с именем *name* и входит в режим его настройки
exit	Выход из режима настройки временного диапазона
no time-range *name*	Удаляет временной диапазон с именем *name*

Если в системе уже есть временной диапазон с именем *name*, команда **time-range name** позволяет войти в режим его настройки, не создавая новый временной диапазон.

59.2.2 Добавление/удаление абсолютного временного диапазона

Каждый временной диапазон имеет не более одного абсолютного временного интервала. Абсолютный диапазон может иметь время начала и время окончания одновременно, или иметь время окончания, но не время начала, или иметь время начала, но не иметь времени окончания. Если абсолютный интервал не имеет начального времени, в качестве начального принимается текущее время; когда не указано конечное время, абсолютный диапазон действует вечно.

Чтобы настроить абсолютный диапазон, выполните следующую команду:

Команда	Описание

absolute {**start** *hour:minute day month year* **end** *hour:minute day month year* | **start** *hour:minute day month year* | **end** *hour:minute day month year*}	Добавляет абсолютный временной диапазон
no absolute	Удаляет абсолютный временной диапазон

Если во временном диапазоне имеется абсолютный интервал, команда **absolute** изменяет его.

59.2.3 Добавление/удаление периодического временного диапазона

Временной диапазон может иметь множество периодических интервалов. Все периодические временные интервалы разные, но их области могут перекрываться.

Чтобы настроить периодическое время, выполните следующую команду:

Команда	Описание
periodic [**daily** *hour:minute* **to** *hour:minute* | **weekdays** *hour:minute* **to** *hour:minute* | **weekend** *hour:minute* **to** *hour:minute* | {**Friday** | **Monday** | **Saturday** | **Sunday** | **Thursday** | **Tuesday** | **Wednesday**} *hour:minute* **to** *hour:minute* | {**Friday** | **Monday** | **Saturday** | **Sunday** | **Thursday** | **Tuesday** | **Wednesday**} *hour:minute* **to** {**Friday** | **Monday** | **Saturday** | **Sunday** | **Thursday** | **Tuesday** | **Wednesday**} *hour:minute*]	Добавляет периодический временной диапазон
no periodic [**daily** *hour:minute* **to** *hour:minute* | **weekdays** *hour:minute* **to** *hour:minute* | **weekend** *hour:minute* **to** *hour:minute* | {**Friday** | **Monday** | **Saturday** | **Sunday** | **Thursday** | **Tuesday** | **Wednesday**} *hour:minute* **to** *hour:minute* | {**Friday** | **Monday** | **Saturday** | **Sunday** | **Thursday** | **Tuesday** | **Wednesday**} *hour:minute* **to** {**Friday** | **Monday** | **Saturday** | **Sunday** | **Thursday** | **Tuesday** | **Wednesday**} *hour:minute*]	Удаляет периодический временной диапазон

59.2.4 Применение временного диапазона

Созданный временной диапазон можно применить к одному или нескольким функциональным модулям. В данной версии программного обеспечения временной диапазон можно применить только к функциональному модулю IP ACL.

Чтобы применить временной диапазон к IP ACL, необходимо ввести имя временного диапазона в конце подкоманды **time-range** при настройке списка управления доступом. В конце данной главы приведен подробный пример настройки и применения временного диапазона.

Временной диапазон можно применить только к расширенному ACL, но не к стандартному.

59.2.5 Мониторинг конфигурации и состояния временного диапазона

Чтобы отслеживать конфигурацию временного диапазона, выполните следующую команду:

Команда	Описание
show time-range	Отображает конфигурацию всех временных диапазонов в системе
show time-range *name*	Отображает конфигурацию временного диапазона с именем *name*

Результат выполнения команды отображается на экране следующим образом:

```
Switch_config#show time-range

Now: Date: 2023.3.7    Time: 13:16    Week: Tuesday

time-range entry: x (inactive)
      absolute start 12:00 1 January 2023 end 13:00 2 January 2030
      periodic weekdays  09:00 to 18:00
time-range entry: y (empty)
time-range entry: z (active)
      periodic daily    12:00 to 13:00
      periodic Monday   Thursday  Friday   08:00 to 09:00
      periodic Saturday  15:00 to Sunday   20:00
      periodic daily    09:00 to 18:00

Switch_config#
```

В первой строке указано «Now: Date: 2023.3.7 Time: 13:16 Week: Tuesday», что означает дату 7 марта 2023 г.; время 13:16; день вторник.

Далее на экране отображается конфигурация и состояние временных диапазонов с именами x, y и z соответственно. Временной диапазон x имеет два элемента: абсолютное время и период и находится в неактивном состоянии; Временной диапазон y не имеет ни одного элемента и находится в пустом состоянии; Временной диапазон z имеет 4 периода и находится в активном состоянии.

59.3 Пример настройки временного диапазона

В следующем примере показано, как применить временной диапазон «sample» к правилу расширенного IP ACL с именем «ex».

```
Switch_config#
Switch_config#time-range sample
Switch_config_time_range_sample#periodic monday 12:00 to 13:00
Switch_config_time_range_sample#exit
Switch_config#ip access-list extended ex
Switch_config_ext_nacl#
Switch_config_ext_nacl#permit ip 192.168.213.180 255.255.255.255 any time-range
sample
Switch_config_ext_nacl#exit
Switch_config#
```

60. Настройка uRPF

60.1 Обзор

uRPF (Unicast Reverse Path Forwarding) – это механизм, позволяющий устройствам проверять, находится ли адрес источника в локальной таблице маршрутизации, прежде чем пересылать его. Это полезно для проверки подделки исходного адреса и защиты от DOS-атак.

Существует два режима uRPF: строгий (strict) и свободный (loose). Строгий режим проверяет, что исходный адрес имеет запись в таблице маршрутизации и что выходной интерфейс для маршрута совпадает с интерфейсом, на котором был получен пакет. Свободный режим только проверяет наличие маршрута в таблице перед пересылкой пакета.

60.2 Включение uRPF в глобальной конфигурации

Чтобы использовать uRPF, включите uRPF в режиме глобальной конфигурации:

Команда	Описание
[no] urpf check	Включает/отключает проверку uRPF в глобальной конфигурации

60.3 Настройка режима проверки uRPF на интерфейсе VLAN

Настройте режим проверки uRPF на интерфейсе VLAN (строгий или свободный режим). В строгом режиме адрес источника пакета будет использоваться не только для проверки его доступности в таблице FIB, но также для проверки соответствия порта входа пакета интерфейсу следующего перехода. В свободном режиме адрес источника пакета будет использоваться только для проверки его доступности в таблице FIB.

После настройки uRPF также поддерживается фильтрация маршрутов. Когда маршрут по умолчанию настроен и uRPF проверяет исходный адрес на основе таблицы FIB, все исходные адреса могут найти соответствующий элемент. По умолчанию, если результат проверки uRPF в таблице FIB является маршрутом по умолчанию, это будет восприниматься как отсутствие записи и пакеты будут отброшены.

Для настройки режима uRPF на интерфейсе VLAN выполните следующую команду в режиме настройки интерфейса:

Команда	Описание
[**no**] **urpf check** *strict/loose* [*uncheck-default-route*]	Настраивает режим проверки uRPF на интерфейсе VLAN. uncheck-default-route отключен по умолчанию

Включите функцию «enable uncheck-default-route». Если адрес источника пакета соответствует элементу в таблице FIB, то данный элемент будет принят как допустимый и пакет будет обработан. По умолчанию (если функция «uncheck-default-route» не включена), адрес источника пакета ищет соответствующий элемент в таблице FIB, и если данный элемент является маршрутом по умолчанию, то процесс uRPF завершается неудачей и пакет отбасывается.

61. Диагностика кабеля

61.1 Включение диагностики кабеля Ethernet

Чтобы включить диагностику кабеля, используйте следующую команду в режиме настройки интерфейса:

Команда	Описание
cable-diagnostic {*period* | <cr>} (TX port)	Устанавливает период проверки интерфейсного кабеля. Если он равен 0, проверка будет проведена только один раз

no cable-diagnostic	Восстанавливает настройки по умолчанию (диагностика выключена)

Диагностика не может гарантировать отсутствие погрешности для кабелей всех производителей. Результаты проверки предназначены только для справки.

Эта команда может через короткое время повлиять на нормальное использование служб интерфейса. После выполнения можно просмотреть результат теста с помощью команды **show interface**:

```
show interface g0/4
.....
 Cable Ok (4 pairs)
    Pair A Ok, length < 1 metres
    Pair B Ok, length < 1 metres
    Pair C Ok, length < 1 metres
    Pair D Ok, length < 1 metres
.....
```

Состояние кабеля:

OK: указывает на то, что витая пара в нормальном состоянии.

Open: указывает на то, что витая пара разомкнута.

Short: указывает на короткое замыкание пары проводов.

Crosstalk: указывает на наличие перекрестных помех между парами проводов.

Unknown: другие причины сбоя.

62. Настройка дополнительных функций оптического порта

62.1 Включение функции DDM

Чтобы включить DDM, используйте следующую команду в режиме глобальной конфигурации:

Команда	Описание
ddm {enable}	Включает функцию проверки DDM для всех оптических портов

no ddm	Отключает функцию проверки DDM для всех оптических портов

После включения функции проверки DDM информация оптического модуля может отображаться при помощи команды **show interface**. Если оптический модуль отсутствует, информация DDM не будет отображаться.

После включения функции загрузка ЦП может немного увеличиться в зависимости от конструкции оборудования. Информация включает в себя характеристики модуля, длину волны, информацию о производителе, серийный номер, дату производства и т. д. Если оптический модуль поддерживает функцию цифрового диагностического мониторинга, также будет отображаться полученная оптическая мощность, напряжение, ток смещения, температура и соответствующая пороговая информация:

ddm enable

show int g0/25

.....

Transceiver Info:

SFP,LC,850nm,10000BASE-FX-SR,LOS:yes

MM 80M(50um OM2 fiber) 30M(62.5um OM1 fiber) 300M(50um OM3 fiber)

DDM:YES,Vend:FINISAR,PN:FTLX8571D3BCL-HW

SerialNum:AQN03Y5,Date:2021-04-04

DDM info:

TX power:-9.40 dBm, RX power:-36.99 dBm

SFP temperature:21.00 C,supply voltage :3.40V,Bias Current.:5.00mA

DDM Thresholds:	Low-Alarm	Low-Warning	High-Warning	High-Alarm
TX power(dBm):	-6.00	-5.00	0.50	1.50
RX power(dBm):	-13.00	-12.50	0.50	1.50
SFP temperature(C):	-10	0	75	85
Supply voltage(v):	3.00	3.10	3.50	3.60
Bias Current(mA):	1.00	1.00	100.00	110.00

62.2 Функция поддержки одноволоконного трансивера

Чтобы включить функцию поддержки одноволоконного трансивера для оптического порта, используйте следующую команду:

Команда	Описание

single-fiber one-way {tx | rx}	Включает функцию порта для работы с одним волокном (отправка или прием)
no single-fiber	Отключает функцию поддержки одноволоконного трансивера порта

После включения этой функции порт немедленно переходит в состояние LINK UP. Вы можете вставить оптический кабель в коннектор TX или RX оптического модуля в соответствии с настроенной функцией. Данные будут передаваться только в одном направлении.

62.3 Функция адаптации к оптическому модулю

Команда	Описание
fiber-auto-config {full}	Позволяет настроить функцию адаптации порта к оптическому модулю. При использовании параметра **full** устройство переключается в принудительный режим
no fiber-auto-config	Отключает функцию автосогласования порта

После включения этой функции порт будет выбирать режим работы в соответствии с типом установленного оптического модуля. Например, оптический порт 10G с установленным модулем Gigabit переключится в оптический режим Gigabit, а оптический порт Gigabit с установленным модулем 100M переключится в оптический режим 100M.

10-гигабитный порт имеет только один рабочий режим, а гигабитный порт – два режима: автоадаптивный и принудительный. Таким образом, 10-гигабитный оптический порт с установленным гигабитным оптическим модулем по умолчанию переключится в гигабитный адаптивный режим. Чтобы переключиться в режим принудительного использования Gigabit, необходимо после этой команды добавить параметр **full**. Порт 100M имеет только один рабочий режим, поэтому параметр **full** не требуется. Если используется оптико-электрический модуль, для правильной работы необходимо добавить параметр **full**.

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
AS	Autonomous System	Автономная система
ASBR	Autonomous System Boundary Router	Граничный маршрутизатор автономной системы
ARP	Address Resolution Protocol	Протокол определения MAC-адреса другого узла по известному IP-адресу
ATAP	Address Table Aging Protection	Функция, которая защищает MAC-адреса в таблице MAC-адресов от быстрого истечения их времени жизни
BDR	Backup Designated Router	Резервный выделенный маршрутизатор
BootP	Bootstrap Protocol	Протокол, используемый для автоматического получения клиентом IP-адреса
BPDU	Bridge Protocol Data Unit	Блок данных протокола управления сетевыми мостами
CAR	Committed Access Rate	Гарантированная скорость доступа
CFM	Connectivity Fault Management	Протокол обнаружения и устранения проблем сетевой связи
CHAP	Challenge Handshake Authentication Protocol	Протокол аутентификации с косвенным согласованием. Является алгоритмом проверки подлинности и предусматривает передачу не самого пароля пользователя, а косвенных сведений о нём
CIDR	Classless Inter-Domain Routing	Бесклассовая междоменная маршрутизация
CIST	Common and Internal Spanning Tree	Общее и внутреннее связующее дерево
CLI	Command Line Interface	Интерфейс командной строки
CoS	Class of Service	Класс сервиса
CST	Common Spanning Tree	Общее связующее дерево
DAI	Dynamic ARP Inspection	Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP
DD	Database Description	Описание базы данных
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки узла
DHP	Dual Homing Protocol	Протокол, позволяющий подключить устройство к двум разным коммутаторам, обеспечивая резервирование подключения
DNS	Domain Name System	Система доменных имен

DR	Designated Router	Назначенный маршрутизатор
DSCP	Differentiated Services CodePoint	Точка кода дифференцированных услуг
DST	Daylight Saving Time	Переход на летнее время
EAP	Extensible Authentication Protocol	Расширяемый протокол аутентификации
EAPS	Ethernet Automatic Protection Switching	Протокол канального уровня для построения и защиты кольцевой топологии Ethernet
EFM OAM	Ethernet in the First Mile Operations, Administration, and Maintenance	Набор механизмов и протоколов «первой мили» для управления, администрирования и обслуживания Ethernet-соединений в местных сетях доступа
FTP	File Transfer Protocol	Протокол передачи файлов
GARP	Generic Attribute Registration Protocol	Протокол регистрации основных атрибутов
GVRP	GARP VLAN Registration Protocol	Протокол GARP для регистрации VLAN
HTTP	Hyper Text Transfer Protocol	Протокол передачи гипертекста
ICMP	Internet Control Message Protocol	Протокол межсетевых управляющих сообщений
IED	Intelligent Electronic Device	Интеллектуальное электронное устройство
IGMP	Internet Group Management Protocol	Протокол управления группами Интернета (протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP)
IGMP Snooping	Internet Group Management Protocol Snooping	Протокол отслеживания сетевого трафика IGMP
IST	Internal Spanning Tree	Внутреннее связующее дерево
LACP	Link Aggregation Control Protocol	Протокол агрегирования каналов
LLDP	Link Layer Discovery Protocol	Протокол обнаружения канального уровня
LLDPDU	Link Layer Discovery Protocol Data Unit	Блок данных протокола обнаружения уровня канала
LSA	Link State Advertisement	Сообщение с описанием локального состояния маршрутизатора или сети
LSAck	Link State Acknowledgment	Пакет подтверждения состояния канала
LSDB	Link State Database	База данных о состоянии каналов
LSR	Link State Request	Пакет запроса о состоянии канала
LSU	Link State Update	Пакет подтверждения состояния канала
MAB	MAC Authentication Bypass	Аутентификация устройств, подключенных к сети по MAC-адресам
MIB	Management Information Base	Виртуальная база данных, используемая для управления объектами в сети связи
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
NAS	Network Access Server	Сервер сетевого доступа
ND	Neighbor Discovery protocol	Протокол обнаружения соседей
NetBIOS	Network Basic Input/Output System	Базовая сетевая система ввода-вывода
NMS	Network Management System	Система управления сетью
NTP	Network Time Protocol	Сетевой протокол синхронизации 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
PBR	Policy Based Routing	Маршрутизация на основе политик
PDP	Protocol Discovery Protocol	Протокол, позволяющий находить все соседние устройства, связанные с определенным устройством в сети
PVLAN	Private VLAN	Частная виртуальная локальная сеть
QoS	Quality of Service	Качество обслуживания (технология предоставления различным классам трафика различных приоритетов в обслуживании)
RADIUS	Remote Authentication Dial-In User Service	Служба удалённой аутентификации пользователей
RID	Router ID	Идентификатор маршрутизатора
RIP	Routing Information Protocol	Протокол дистанционно-векторной маршрутизации
RMON	Remote Network Monitoring	Дистанционный мониторинг сети (расширение SNMP, разработанное IETF)
RSA	Rivest, Shamir, Adleman	Криптографический алгоритм с открытым ключом
RSTP	Rapid Spanning Tree Protocol	Быстрый протокол связующего дерева (версия протокола STP с ускоренной реконфигурацией дерева)
RTC	Real Time Clock	Часы реального времени
SNMP	Simple Network Management Protocol	Простой протокол сетевого управления (интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP)

SNTP	Simple Network Time Protocol	Простой протокол синхронизации времени (является упрощённой реализацией протокола NTP)
SPVLAN	Service Provider's VLAN	Технология, используемая в сетях провайдеров, позволяющая разделять трафик клиентов на разные VLAN, обеспечивая безопасность и изоляцию сетевых сервисов
SSH	Secure Shell	«Безопасная оболочка», сетевой протокол прикладного уровня
SSL	Secure Sockets Layer	Уровень защищённых сокетов; криптографический протокол, который отвечает за безопасную передачу данных на сеансовом уровне
SSTP	Single Spanning Tree Protocol (802.1D STP)	Протокол единого связующего дерева
STP	Spanning Tree Protocol	Протокол связующего дерева
TACACS+	Terminal Access Controller Access Control System	Сеансовый протокол аутентификации, авторизации и учета доступа
TCP	Transmission Control Protocol	Протокол управления передачей
TFTP	Trivial File Transfer Protocol	Простой протокол передачи файлов
UDLD	Unidirectional Link Detection	Протокол обнаружения однонаправленного соединения
UDP	User Datagram Protocol	Протокол пользовательских дейтаграмм
uRPF	Unicast Reverse Path Forwarding	Метод, используемый для обеспечения безцикловой пересылки многоадресных пакетов при многоадресной маршрутизации и для предотвращения подмены IP-адресов при одноадресной маршрутизации
USM	User-Based Security Model	Модель безопасности на основе пользователей
VLAN	Virtual Local Area Network	Виртуальная локальная сеть
VPN	Virtual Private Network	Виртуальная частная сеть
VRF	VPN Routing/Forwarding table	Таблица маршрутизации VPN
VRRP	Virtual Router Redundancy Protocol	Протокол резервирования виртуальных маршрутизаторов
VSA	Vendor-Specific Attributes	Атрибуты, специфичные для поставщика
WRR	Weighted Round Robin	Взвешенная очередь