Руководство по настройке коммутаторов SNR

S2985G S2965 S2982G S2962

Оглавление

1. Основные настройки управления

1.1. Виды управления коммутатором

После приобретения коммутатора необходима его настройка для корректной работы. Поддерживается два вида управления: **in-band** и **out-of-band**.

1.1.1. Out-of-band управление

Out-of-Band управление осуществляется через консольный порт коммутатора для его первоначальной настройки или когда in-band управление недоступно. Например вы можете назначить ip-адрес коммутатору через консоль для того, чтобы иметь возможность управлять коммутатором по протоколу telnet.

Для связи с коммутатором через консольный порт на ПК необходимо выполнить следующие действия:

- Соединить Serial-порт ПК с портом Console коммутатора консольным кабелем идущим в комплекте с коммутатором.
- Запустить программу эмуляции терминала (Putty, Minicom, HyperTerminal) и произвести следующие настройки:
  - Выбрать соответствующий Serial порт компьютера .
  - Установить скорость передачи данных 9600.
  - Задать формат данных: 8 бит данных, 1 стоповый бит, без контроля четности.
  - Отключить аппаратное и программное управление потоком данных.
  - Включить питание коммутатора

При правильном выполнении вышеперечисленных пунктов в эмуляторе терминала появится лог загрузки коммутатора:

```
System is booting, please wait…
Net Initialization Skipped
Bootrom version: 7.2.25
Creation date: Sep  2 2015 - 10:07:04
Testing RAM...
0x08000000 RAM OK.
Loading flash:/nos.img ...
### JFFS2 loading 'nos.img' to 0x81000000
### JFFS2 load complete: 12781972 bytes loaded to
0x81000000
## Booting kernel from Legacy Image at 81000100 ...
   Image Name:
   Created:      2017-01-20   7:41:49 UTC
   Image Type:   MIPS Linux Kernel Image (gzip compressed)
   Data Size:    12734504 Bytes = 12.1 MiB
  Load Address: 80000000
Entry Point:  80003710
```

```
Verifying Checksum ... OK
Uncompressing Kernel Image ... OK
Starting kernel ...
Current time is Sun Jan 01 00:00:00 2006 [UTC]
SNR-S2965-24T Series Switch Operating System
Software Version 7.0.3.5(R0241.0136)
Compiled Jan 20 15:26:28 2017
```

После окончания загрузки коммутатора необходимо ввести имя пользователя (Username) и пароль (Password) (по умолчанию admin/admin). После чего открывается доступ к конфигурированию коммутатора. Более подробно конфигурирование коммутатора будет рассмотрено далее .

1.1.2. In-band управление

In-band управление предполагает управление коммутаторам используя протоколы Telnet, SSH, HTTP или SNMP с устройств подключенных к коммутатору. Если in-band управление недоступно используйте out-of-band управеление для настройки коммутатора.

1.1.2.1. Настройка коммутатора при помощи Telnet

Для управления коммутатором, используя протокол Telnet необходимо чтобы на коммутаторе был сконфигурирован ipv4 или ipv6 адрес и хост с Telnet клиентом был доступен с коммутатора (находился в одной сети с ним или был доступен через маршрутизатор). Коммутатор по умолчанию имеет ip-адрес 192.168.1.1 в Vlan 1. Коммутатор может иметь несколько ip-адресов для управления в т.ч. в различных Vlan. Более подробное описание настройки приведено в соответствующем разделе данного Руководства.

Пример подключения к коммутатору с конфигурацией по умолчанию используя протокол Telnet.

В примере коммутатор имеет ip-адрес по умолчанию **192.168.1.1**, маска **255.255.255.0**. Сначала необходимо настроить IP-адрес на ПК с которого будет осуществляться управление. Настроим адрес **192.168.1.2**, маска **255.255.255.0**. Соединим ПК и коммутатор патчкордом Ethernet. Выполним команду: `telnet 192.168.1.1`. Затем введем Login и пароль (по умолчанию admin/admin).

```
telnet 192.168.1.1
Trying 192.168.1.1…
Connected to 192.168.1.1.
Escape character is '^]'.
login:admin
Password:*****
SNR-S2965-24T#
```

1.1.2.2. Управление по HTTP (WEB-интерфейс)

Для управления коммутатором, используя HTTP (WEB-интерфейс) необходимо чтобы на коммутаторе был сконфигурирован ipv4 или ipv6 адрес и хост с HTTP клиентом был доступен с коммутатора (находился в одной сети с ним или был доступен через маршрутизатор). Коммутатор по умолчанию имеет ip-адрес 192.168.1.1 в Vlan 1.

Коммутатор может иметь несколько ip-адресов для управления в т.ч. в различных Vlan. Более подробное описание настройки приведено в соответствующем разделе данного Руководства.

Для доступа к коммутатору через WEB-интерфейс откройте WEB-браузер и введите в адресной строке http://ip-коммутатора, например http://192.168.1.1 . В открывшейся странице введите имя пользователя и пароль (По умолчанию admin/admin).

Рис. 1-1 Страница авторизации WEB-интерфейса

При верном вводе имени пользователя и пароля откроется основной WEB-интерфейс.

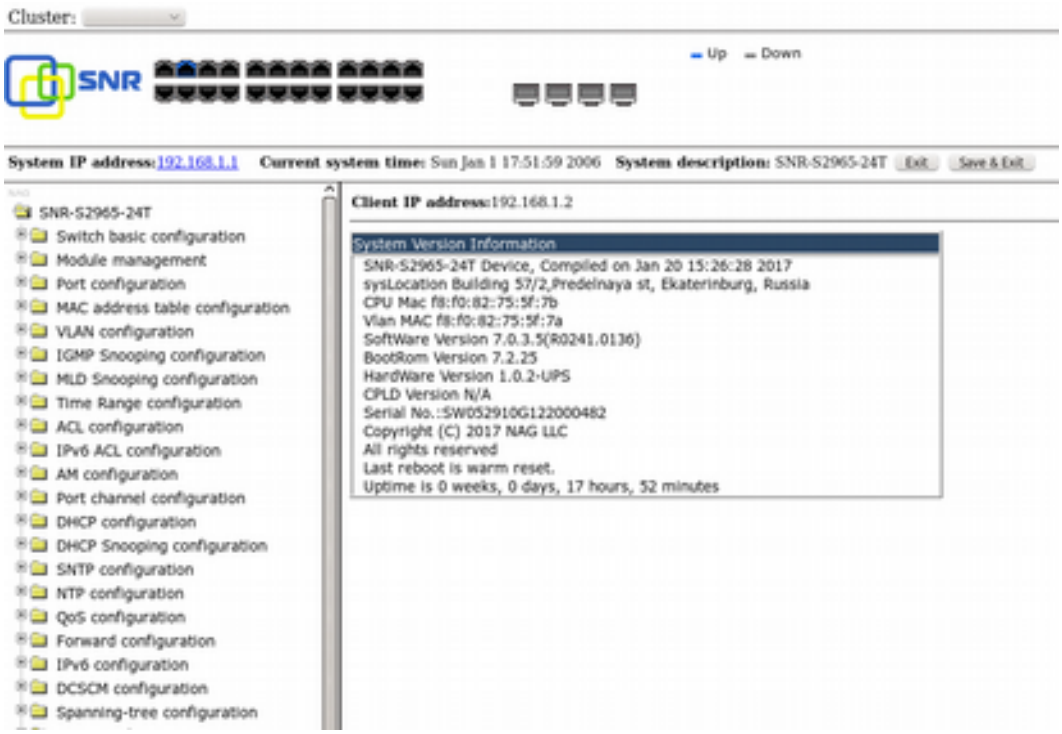


Рис. 1-2. Основное меню WEB-интерфейса.

1.1.2.3. Управление коммутатором по SNMP

Для управления коммутатором по SNMP необходимо чтобы на коммутаторе был сконфигурирован ipv4 или ipv6 адрес и хост с SNMP клиентом был доступен с коммутатора (находился в одной сети с ним или был доступен через маршрутизатор). Коммутатор по умолчанию имеет ip-адрес 192.168.1.1 в Vlan 1.

Коммутатор может иметь несколько ip-адресов для управления в т.ч. в различных Vlan. Более подробное описание настройки приведено в соответствующем разделе данного Руководства.

1.2. Интерфейс командной строки (CLI)

Коммутатор поддерживает 3 типа интерфейса для конфигурирования: CLI (Command Line Interface), WEB-интерфейс и SNMP. CLI интерфейс знаком большинству пользователей и как уже описывалось выше out-of-band управление и Telnet используют CLI интерфейс для настройки коммутатора.

В основе CLI интерфейса лежит оболочка, состоящая из набора команд. Команды разделены по категориям в соответствии со своими функциями по настройке и управлению коммутатором. Каждая категория определяется различными конфигурационными режимами.

CLI интерфейс определяется:

- Режимами конфигурирования.
- Синтаксисом команд.
- Короткими сочетаниями клавиш.
- Функцией справки.
- Проверкой корректности ввода.
- Сокращенным вводом команд.

1.2.1. Режимы конфигурирования

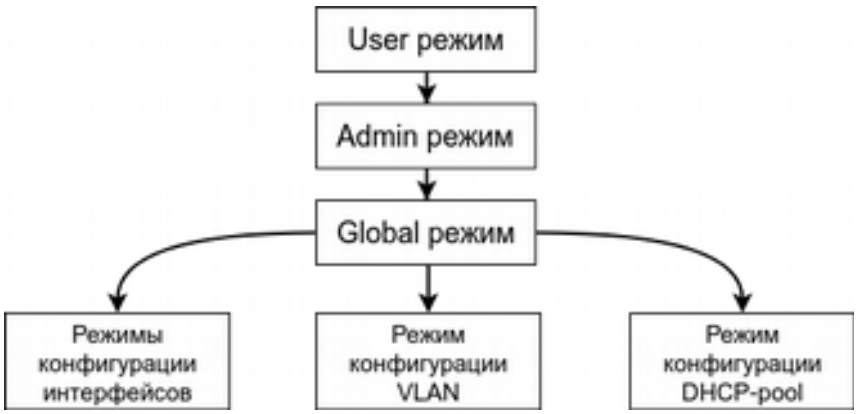


Рис. 1-3 Режимы конфигурирования CLI

User режим

При входе в CLI интерфейс, пользователя с привилегиями 1-14 попадает в режим user. В User режиме приглашение выглядит как `hostname>`. Символ “>” означает что пользователь находится в user режиме. При выходе из Admin режима пользователь также попадает в User режим.

В user режиме недоступна настройка коммутатора, разрешены только команды **show**.

Admin режим

В Admin режим попадают пользователи с привилегиями 15 либо пользователи с привилегиями 1-14 после ввода команды enable и пароля, если задан пароль для enable.

В admin режиме приглашение CLi выглядит как `hostname#`. Символ ‘#” означает что пользователь находится в admin режиме. Для выхода в Admin режим из любых других режимов кроме User поддерживается короткое сочетание клавиш “Ctrl+z”.

В Admin режиме пользователь может запрашивать вывод полной конфигурации и статуса коммутатора, а также может переходить в режим глобального конфигурирования (Global режим) для настройки любых параметров коммутатора. В связи с этим рекомендуется задавать пароль для перехода в Admin режим, для предотвращения несанкционированного доступа и изменений настроек коммутатора.

Global режим (Режим глобальной конфигурации)
При вводе команды config из Admin режима пользователь попадает в режим глобальной конфигурации. Для возврата в Global режим из вышестоящих режимов конфигурации, таких как Vlan, Порт и.т.д. предназначена команда exit.

В Global режиме доступна конфигурация глобальных параметров коммутатора, таких как таблица мак-адресов, настройка SNMP, пользователей и.т.п., а так же возможен переход в режимы конфигурации интерфейсов, Vlan и.т.п.

Режим конфигурации интерфейсов:
Для перехода в режим конфигурирования интерфейсов используйте команду interface <name>. Для возврата в глобальный режим конфигурации используйте команду Exit.

Поддерживаются три вида интерфейсов:
1. Vlan интерфейс.
2. Ethernet порт.
3. Port-channel интерфейс.

Тип интерфейса	Команда	Описание
VLAN интерфейс	`interface vlan <Vlan-id>` В режиме глобальной конфигурации	Настройка L3 интерфейсов коммутатора
Ethernet порт	`interface ethernet <interface-list>` В режиме глобальной конфигурации	Настройка параметров физических интерфейсов (скорость, режим и.т.п)

port-channel	`interface port-channel <port-channel-number>` В режиме глобальной конфигурации	Настройка параметров Port-Channel интерфейсов (режим, vlan и.т.п.)

Режим конфигурации Vlan
Для перехода в режим конфигурации Vlan используйте команду vlan <vlan-id> в режиме глобальной конфигурации конфигурирования. В этом режиме настраиваются параметры vlan, такие как имя vlan, remote-span, multicast vlan.

Режим конфигурации DHCP пула
Для перехода в режим настройки DHCP пула введите команду ip dhcp pool <name> в режиме глобальной конфигурации.

1.2.2. Синтаксис

Коммутатор поддерживает большое количество команд, тем не менее все они имеют общий синтаксис:

`cmdtxt` `<variable> {enum1 | … | enumN } [option1 | … | optionN]`

Условные обозначения:

- **`cmdtxt`** жирным шрифтом обозначает название ключевое слово команды;
- `<variable>` обозначает обязательный параметр;
- `{enum1 | … | enumN }` обозначает обязательный параметр, который должен быть указан из ряда значений enum1~enumN;
- квадратные скобки ([ ]) в `[option1 | … | optionN]` обозначают необязательные параметры.

В CLI поддерживаются различные комбинации “< >“, “{ }” и “[ ]” , такие как `[<variable>], {enum1 <variable>| enum2}, [option1 [option2]]`, и т.д..

Ниже приведены примеры команд в конфигурационном режиме:
- `show version`, Эта команда не требует параметров, просто введите команду и нажмите Enter для её выполнения.
- `vlan <vlan-id>`, требуется ввести параметр - номер vlan для выполнения команды.
- `firewall {enable|disable}`, при вводе команды после ключевого слова firewall необходимо указать enable или disable.
- `snmp-server community {ro | rw} <string>`, допустимы следующие варианты:

```
snmp-server community ro <string>
snmp-server community rw <string>
```

1.2.3. Горячие клавиши

CLI поддерживает ряд коротких сочетаний клавиш для упрощения работы. Если терминальный клиент не распознает клавиши Вверх и Вниз, можно использовать сочетания “Ctrl+P” и “Ctrl+N” вместо них.

Сочетание клавиш	Функция
Back Space	Удаляет символ перед курсором и сдвигает позицию курсора на один символ назад.
Вверх “↑”	История введенных команд. Выводит предыдущую введенную команду. Многократное нажатие выводит ранее введенные команды по порядку.
Вниз “↓”	История введенных команд. Выводит следующую введенную команду.
Влево “←”	Сдвиг курсора на один символ влево
Вправо “→”	Сдвиг курсора на один символ вправо
Ctrl + P	То же что и клавиша Вверх “↑”.
Ctrl + N	То же что и клавиша Вниз “↓”.
Ctrl + Z	Возврат в Admin режим из любого конфигурационного режима
Ctrl + C	Остановка запущенной команды, например ping
Tab	При частичном вводе команды, при нажатии клавиши Tab, выводятся все допустимые варианты продолжения команды.

1.2.4. Справка

CLI поддерживает две команды для вызова справки: команда “help” и “?”

Команда	Описание
help	В любом режиме команда help выводит краткую информацию по использованию функции справки

“?”	В любом режиме ввод “?” выводит список всех допустимых для данного режима команд с описанием; Ввод “?” через пробел после ключевого слова выводит список допустимых параметров/ключевых слов с коротким описанием. Вывод “<cr>“ означает что команда введена полностью введена и необходимо нажать Enter для её выполнения; Ввод “?” сразу после строки. В этом случае выводятся все допустимые команды, начинающиеся с введенной строки.

1.2.5. Проверка ввода

Все введенные команды проверяются на правильность. При некорректном вводе возвращается информация об ошибке.

Информация об ошибке	Описание
% Incomplete command.	Команда введена не полностью либо отсутствует обязательный параметр.
% Invalid input detected at '^' marker.	Неправильный ввод команды. Маркер ‘^’ указывает на место неправильного ввода.
% Ambiguous command:	Введенная команда имеет два и более варианта интерпретации.

1.2.6. Сокращенный ввод команд

CLI поддерживает сокращенный ввод команд, если введенная строка может быть однозначно дополнена до полной команды и интерпретирована.

Пример:

1. Для команды `show interfaces status ethernet1/0/1` допустим сокращенный ввод `sh int status eth1/0/1`
2. Для команды `show running-config` сокращенный ввод `show r` вернет ошибку “**% Ambiguous command:** “ так как существует несколько команд начинающихся с `sh r`: `show running-config`, `show radius`, `show reload`. В то же время команда `show ru` будет выполнена, так как существует единственный вариант интерпретации.

2. Базовые настройки коммутатора

2.1. Базовая конфигурация

Базовые настройки коммутатора включают в себя команды для входа/выхода из admin режима, конфигурации и просмотра времени, вывода базовой информации о коммутаторе.

Команда	Описание
Режимы User и Admin	

`enable [<1-15>]`
 	
`disable`
	Команда **`enable`** предназначена для перехода из User в Admin режим, либо для смены уровня привилегий у текущего пользователя.
	
	Команда **`disable`** служит для выхода из режима Admin.

Admin режим	
`config [terminal]`	Переход в режим глобального конфигурирования (Global) из режима Admin.
Все режимы	
`exit`	Выход из текущего режима конфигурирования в нижестоящий режим. Например из Global режима в Admin.
`show privilege`	Вывод текущего уровня привилегий пользователя.
Все режимы за исключением User и Admin	
`end`	Выход из текущего режима конфигурирования и возврат в Admin режим.
Admin режим	
`clock set <HH:MM:SS> [YYYY.MM.DD]`	Установка системной даты и времени.
`show version`	Вывод информации о коммутаторе.
`set default`	Сброс текущей конфигурации к конфигурации по умолчанию.

write	Сохранение текущей конфигурации коммутатора на Flash память.
reload	Перезагрузка коммутатора.
show cpu usage	Вывод информации о свободных ресурсах CPU.
show cpu utilization	Вывод информации о текущей загрузке CPU.
show memory usage	Вывод информации о текущей утилизации ОЗУ коммутатора.
Global режим	
banner motd <LINE> no banner motd	Настройка информации, отображающейся при входе пользователя на коммутатор.
web-auth privilege <1-15> no web-auth privilege	Настройка уровня привилегий для WEB-интерфейса коммутатора.

2.2. Telnet

2.2.1. Обзор протокола Telnet

Telnet это простой протокол для доступа к удаленному терминалу. Используя Telnet пользователь может удаленно зайти на оборудование зная его ip-адрес или доменное имя. Telnet может отправлять введенную пользователем информацию на удаленный хост и выводить ответы хоста на терминал пользователя аналогично тому что пользователь подключен напрямую к оборудованию.
Telnet работает Клиент-Серверной технологии, на локальной системе работает Telnet клиент, а на удаленном хосте Telnet server. Коммутатор может работать как в роли Telnet сервера, так и в роли Telnet клиента. При работе коммутатора в роли Telnet сервера, пользователи могут удаленно заходить на него используя Telnet клиент, как было описано ранее в разделе In-band управления.
Используя коммутатор в качестве Telnet клиента пользователь может удаленно заходить на другие хосты.

2.2.2. Настройка Telnet

1. Настройте Telnet сервер на коммутаторе
2. Зайдите на коммутатор с удаленного терминала

Команда	Описание

`telnet-server enable`
`no telnet-server enable`
 	
В режиме глобальной конфигурации
	Включить Telnet сервера на коммутаторе (по-умолчанию Telnet включен).
	Команда с приставкой **no** отключает Telnet сервер на коммутаторе.

`username <user-name>`
`[privilege <privilege>]`
`[password [0 | 7] <password>]`
`no username <username>`
 	
В режиме глобальной конфигурации
	Настроить имя пользователя и пароля для доступа на коммутатор.
	`<user-name>` - имя пользователя
	`<privilege>` - уровень привилегий (по умолчанию 1)
	`password [0 | 7]` - тип пароля
	0 пароль в открытом виде
	7 - пароль в зашифрованном виде
	`<password>` - пароль
	Команда с приставкой **no** удаляет пользователя.

`aaa authorization config-commands`
`no aaa authorization config-commands`
 	
В режиме глобальной конфигурации
	Включить авторизацию вводимых команд для удаленных пользователей Команда **no** отключает авторизацию введенных команд .

`authentication securityip <ip-addr>`
`no authentication securityip <ip-addr>`
 	
В режиме глобальной конфигурации
	Настроить доверенный ipv4-адрес, с которого будет разрешен удаленный доступ коммутатору. (При применении данной команды доступ к управлению коммутатора с других ip-адресов будет запрещен)
	
	Удаление адреса из списка **authentication securityip**

`authentication securityipv6 <ipv6-addr>`
`no authentication securityipv6 <ipv6-addr>`
 	
В режиме глобальной конфигурации
	Настроить доверенный ipv6-адрес, с которого будет разрешен удаленный доступ коммутатору. (При применении данной команды доступ к управлению коммутатора с других ip-адресов будет запрещен)
	Команда **no** удаляет адреса из списка **authentication securityip6**

`authentication ip access-class {<num>|<name>} in [ssh|telnet|web]` `no authentication ip access-class [ssh|telnet|web]`	Настроить ограничения удаленного доступа к ipv4 адресу коммутатора по ACL `<num>` - номер ACL `<name>` - имя ACL `ssh` - ограничение доступа по SSH `telnet` - ограничение доступа по Telnet

В режиме глобальной конфигурации	`web` - ограничение доступа к WEB без указания `[ssh|telnet|web]` доступ ограничивается по всем протоколам Команда **no** отменяет ограничения доступа по ACL

`authentication ipv6 access-class {<num>|<name>} in [ssh|telnet|web]`
`no authentication ipv6 access-class`
 	
В режиме глобальной конфигурации
	Настроить ограничения удаленного доступа к ipv6 адресу коммутатора по ACL
	`num` - номер ACL
	`name` - имя ACL
	`ssh` - ограничение доступа по SSH
	`telnet` - ограничение доступа по Telnet
	`web` - ограничение доступа к WEB
	без указания `[ssh|telnet|web]` доступ ограничивается по всем протоколам
	Команда **no** отменяет ограничения доступа по ACL

`authentication line {console | vty | web} login <method> [<method> …]`
`no authentication line {console | vty | web} login`
 	
В режиме глобальной конфигурации
	Настроить метод аутентификации для доступа через консоль, vty (telnet или SSH) и Web
	Значения `<method>`:
	`local` - локальная аутентификация
	`radius` - Radius аутентификация
	`tacacs` - Tacacs аутентификация
	Команда **no** отменяет настройки методов аутентификации

`authentication enable <method> [<method> …]`
`no authentication enable`
 	
В режиме глобальной конфигурации
	Настроить метод аутентификации для перехода в Admin режим
	Значения `<method>`:
	`local` - локальная аутентификация
	`radius` - Radius аутентификация
	`tacacs` - Tacacs аутентификация
	
	Команда **no** отменяет настройки методов аутентификации для перехода в Admin режим

`authorization line {console | vty | web} exec <method> [<method> …]`
`no authorization line {console | vty | web} exec`
 	
В режиме глобальной конфигурации
	Настроить метод авторизации
	при доступе на коммутатор через консоль, vty (telnet или SSH) и Web
	Значения `<method>`:
	`local` - локальная аутентификация
	`radius` - Radius аутентификация
	`tacacs` - Tacacs аутентификация

	Команда **no** отменяет настройки метода авторизации

`authorization line vty command <1-15> <method> [<method> …]`
`no authorization line vty command <1-15>`
 	
В режиме глобальной конфигурации
	Настроить метод авторизации вводимых команд для определенного уровня привилегий
	`<1-15>` - Уровень привилегий для которого настраивается метод авторизации команд
	Значения `<method>`:
	`local` - локальная авторизация
	`radius` - Radius авторизация
	`tacacs` - Tacacs авторизация
	`none` - авторизация отключена
	Команда **no** отменяет настройки метода авторизации вводимых команд

`accounting line {console | vty} command <1-15> {start-stop | stop-only | none} method1 [method2…]`
`no accounting line {console | vty} command <1-15>`
 	
В режиме глобальной конфигурации
	Настроить учет вводимых команд для определенного метода доступа и уровня привилегий
	`console` - доступ через консоль
	`vty` - доступ через Telnet/SSH
	`<1-15>` - Уровень привилегий для которого настраивается метод аккаунтинга команд
	`start-stop`, `stop-only` - не имеет значения, отсылаются только stop записи.
	Значения `<method>`:
	Поддерживается только метод `tacas`
	
	Команда **no** отменяет настройки метода учета вводимых команд для определенного уровня привилегий

`terminal monitor`
 	
`terminal no monitor`
 	
В Admin режиме
	Вывод сообщений уровня debug на терминал
	
	Отмена вывода сообщений уровня debug на терминал

`show users` В Admin режиме	Вывод информации о текущих пользователях, авторизованных на коммутаторе включая номер линии, имя пользователя и ip-адрес

`clear line vty <0-31>` В Admin режиме	Отключение активного пользователя с терминальной линии.

Использование Telnet-клиента на коммутаторе

Команда	Описание
`telnet [vrf <vrf-name>] {<ip-addr> | <ipv6-addr> | host <hostname>} [<port>]` В Admin режиме	Подключение к удаленному терминалу по протоколу Telnet `vrf <vrf-name>` - имя VRF (не поддерживается на коммутаторах SNR-S2965/2985) `ip-addr` – ipv4-адрес удаленного терминала `ipv6-addr` - ipv6-адрес удаленного терминала `hostname` - доменное имя удаленного терминала `port` – TCP порт для подключения (по умолчанию 23)

2.3 SSH

2.3.1 Настройка SSH сервера на коммутаторе

Команда	Описание

`ssh-server enable`
 	
`no ssh-server enable`
 	
В режиме глобальной конфигурации
	Включение SSH сервера на коммутаторе
	
	Отключение SSH сервера на коммутаторе

`ssh-server timeout <timeout>`
 	
`no ssh-server timeout`
 	
В режиме глобальной конфигурации
	Настройка таймаута аутентификации при подключении по SSH
	Настройка значения таймаута аутентификации по умолчанию

`ssh-server authentication-retires <authentication-retires>`	Настройка ограничения количества попыток аутентификации при подключении к SSH

`no ssh-server authentication-retries` В режиме глобальной конфигурации	Сброс ограничения количества попыток аутентификации к значению по умолчанию.
`ssh-server host-key create rsa [modulus <moduls>]` В режиме глобальной конфигурации	Генерация ключа RSA <moduls> - длина модуля ключа

2.4 Настройка ip-адреса коммутатора

Хотя коммутаторы серий SNR-S2965 и SNR-S2985G являются оборудованием уровня 2, на них есть возможность создать L3 Vlan интерфейс (SVI) с ip-адресом, который также является ip-адресом для управления коммутатором.
Поддерживается три варианта назначения ip-адреса коммутатору:

- Статический
- BOOTP
- DHCP

Статический ip-адрес настраивается вручную на коммутаторе.
В режиме BOOTP/DHCP, коммутатор работает в роли BOOTP или DHCP клиента и получает ip-адрес динамически от BOOTP/DHCP сервера. Также коммутатор может сам выступать в роли DHCP сервера, динамически раздавая адреса подключенному оборудованию. Настройка DHCP сервера будет рассмотрена позже.

2.4.1 Настройка ip-адреса на коммутаторе

1. Создание Vlan интерфейса на коммутаторе
2. Статическая настройка ip-адреса
3. Динамическое получение ip-адреса по протоколу BOOTP
4. Динамическое получение ip-адреса по протоколу DHCP

1. Создание Vlan интерфейса на коммутаторе

Команда	Описание

`interface vlan <vlan-id>`
 	
`no interface vlan <vlan-id>`
 	
В режиме глобальной конфигурации
	Создание L3 интерфейса в Vlan `<vlan-id>`
	
	Удаление L3 интерфейса в Vlan `<vlan-id>`

2. Статическая настройка ip-адреса

Команда	Описание

`ip address <ip_address> <mask> [secondary]`
 	
`no ip address <ip_address> <mask> [secondary]`
 	
В режиме конфигурации Interface VLAN
	Настройка статического IPv4-адреса `<ip_address>` с маской `<mask>` на Vlan интерфейсе.
	`secondary` - ip-адрес будет добавлен на интерфейс как дополнительный (secondary)
	
	Удаление статического ip-адреса с интерфейса

`ipv6 address [<prefix-name>] <ipv6-address/prefix-length> [eui-64]`
 	
`no ipv6 address <ipv6-address/prefix-length>`
 	
В режиме конфигурации Interface VLAN
	Настройка статического IPv6-адреса `<ipv6_address/prefix>`
	`eui-64` - использовать EUI-64 для формирования IPv6 адреса
	
	Удаление статического IPv6-адреса с интерфейса

3. Динамическое получение ip-адреса по протоколу BOOTP

Команда	Описание

`ip bootp-client enable`
 	
`no ip bootp-client enable`
 	
В режиме конфигурации Interface VLAN
	Включить BOOTP клиент на Interface Vlan
	
	Отключить BOOTP клиент на Interface Vlan

4. Динамическое получение ip-адреса по протоколу DHCP

Команда	Описание

`ip dhcp-client enable`
 	
`no ip dhcp-client enable`
В режиме конфигурации Interface VLAN
	Включить DHCP клиент на Interface Vlan
	
	Отключить DHCP клиент на Interface Vlan

2.5 Настройка SNMP

2.5.1 Описание протокола SNMP

SNMP (Simple Network Management Protocol) — стандартный протокол, который широко используется для управления сетевыми устройствами. SNMP протокол работает по технологии клиент-сервер. В роли сервера выступает SNMP Агент, которые работает на управляемых устройствах, например коммутаторах. В роли клиента NMS (Network Management Station) — станция управления сетью. На коммутаторах SNR поддерживается только функции SNMP агента.

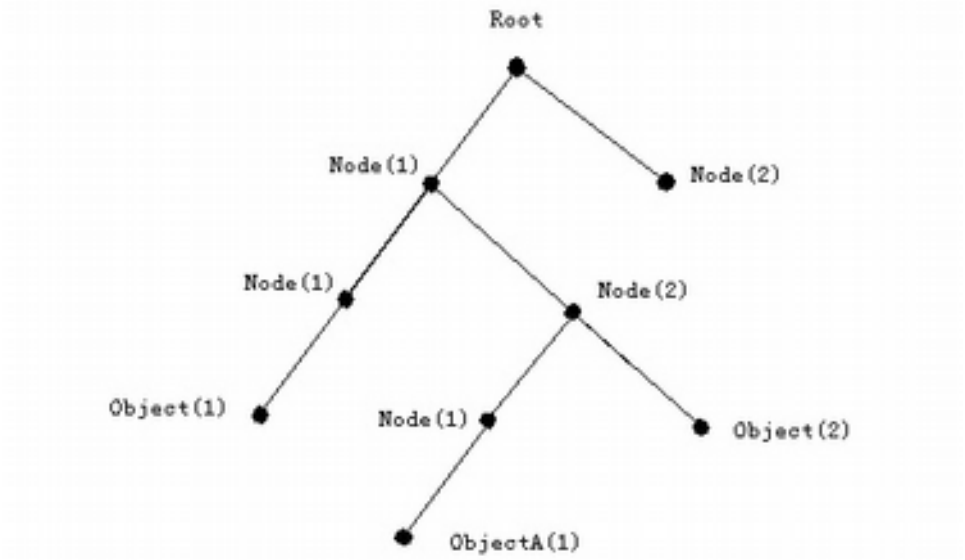
Обмен информацией между NMS и SNMP агентом осуществляется путем отправки стандартизированных сообщений. В SNMP определены 7 типов сообщений:

- Get-Request
- Get-Response
- Get-Next-Request
- Get-Bulk-Request
- Set-Request
- Trap
- Inform-Request

NMS может посылать следующие сообщения Агенту: Get-Request, Get-Next-Request, Get-Bulk-Request и Set-Request. Агент отвечает сообщением Get-Response. Так-же Агент может отсылать Trap сообщения на NMS для информирования о событиях, например UP/DOWN порта и.т.п. Сообщение Inform-Request используется для обмена информацией между NMS.

2.5.2 Описание MIB

Формат сообщений которыми обмениваются NMS и SNMP Агент описан в Management Information Base (MIB). Информация в MIB организована в виде иерархической древовидной структуры. Каждая запись содержит OID (object identifier) и короткое описание. OID состоит из набора чисел разделенных точками. Он определяет объект и его положение в дереве MIB как показано на рисунке.



Древовидная структура MIB

Как показано на рисунке, OID объекта A - 1.2.1.1. NMS зная этот OID может получить

значения данного объекта. Таким образом в MIB определяется набор стандартных объектов для управляемых устройств.Для просмотра базы MIB можно использовать специализированное ПО называемое MIB Browser.
MIB разделяются на публичные (public) и частные (private). Public MIB определяются RFC и являются общими для всех поддерживающих их Агентов, например MIB для управления интерфейсами - IF-MIB определенный в RFC 2863. Private MIB создаются производителями оборудования и соответственно поддерживаются только на оборудовании данного производителя.
SNMP агент на коммутаторах SNR поддерживает основные публичные MIB, такие как MIB-II, IF-MIB, BRIDGE-MIB и др. а также Private SNR MIB.

2.5.3 Описание RMON

RMON это расширение стандарта SNMP. База RMON MIB обладает улучшенным набором свойств для удаленного управления, так как содержит агрегированную информацию об устройстве, не требующую передачи по сети больших объемов информации. Объекты RMON MIB включают дополнительные счетчики ошибок в пакетах, более гибкие средства анализа трендов и статистики, более мощные средства фильтрации для захвата и анализа отдельных пакетов, а также более сложные условия установления сигналов предупреждения. Агенты RMON MIB более интеллектуальны по сравнению с агентами MIB-I или MIB-II и выполняют значительную часть работы по обработке информации об устройстве, которую раньше выполняли менеджеры.
RMON содержит 10 групп. Коммутаторы SNR поддерживают наиболее часто используемые группы 1,2,3 и 9:

- **Statistics** - текущие накопленные статистические данные о характеристиках пакетов, количестве коллизий и т. п.
- **History** - статистические данные, сохраненные через определенные промежутки времени для последующего анализа тенденций их изменений.
- **Alarms** - пороговые значения статистических показателей, при превышении которых агент RMON посылает сообщение менеджеру.
- **Event** - условия регистрации и генерации событий.

Группы Alarm и Event позволяют отслеживать изменения любых количественных показателей в сети и оповещать при их превышении.

2.5.4 Настройка SNMP

1. Включение/отключение SNMP агента

Команда	Описание

`snmp-server enable`
 	
`no snmp-server enable`
В режиме глобальной конфигурации
	Включение SNMP Агента на коммутаторе
	
	Отключение SNMP Агента на коммутаторе

2. Настройка SNMP community

Команда	Описание
`snmp-server community {ro | rw} {0 | 7} <string> [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}] [read <read-view-name>] [write <write-view-name>]`	Настройка SNMP community `ro` - только чтение `rw` - чтение и запись `0` - community в открытом виде `7` - community в зашифрованном виде `<string>` - SNMP community `<num-std>|<name>` - номер или имя IP ACL со списком разрешенных адресов для данного community `<ipv6-num-std>|<ipv6-name>` номер или имя IPv6 ACL со списком разрешенных адресов для данного community `<read-view-name>` - Имя SNMP View для чтения `<write-view-name>` имя SNMP View для чтения и записи
`no snmp-server community <string> [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]` В режиме глобальной конфигурации	Удаление SNMP community

3. Настройка ограничения доступа к SNMP серверу

Команда	Описание

`snmp-server securityip enable`
 	
`snmp-server securityip disable`
 	
В режиме глобальной конфигурации
	Включение ограничения доступа к SNMP серверу
	
	Отключение ограничения доступа к SNMP серверу

`snmp-server securityip {<ipv4-address>|<ipv6-address> }`
 	
`no snmp-server securityip {<ipv4-address>|<ipv6-address> }`
 	
В режиме глобальной конфигурации
	Добавление адреса `<ipv4-address>|<ipv6-address>` к списку разрешенных адресов для доступа к SNMP серверу
	
	Удаление `<ipv4-address>|<ipv6-address>` из списка разрешенных адресов для доступа к SNMP серверу

4. Настройка engine ID

Команда	Описание

`snmp-server engineid <engine-string>`
 	
`no snmp-server engineid`
 	
В режиме глобальной конфигурации
	Настройка engine-id `<engine-string>` для SNMPv3 сервера
	
	Отмена engine-id

5. Настройка пользователя SNMP

Команда	Описание

`snmp-server user <user-string> <group-string> [{authPriv {3des|aes|des} <key> | authNoPriv } auth {md5 | sha} <pass>] [access {<num-std>| <name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]`
 	
`no snmp-server user <user-string> [access {<num-std>| <name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]`
 	
В режиме глобальной конфигурации
	Добавление пользователя в группу SNMP
	`<user-string>` - имя пользователя
	`<group-string>` - имя SNMP группы
	`authPriv` - использовать шифрование данных
	`3des|aes|des`
	`<key>` - ключ
	`authNoPriv` – Не использовать шифрование данных
	`auth {md5 | sha}` – использовать аутентификацию md5 или sha
	`<pass>` - пароль
	`<num-std>|<name>` - номер или имя IP ACL со списком разрешенных адресов для данного пользователя
	`<ipv6-num-std>|<ipv6-name>` номер или имя IPv6 ACL со списком разрешенных адресов для данного пользователя
	
	удаление SNMP пользователя либо ограничения доступа пользователя по ACL

6. Настройка SNMP группы

Команда	Описание

snmp-server group <group-string> {noauthnopriv|authnopriv|authpriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]] [access {<num-std>|<name>}] [ipv6-access <ipv6-num-std>|<ipv6-name>}] no snmp-server group <group-string> {noauthnopriv|authnopriv|authpriv} [access {<num-std>|<name>}] [ipv6-access <ipv6-num-std>|<ipv6-name> В режиме глобальной конфигурации	Создание SNMP группы <group-string> - имя группы noauthnopriv - без шифрования паролей и данных authnopriv - шифрование паролей без шифрования данных authpriv - шифрование и паролей и данных <read-string> - имя SNMP View с доступом только на чтение <write-string> - имя SNMP View с доступом на чтение и запись <notify-string> - имя SNMP View с правами на уведомления <num-std>|<name> - номер или имя IP ACL со списком разрешенных адресов для данной группы <ipv6-num-std>|<ipv6-name> номер или имя IPv6 ACL со списком разрешенных адресов для данной группы Удаление группы SNMP <group-string> либо ограничения доступа по ACL для группы

7. Настройка SNMP View

Команда	Описание
snmp-server view <view-string> <oid-string> {include|exclude} no snmp-server view <view-string> [<oid-string>] В режиме глобальной конфигурации	Настройка SNMP View <view-string> - имя SNMP View <oid-string> - OID include - добавить OID в View exclude - исключить OID из View Удаление SNMP View <view-string> либо отмена настройки <oid-string> для данного SNMP View

8. Настройка SNMP TRAP

Команда	Описание

`snmp-server enable traps`
 	
`no snmp-server enable traps`
 	
В режиме глобальной конфигурации
	Глобальное включение SNMP Trap
	
	Отключение SNMP Trap

`snmp-server host {<host-ipv4-address> | <host-ipv6-address>} {v1|v2c| {v3 {noauthnopriv | authnopriv | authpriv}}} <string>`
 	
`no snmp-server host {<host-ipv4-address> | <host-ipv6-address> } {v1 | v2c | {v3 {noauthnopriv | authnopriv | authpriv}}} <string>`
 	
В режиме глобальной конфигурации
	Настройка ipv4/ipv6 адреса `<host-ipv4-address>/<host-ipv6-address>` на который будут отсылаться Trap сообщения
	`v1|v2c|v3` - Версия SNMP Trap
	`noauthnopriv|authnopriv|authpriv` - настройки шифрования (только для SNMPv3)
	`<string>` - community (для SNMPv1/v2c); имя пользователя для SNMPv3
	
	Удаление ipv4/ipv6 адреса для отправки Trap сообщения с community `<string>`

`snmp-server trap-source {<ipv4-address> | <ipv6-address>}`
 	
`no snmp-server trap-source {<ipv4-address> | <ipv6-address>}`
 	
В режиме глобальной конфигурации
	Настройка ipv4/ipv6 адреса коммутатора для отправки SNMP Trap сообщений
	
	Отмена настройки ipv4/ipv6 адреса коммутатора для отправки SNMP Trap сообщений

`[no] switchport updown notification enable` В режиме конфигурации порта	Включение/отключение отсылки трапов при изменении статуса порта UP/Down. По умолчанию вкл.

9. Включение/отключение RMON

Команда	Описание

`rmon enable`
 	
`no rmon enable`
 	
В режиме глобальной конфигурации
	Включить RMON
	
	Отключить RMON

2.5.5 Примеры настройки SNMP

Во всех примерах IP-адрес NMS - 1.1.1.5, ip-адрес SNMP-агента (коммутатора) 1.1.1.9.
Сценарий 1: NMS используется для получения данных через SNMP с коммутатора.

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server community rw private
Switch(config)#snmp-server community ro public
Switch(config)#snmp-server securityip 1.1.1.5
```

NMS использует SNMP community `public` с правами только на чтение, community `private` имеет права на чтение и запись.

Сценарий 2: NMS используется для получения SNMP Trap с коммутатора с community `usertrap`

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server host 1.1.1.5 v1 usertrap
Switch(config)#snmp-server enable traps
```

Сценарий 3:NMS использует SNMPv3 для получения данных с коммутатора с пользователем `tester`, паролем `hellotst` и доступом на чтение, запись и уведомления на всю ветку OID с .1.

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server user tester UserGroup authnoPriv auth md5
hellotst
Switch(config)#snmp-server group UserGroup AuthnoPriv read max write
max notify max
Switch(config)#snmp-server view max 1 include
```

2.5.6 SNMP Troubleshooting

При возникновении проблем с получением или отправкой данных с SNMP сервера на коммутатор проверьте следующие пункты:

- Соединение между SNMP сервером и коммутатором утилитой ping
- На коммутаторе включен SNMP агент (команда `sh snmp status`)
- IP-адрес NMS правильно сконфигурирован в команде `snmp-server securityip`
- SNMP Community для SNMPv1/v2 или аутентификация для SNMPv3 правильно

сконфигурирована и совпадает с конфигурацией на NMS.

- Используя команду `sh snmp` проверьте что коммутатор получает и отправляет пакеты. Также можно использовать команду `debug snmp packet` для вывода отладочной информации о работе SNMP агента.

3. Обновление ПО коммутатора

3.1 Системные файлы коммутатора

Для работы коммутатора необходимы два файла - образ ПО (system image) и загрузчик (BootRom). При обновлении коммутатора необходимо обновить system image и в случае если версия BootRom на коммутаторе младше чем в архиве с прошивкой, то BootRom также необходимо обновить.
Образ ПО (system image) имеет расширение nos.img и хранится на Flash памяти коммутатора обычно с именем nos.img.
Загрузчик (BootRom) предназначен для инициализации коммутатора при включении и обязательно должен храниться на коммутаторе с именем boot.rom. Версию boot.rom и образа ПО можно посмотреть в выводе команды sh version

3.2 Обновление через boot-меню

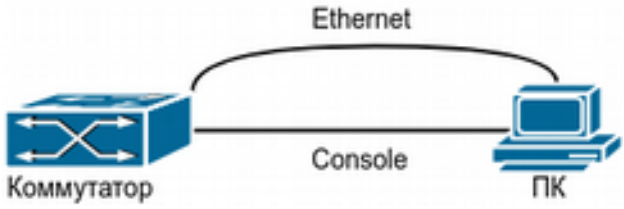


рисунок 2.6.1 обновление через boot-меню

Один из способов обновления коммутатора - через boot-меню по TFTP. В целях безопасности на данном коммутаторе отсутствует возможность записать файл NOS через boot-меню. Тем не менее загруженный NOS может быть запущен, а файл boot.rom может быть обновлен через boot-меню.

Шаг 1. Как показано на рисунке 2.6.1, ПК необходимо подключить одновременно к консольному порту, а также к одному из Ethernet портов коммутатора. ПК должен поддерживать функцию TFTP-сервера.

Шаг 2. Во время загрузки, сразу после включении коммутатора в сеть нажмите сочетание клавиш Ctrl+B и перейдите в boot-меню:

```
[Boot]:
```

Шаг 3. С помощью команды “setconfig” задайте IP-адрес и маску подсети для коммутатора и IP-адрес и маску подсети для сервера:

```
[Boot]: setconfig
Host IP Address: [10.1.1.1] 192.168.1.2
Server IP Address: [10.1.1.2] 192.168.1.66
```

Шаг 4. Загрузите актуальный файл boot.rom и nos.img в корень TFTP-сервера. Для обновления boot.rom примените команду “**load boot.rom**”, а после успешной передачи “**write boot.rom**”:

```
      [Boot]: load boot.rom
      TFTP from server 192.168.1.66; our IP address is 192.168.1.2
      Filename 'boot.rom'.
      Load address: 0x81000000
      Loading:
##################################################################
            ################################
      done
      Bytes transferred = 438700 (6b1ac hex)
      [Boot]:
      [Boot]: write boot.rom
      File exists, overwrite? (Y/N)[N] y


      Writing flash:/boot.rom......
      Write flash:/boot.rom OK.

      [Boot]:
```

Шаг 5. После успешного обновления примените **run** или **reboot** для возврата в NOS. Команда **run** может быть применена вместе с параметров **tftp:nos.img** для загрузки и старта NOS.

3.3 TFTP и FTP

3.3.1 Общие сведения о TFTP и FTP

FTP(File Transfer Protocol)/TFTP(Trivial File Transfer Protocol) - протоколы передачи данных 4го уровня, используют в своей работе TCP\IP стек.

FTP использует TCP для обеспечения надежной передачи данных, однако использует простой механизм проверки подлинности. Для передачи данных FTP устанавливает 2 соединения: соединение управления (21 порт) и соединение для передачи данными (20 порт). FTP может использовать для соединения 2 режима: активный и пассивный.

В активном с клиент передает свой IP адрес и номер порта для передачи данных на сервер, соединение управления поддерживается до завершения передачи данных. Затем, используя адрес и номер порта клиента, сервер устанавливает соединение для передачи данных на порту 20, если порт свободен. При пассивном соединении клиент устанавливает через соединение управления уведомляет сервер о создании пассивного соединения и получает от сервера его IP-адрес и номер порта, которые затем используются клиентом для открытия соединения данных с произвольного клиентского порта к полученному адресу и порту.

TFTP использует UDP и не подразумевает механизмы аутентификации. Он обеспечивает правильность переданных данных с помощью механизма отправки, подтверждения и повторной передачи по тайм-ауту. Преимущество TFTP перед FTP состоит в том, что

использование TFTP проще. Он может быть использован для передачи служебных данных, не требующих защиты.
Коммутатор может использоваться в качестве FTP или TFTP-клиента или сервера. С помощью FTP или TFTP клиента на коммутатор могут быть загружены файлы конфигурации, NOS или bootROM не влияя на работу его остальных функций. Коммутатор также может предоставлять функцию FTP или TFTP сервера для передачи находящихся в его памяти файлов.

3.3.2 Конфигурация TFTP и FTP

1. Использование TFTP и FTP клиента:
    a. Принять\передать файлы через TFTP или FTP;
    b. Получить список файлы через FTP;
2. Конфигурация FTP сервера:
    a. Запустить FTP сервера;
    b. Задать логин и пароль для FTP;
    c. Задать таймаут соединения;
3. Конфигурация TFTP сервера:
    a. Запустить TFTP сервер;
    b. Задать таймаут получения подтверждения;
    c. Задать число повторных передач;

1. Использование TFTP и FTP клиента:
    a. Принять\передать файлы через TFTP или FTP:

Команда	Описание
`copy <source-url> <destination-url>` В Admin режиме	Принять передать файлы через FTP или TFTP. В качестве одного из аргументов `<source-url>` или `<destination-url>` должен быть использован URL файла на TFTP/FTP сервере, в качестве другого - имя файла на в памяти коммутатора. При использовании FTP сервера должен применяться следующий формат URL: `ftp: //user:password@IPv4|IPv6 Address`.

    b. Получить список файлы через FTP:

Команда	Описание
`ftp-dir <ftpServerUrl>` В Admin режиме	Получить список файлов каталога по FTP. В качестве `<ftpServerUrl>` должен быть использован следующий формат: `ftp: //user:password@IPv4|IPv6 Address`

2. Конфигурация FTP сервера:
   a. Запустить FTP сервера:

Команда	Описание
ftp-server enable no ftp-server enable В режиме глобальной конфигурации	Включить функцию FTP-сервера. Команда `no` отключает эту функцию.

   b. Задать логин и пароль для FTP:

Команда	Описание
ip ftp username <*username*> password [0 | 7] <*password*> no ip ftp username<*username*> В режиме глобальной конфигурации	Задать имя FTP пользователя и пароль. Команда `no` восстанавливает использование анонимного пользователя.

   c. Задать таймаут соединения:

Команда	Описание
ftp-server timeout <*seconds*> no ftp-server timeout В режиме глобальной конфигурации	Задать тайм-аут для FTP соединения. Команда `no` восстанавливает конфигурацию по-умолчанию - 600 секунд.

3. Конфигурация TFTP сервера:
   a. Запустить TFTP сервер:

Команда	Описание
tftp-server enable no tftp-server enable В режиме глобальной конфигурации	Включить функцию TFTP-сервера. Команда `no` отключает эту функцию.

   b. Задать таймаут передачи:

Команда	Описание
`tftp-server transmission-timeout` <*seconds*> В режиме глобальной конфигурации	Задать тайм-аут передачи. Команда no восстанавливает конфигурацию по-умолчанию - 600 секунд.

   c. Задать число повторных передач:

Команда	Описание
`tftp-server retransmission-number <number>` В режиме глобальной конфигурации	Задать число повторных передачи. Команда no восстанавливает конфигурацию по-умолчанию - 5.

3.3.3 Пример конфигурации TFTP и FTP

Пример 1: коммутатор используется в качестве FTP и TFTP клиента. FTP/TFTP-сервер с адресом 10.1.1.1 подключен к одному из портов коммутатора.
Интерфейс управления коммутатором имеет IP адрес 10.1.1.2. Необходимо обновить ПО коммутатора, загрузив файл образа новой версии NOS “nos.img”.

Использование **FTP**:
В корневом каталоге пользователя “admin” FTP сервера расположен файл образа последней версии ПО коммутатора “7.0.3.5(R0241.0280)nos.img”. Пароль пользователя admin - “switch”.

```
Switch#copy ftp://admin:switch@10.1.1.1/7.0.3.5(R0241.0280)nos.img
nos.img
```

Использование **TFTP**:
В корневом каталоге TFTP сервера расположен файл образа последней версии ПО коммутатора “7.0.3.5(R0241.0280)nos.img”.

```
Switch#copy tftp: //10.1.1.1/12_30_nos.img nos.img
```

Пример 2: коммутатор используется как FTP сервер. Для доступа к нему используется имя пользователя “admin”, пароль - “switch”.

Конфигурация коммутатора:

```
Switch(config)#ftp-server enable
Switch(config)# username Admin password 0 superuser
```

Пример 3: коммутатор используется как TFTP сервер.

Конфигурация коммутатора:

```
Switch(config)#tftp-server enable
```

3.3.4 Решение проблем с TFTP и FTP

- Ниже показан лог коммутатора при передаче файла по FTP с помощью команды

copy. Если лог на вашем коммутаторе отличается, проверьте IP связность и конфигурацию FTP сервера и попробуйте выполнить копирование снова.

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
nos.img file length = 1526021
read file ok
send file
150 Opening ASCII mode data connection for nos.img.
226 Transfer complete.
close ftp client.
```

- Ниже показан лог коммутатора при приеме файла по FTP с помощью команды copy. Если лог на вашем коммутаторе отличается, проверьте IP связность и конфигурацию FTP сервера и попробуйте выполнить копирование снова.

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
recv total = 1526037
**********************
write ok
150 Opening ASCII mode data connection for nos.img (1526037 bytes).
226 Transfer complete.
```

- Ниже представлен лог успешной передачи файла по TFTP с помощью команды copy. Если лог на вашем коммутаторе отличается, проверьте IP связность и конфигурацию TFTP сервера и попробуйте выполнить копирование снова:

```
nos.img file length = 1526021
read file ok
begin to send file, wait...
file transfers complete.
Close tftp client.
```

- Ниже представлен лог успешного приема файла по TFTP с помощью команды copy. Если лог на вашем коммутаторе отличается, проверьте IP связность и конфигурацию FTP сервера и попробуйте выполнить копирование снова.

```
begin to receive file, wait...
recv 1526037
**********************
write ok
```

```
transfer complete
close tftp client.
```

- Если на коммутаторе происходит обновление системных файлов с помощью TFTP/FTP, не перезагружайте коммутатор до тех пор, пока не появится сообщение “close tftp client” или “close ftp client” или “226 Transfer complete”, иначе коммутатор может не загрузится. Если это все же произошло и коммутатор не загружается, попробуйте зайти в boot-меню и запустить NOS из него. При повреждении boot.rom может потребоваться ремонт в Сервисном Центре ООО “НАГ”.

4. Операции с файловой системой

4.1 Общие сведения о файловой системе коммутатора

В качестве устройства для хранения файлов используется встроенная FLASH-память. Обычно она используется для хранения файлов - образов ПО коммутатора (IMG файл), файла загрузки системы (ROM файл) и файлов конфигурации (CFG файл). FLASH может копировать, удалять и переименовывать файлы как в режиме работы NOS, так и в меню загрузчика.

4.2 Операции с файловой системой

1. Операция форматирования устройства;
2. Операция удаления файла;
3. Операция изменения имени;
4. Операция копирования.

1. Операция форматирования устройства:

Команда	Описание
`format <device>` В привилегированном режиме	Форматировать устройство `<device>`

2. Операция удаления файла:

Команда	Описание
`delete <file-url>` В привилегированном режиме	Удалить файл `<file-url>`

3. Операция изменения имени:

Команда	Описание
rename <*source-file-url*> <*dest-file*> В привилегированном режиме	Переименовать файл **<*file-url*>**

4. Операция копирования:

Команда	Описание
copy <*source-file-url*> <*dest-file-url*> В привилегированном режиме	Скопировать файл **<*source-file-url*>** в **<*dest-file-url*>**

4.3 Пример операций с файловой системой

Для бекапа образа ПО на flash создать копию файла nos.img с именем 241.0270_nos.img. После копирования проверить содержимое flash.

.

```
Switch#copy flash:/nos.img flash:/241.0270_nos.img
Copy flash:/nos.img to flash:/241.0270_nos.img ? [Y:N] y
Copyed file flash:/nos.img to flash:/241.0270_nos.img.

Switch#dir

total  25297K
-rw-       12.4M          241.0270_nos.img
-rw-       12.4M          nos.img
-rw-       1.1K           startup.cfg

Drive : flash:
Size:30.0M  Used:25.9M  Available:4.1M  Use:86%
```

5. Настройка интерфейсов

5.1 Общие сведения

Для настройки физического Ethernet интерфейса необходимо зайти в режим конфигурации интерфейса из режима глобального конфигурирования при помощи команды `Interface Ethernet <interface-list>`, где в `<interface-list>` должны быть указаны один или несколько номеров Ethernet интерфейсов. Специальные символы ";" и "-" служат для задания нескольких номеров интерфейсов. символ ";" предназначен для разделения отдельных номеров, "-" для задания диапазона интерфейсов.

Например командой `interface ethernet 1/0/2-5` осуществляется переход в режим конфигурирования интерфейсов из диапазона eth1/0/1-eth1/0/5. Команда `interface ethernet 1/0/2;5` переводит в режим конфигурирования интерфейсов 1/0/2 и 1/0/5.

5.2 Настройка параметров Ethernet интерфейсов

Вход в режим конфигурации Ethernet интерфейса

Команда	Описание
Global режим	
`interface ethernet <interface-list>`	Вход в режим конфигурирования Ethernet интерфейса

Команда	Описание
Режим конфигурации Ethernet интерфейса	
`media-type {copper | copper-preferred-auto | fiber | sfp-preferred-auto}`	Настройка режима работы Combo порта `copper` - только медь (RJ45) `copper-preferred-auto` - автоматический режим с приоритетом медного RJ45 порта `fiber` - только SFP `sfp-preferred-auto` - автоматический режим с приоритетом оптического SFP порта

`shutdown`
 	
`no shutdown`
	Административное отключение Ethernet интерфейса
	
	Административное включение Ethernet интерфейса

`description <string>`
 	
`no description`
	Конфигурация имени интерфейса `<string>`
	
	Удаление имени интерфейса

`speed-duplex {auto [10 [100 [1000]] [auto | full| half |]] | force10-half | force10-full | force100-half | force100-full | force100-fx | {force1g-full [nonegotiate [master | slave]]}}`
 	
`no speed-duplex`
	Настройка параметров скорости/дуплекса Ethernet интерфейса
	`auto` - автоматическое согласование скорости (можно указать определенные типы скоростей, которые будут разрешены при автосогласовании)
	`10` - 10 mb/s
	`100` - 100 mb/s
	`1000` - 1000 mb/s
	`auto` - автоматическое согласование дуплекса
	`full` - задать полный дуплекс
	`half` - задать полудуплекс
	`force10-half` - принудительно перевести интерфейс в режим 10 mb/s half-duplex
	`force10-full` - принудительно перевести интерфейс в режим 10 mb/s full-duplex
	`force100-full` - принудительно перевести интерфейс в режим 100 mb/s full-duplex
	`force100-half` - принудительно перевести интерфейс в режим 100 mb/s half-duplex
	`force100-fx` - принудительно перевести интерфейс в режим 100BaseX (100 mb/s full-duplex SFP)
	`force1g-full` - принудительно перевести интерфейс в режим 1000 mb/s full-duplex
	`nonegotiate` – отключение автосогласования в режиме 1000 mb/s full-duplex
	`master` - принудительно перевести интерфейс в режим master
	`slave`- принудительно перевести интерфейс в режим slave
	
	Вернуть настройки скорости-дуплекса по умолчанию (auto)

`negotiation {on|off}`	Включение/отключение режима автосогласования для портов 1000BaseX SFP (по умолчанию режим автосогласования включен)

`bandwidth control <bandwidth> [both | receive | transmit]`
 	
`no bandwidth control`
	Ограничения скорости трафика на интерфейсе
	`<bandwidth>` - ограничение скорости в kbps
	`both` - в обоих направлениях RX и TX
	`receive` - только на RX
	`transmit` - только на TX
	
	Отключить ограничение скорости трафика на порту

`flow control`
 	
`no flow control`
	Включить flow control на порту
	Отключить flow control на порту (по умолчанию)

`loopback`
 	
`no loopback`
	Включить loopback на порту (исходящие в интерфейс пакеты будут отправляться обратно)
	
	Отключить loopback на порту

`switchport flood-control { bcast|mcast|ucast}`
 	
`no switchport flood-control { bcast|mcast|ucast }`
	Запрет отправки broadcast, unknown ucast/mcast трафика в интерфейс
	`bcast` - запрет broadcast трафика
	`mcast` - запрет unknown multicast трафика
	`ucast` - запрет unknown unicast трафика
	отмена команды

`switchport flood-forwarding mcast`
 	
`no switchport flood-forwarding mcast`
	Разрешение отправки multicast трафика в порт без подписки при включенном igmp-snooping
	
	Отмена команды

`port-scan-mode {interrupt | poll}`	Настройка режима отслеживания статуса порта `interrupt` - статус порта определяется по прерыванию `poll` - статус порта периодически опрашивается (по-умолчанию)

`no port-scan-mode`	Возврат значения по умолчанию (poll)
Global режим	
`port-rate-statistics interval <interval-value>`	Настройка интервала за который рассчитывается средняя скорость на интерфейсе, `<interval-value>` интервал (5-600 с)

5.2.2 Пример настройки Ethernet интерфейса

Перевод SFP интерфейса в режиме 100BaseX (100mb/s)

```
SNR-S2985G-24T#conf
SNR-S2985G-24T(config)#interface ethernet 1/0/25
SNR-S2985G-24T(config-if-ethernet1/0/25)#speed-duplex force100-fx
```

Настройка автоопределения скорости 10/100 mb/s, duplex auto на гигабитном интерфейсе 1/0/24

```
SNR-S2985G-24T#conf
SNR-S2985G-24T(config)#interface ethernet 1/0/24
SNR-S2985G-24T(config-if-ethernet1/0/24)#speed-duplex auto 10 100 auto
```

Перевод интерфейса 1/0/1 в режим 100 мб/с full-duplex

```
SNR-S2985G-24T#conf
SNR-S2985G-24T(config)#interface ethernet 1/0/1
SNR-S2985G-24T(config-if-ethernet1/0/1)#speed-duplex force100-full
```

Возврат настроек интерфейса к значению по умолчанию (автоматическое согласование скорости/дуплекса)

```
SNR-S2985G-24T#conf
SNR-S2985G-24T(config)#interface ethernet 1/0/1
SNR-S2985G-24T(config-if-ethernet1/0/1)#no speed-duplex
```

5.3 Настройка ограничения Broadcast, Multicast, Unicast трафика на Ethernet интерфейсе

Коммутатор поддерживает два механизма ограничения входящего трафика - storm-control и rate-violation. Storm-control пропускает трафик до установленного лимита и отбрасывает все пакеты превышающие его. Rate-violation при достижении лимита блокирует весь трафик на порту или переводит порт в shutdown, при этом отсылается SNMP Trap и логируется информация о событии.

5.3.1 Настройка Storm-control

Команда	Описание
`storm-control {kbps | pps}` В режиме глобальной конфигурации	Настройка единиц измерения storm-control `kbps` – килобиты в секунду `pps` – пакеты в секунду

Команда	Описание

`storm-control { broadcast | multicast | unicast} <pps/kbps>`
 	
`no storm-control {broadcast | multicast | unicast}`
В режиме конфигурации порта
	Включение strom control на интерфейсе для определенного типа трафика
	`broadcast` - широковещательный трафик
	`multicast` - мультикаст трафик
	`unicast` - unknown Unicast
	`<pps/kbps>` - ограничение в pps (1-1488905) или kbps (16-1000000)
	
	Отмена ограничения для выбранного типа трафика

5.3.2 Настройка Rate-violation

Команда	Описание

`rate-violation {all | broadcast | multicast | unicast} <pps> }`
 	
`rate-violation control block | {shutdown [ recovery <sec> ]}`
	Включение rate-violation на интерфейсе для определенного типа трафика
	`all` - весь трафик
	`broadcast` - широковещательный трафик
	`multicast` - мультикаст трафик
	`unicast` - unknown Unicast
	`<pps>` - ограничение в pps (10-2000000)
	
	Настройка действия при превышении лимита
	`block` - блокировка всего трафика на порту
	`shutdown` - административное выключение порта
	`recovery <sec>` - таймер восстановления(включения) порта
	
	Отмена ограничения для выбранного типа трафика, отключение действия при превышении лимита

`no rate-violation {all | broadcast | multicast | unicast | control}` В режиме конфигурации порта	

5.3.3 Пример настройки ограничения входящих broadcast, multicast и unknown-unicast пакетов.

Настройка ограничения входящего broadcast и multicast трафика до 112 pps при помощи storm-control:

```
SNR-S2985G-24T#conf
SNR-S2985G-24T(config)#interface ethernet1/0/1
SNR-S2985G-24T(config-if-ethernet1/0/1)#storm-control broadcast 112
SNR-S2985G-24T(config-if-ethernet1/0/1)#storm-control multicast 112
```

Настройка ограничения broadcast трафика до 200 pps при помощи rate-violation с блокировкой трафика на порту при превышении лимита

```
SNR-S2985G-24T#conf
SNR-S2985G-24T(config)#interface ethernet1/0/1
SNR-S2985G-24T(config-if-ethernet1/0/1)#rate-violation broadcast 200
SNR-S2985G-24T(config-if-ethernet1/0/1)#rate-violation control block
```

5.4 Диагностика медного кабеля

5.4.1 Диагностика медного кабеля

Коммутаторы SNR поддерживают диагностику медного кабеля. В процессе диагностики проверяется длина кабеля, а также целостность каждой пары.

Возвращаются следующие статусы:
well - кабель подключен верно
short - короткое замыкание между проводами одной пары
open - кабель не подключен или есть разрыв
abnormal - ненормальное состояние линии, например короткое замыкание между разными парами
fail - не удалось проверить данную пару

Команда	Описание
`virtual-cable-test interface ethernet IFNAME`	Запуск тестирование кабеля интерфейса `IFNAME`

В режиме глобальной конфигурации	

5.4.2 Пример диагностики медного кабеля

Диагностика кабеля, подключенного к порту 1/0/24

```
SNR-S2985G-24T#virtual-cable-test interface eth1/0/24

Interface Ethernet1/0/24:
-------------------------------------------------
Cable pairs      Cable status     Length (meters)
-----------      ------------     ---------------
(1, 2)           well                        83
(3, 6)           well                        83
(4, 5)           well                        83
(7, 8)           well                        83
```

6. Настройка изоляции портов (port isolation)

6.1. Описание функционала изоляции портов

Изоляция портов (Port Isolation) это независимый функционал, который ограничивает передачу пакетов между определенными портами. Коммутаторы SNR-S2965 и SNR-S2985 поддерживают как полную изоляцию трафика между портами, так и изоляцию трафика в рамках определенного Vlan. Настройка функционала сводится к добавлению Ethernet интерфейсов в одну или несколько групп (isolate-port group). Порты внутри одной группы изолируются, то есть трафик между ними не передается. Порты принадлежащие разным isolate-port group или не добавленные ни в одну isolate-port group могут коммутировать пакеты между собой.
Изоляция портов внутри Vlan выполняется аналогично, только применяется к трафику в данном Vlan.

6.2 Настройка изоляции портов

6.2.1 Настройка полной изоляции портов

Создание isolate-port group

Команда	Описание

`isolate-port group <WORD>`
 	
`no isolate-port group <WORD>`
В режиме глобальной конфигурации
	Создание isolate-port group с именем `<WORD>`
	
	Удаление isolate-port group с именем `<WORD>`

Добавление портов в isolate-port group

Команда	Описание

`isolate-port group <WORD> switchport interface [ethernet] <IFNAME>`
 	
`no isolate-port group <WORD> switchport interface [ethernet] <IFNAME>`
В режиме глобальной конфигурации
	Добавление в isolate-port group `<WORD>` интерфейса `<IFNAME>`
	
	Удаление из isolate-port group `<WORD>` интерфейса `<IFNAME>`

6.2.2 Настройка изоляции портов в рамках Vlan

Создание isolate-port group внутри Vlan

Команда	Описание

`isolate-port group <WORD>`
 	
`no isolate-port group <WORD>`
В режиме глобальной конфигурации
	Создание isolate-port group с именем `<WORD>`
	
	Удаление isolate-port group с именем `<WORD>`

Добавление портов в isolate-port group внутри Vlan

Команда	Описание

`isolate-port group <WORD> switchport interface [ethernet] <IFNAME>`
 	
`no isolate-port group <WORD> switchport interface [ethernet] <IFNAME>`
В режиме глобальной конфигурации
	Добавление в isolate-port group `<WORD>` интерфейса `<IFNAME>`
	
	Удаление из isolate-port group `<WORD>` интерфейса `<IFNAME>`

6.2.3 Просмотр конфигурации изоляции портов

Команда	Описание
`show isolate-port group [ <WORD> ]` В режиме глобальной конфигурации	Просмотр конфигурации изоляции портов для всех групп либо для конкретной группы `<WORD>`

6.3 Примеры настройки изоляции портов

Настройка изоляции портов 1/0/2 и 1/0/3 (запрет коммутации трафика между портами 1/0/2 и 1/0/3)

```
SNR-S2985G-24T#conf
SNR-S2985G-24T(config)#isolate-port group 1
SNR-S2985G-24T(config)#isolate-port group 1 switchport interface
ethernet1/0/2
SNR-S2985G-24T(config)#isolate-port group 1 switchport interface
ethernet1/0/3
```

Настройка изоляции трафика в vlan 50 между портами 1/0/4 и 1/0/5

```
SNR-S2985G-8T#conf
SNR-S2985G-8T(config)#vlan 50
SNR-S2985G-8T(config-vlan50)#isolate-port group 2
SNR-S2985G-8T(config-vlan50)#isolate-port group 2 switchport interface
ethernet1/0/4
SNR-S2985G-8T(config)#isolate-port group 2 switchport interface ethernet1/0/5
```

7. Loopback detection

7.1 Общие сведения о функции Loopback detection

Петля коммутации (loopback) - состояние в сети, при котором коммутатор принимает кадры, отправленные им же. При получении кадра впервые, коммутатор добавляет мак-адреса источника в таблицу, создавая соответствие с тем портом, на котором был получен кадр. Следующий кадр с данным мак-адресом получателя будет отправлен в на порт в соответствии с таблицей. Когда MAC-адрес источника уже изучен коммутатором, но кадр тем же MAC-адресом получен через другой порт, коммутатор меняет соответствие для MAC-адреса в таблице. В результате, если на порту существует петля, из-за наличия широковещательных и многоадресных кадров может произойти не только лавинный рост количества таких кадров - все MAC-адреса в пределах L2 сегмента сети будут изучены на порту с пелтей, что вызовет потерб работоспособности сети.
Избежать возникновения петель коммутации поможет функция Loopback detection. С её помощью порт с петлей будет автоматически заблокирован, а коммутатор может послать уведомление в систему мониторинга для своевременного обнаружения петли администратором.

7.2 Конфигурация Loopback detection

1. Настроить таймеры;
2. Включить функцию Loopback detection;
3. Настроить действие при обнаружении петли;
4. Отобразить информацию о конфигурации и отладочную информацию;
5. Включить отправку trap.

1. Настроить таймеры:

Команда	Описание

`loopback-detection interval-time <loopback> <no-loopback>`
`no loopback-detection interval-time`
 	
В режиме глобальной конфигурации
	Задать интервал в секундах отправки BPDU. *<loopback>* - после того, как петля была обнаружена; *<no-loopback>* - если петля не была обнаружена. Команда no восстанавливает значения по-умолчанию - 5 для `loopback` и 3 для `no-loopback`.

`loopback-detection control-recovery timeout <0-3600>` В режиме глобальной конфигурации	Задать время восстановления после выключена порта при обнаружении петли. После применения значения **0** восстановление не происходит автоматически (по-умолчанию).

2. Включить функцию Loopback detection:

Команда	Описание

`loopback-detection specified-vlan <vlan-list>`
`no loopback-detection specified-vlan <vlan-list>`
 	
В режиме конфигурации интерфейса
	Задать VLAN `<vlan-list>` для которых будет проверяться наличие петли. Команда `no` удаляет эту конфигурацию.

3. Настроить действие при обнаружении петли:

Команда	Описание
`loopback-detection control {shutdown |block }` `no loopback-detection control`	Выбрать действие при обнаружении петли. Команда `no` удаляет эту конфигурацию.

4. Отобразить информацию о конфигурации и отладочную информацию:

Команда	Описание

`debug loopback-detection`
`no debug loopback-detection`
 	
В Admin режиме
	Выводить отладочную информацию. Команда no отменяет вывод отладочной информации.

show loopback-detection [interface *<interface-list>*] В Admin режиме	Вывести информацию и состоянии и конфигурации Loopback-detection. Если указан параметр **interface *<interface-list>*** информация будет выведена только для указанного интерфейса.

5. Включить отправку trap:

Команда	Описание

`loopback-detection trap enable`
`no loopback-detection trap enable`
 	
В режиме глобальной конфигурации
	Включить отправку SNMP trap при обнаружении петли. Команда `no` отключает эту функцию.

7.3 Пример конфигурации Loopback detection

Чтобы защитить сеть от последствий возникновения петли коммутации из-за ошибки пользователя, неисправности линии или оборудования, подключенных к порту 1/0/1

коммутатора Switch, необходимо настроить функцию loopback-detection.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#loopback-detection interval-time 35 15
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#loopback-detection special-vlan 1-3
Switch(Config-If-Ethernet1/0/1)#loopback-detection control block
```

С выбранным действием при обнаружении петли - block, коммутатор будет блокировать весь трафик с порта в не зависимости от того, в каком VLAN была обнаружена петля. Для преодоления этой особенности существует возможность настроить MST Instance. В этом случае коммутатор будет блокировать трафик только в Isntance, содержащий VLAN с петлей.

Пример конфигурации MST Instance:

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1
Switch(Config-Mstp-Region)#instance 2 vlan 2
```

7.4 Решение проблем с конфигурацией Loopback detection

- Убедитесь, что оборудование, подключенное к интерфейсу с loopback detection, прозрачно пропускает Loopback-detection BPDU, иначе функция не будет работать;
- Рекомендуется использовать Loopback-detection только на портах в сторону неконтролируемого участка сети (порты доступа, сегменты с неуправляемыми коммутаторами);
- Не рекомендуется использовать loopback-detection на одном порту с протоколами STP, так как это может повлечь за собой некорректную работу STP или Loopback-detection;

8. ULDP

8.1 Общие сведения о ULDP

Однонаправленное соединение (Unidirectional Link) - состояние канала, при котором один порт может принимать данные от другого порта, но не может передавать их, или наоборот, может только передавать. Если при м на физическом уровне соединение установлено, проблема связи между устройствами не может быть обнаружена.
Однонаправленное соединение - распространенная проблема в сети, особенно для оптических соединений. Такое состояние может вызвать целый ряд проблем, таких как петлю коммутации при использовании протоколов STP и широковещательный шторм.
ULDP (Unidirectional Link Detection Protocol) - распознает удаленные устройства и проверяет статус соединений используя систему собственных сообщений. После отправки сообщения ULDP ждет ответ на него от удаленного устройства. Если ответ не приходит ULDP уведомляет пользователя о проблеме, а в зависимости от режима работы может заблокировать порт. Время жизни сообщения ULDP и интервал их отправки могут быть настроены пользователем и синхронизированы с удаленным устройством.

8.2 Конфигурация ULDP

1. Включить функцию ULDP;
2. Настроить режим работы;
3. Настроить метод выключения однонаправленного соединения;
4. Настроить интервалы и таймеры;
5. Сбросить состояние интерфейса;
6. Вывести информацию о конфигурации и отладке;

1. Включить функцию ULDP:

Команда	Описание

`uldp enable`
`uldp disable`
 	
В режиме глобальной конфигурации
	Включить/выключить ULDP глобально

`uldp enable`
`uldp disable`
 	
В режиме конфигурации порта
	Включить/выключить ULDP на порту

2. Настроить режим работы:

Команда	Описание
`uldp aggressive-mode` `no uldp aggressive-mode`	Включить глобально режим отключения порта при обнаружении однонаправленного

В режиме глобальной конфигурации	соединения. Команда `no` активирует режим normal - порт не будет выключен, функционал ограничится отправкой уведомления.

`uldp aggressive-mode`
`no uldp aggressive-mode`
 	
В режиме конфигурации порта
	Включить на порту режим отключения порта при обнаружении однонаправленного соединения. Команда `no` активирует режим normal - порт не будет выключен, функционал ограничится отправкой уведомления.

3. Настроить метод выключения однонаправленного соединения:

Команда	Описание

`uldp manual-shutdown`
`no uldp manual-shutdown`
 	
В режиме глобальной конфигурации
	Выбрать метод выключения порта с однонаправленным соединением. Команда no выбирает автоматический режим

4. Настроить интервалы и таймеры:

Команда	Описание
`uldp hello-interval` *`<integer>`* `no uldp hello-interval` В режиме глобальной конфигурации	Задать интервал отправки сообщений ULDP в секундах. Команда `no` восстанавливает значение по-умолчанию - 10.
`uldp recovery-time` *`<integer>`* `no uldp recovery-time` *`<integer>`* В режиме глобальной конфигурации	Задать время в секундах восстановления статуса порта после отключения протоколом ULDP. Команда no восстанавливает значение по-умолчанию - 0 (порт не будет восстановлен автоматически).

5. Сбросить состояние интерфейса:

Команда	Описание
`uldp reset` В режиме глобальной конфигурации	Сбросить состояние ULDP для всех портов.
`uldp reset` В режиме конфигурации порта	Сбросить состояние ULDP для текущего порта.

6. Вывести информацию о конфигурации и отладке:

Команда	Описание
`show uldp [interface ethernet IFNAME]` В Admin режиме	Вывести информацию о состоянии и конфигурации ULDP. Если задан параметр `[interface ethernet IFNAME]`, информация будет отображена только для заданного порта.

`debug uldp fsm interface ethernet <IFname>`
`no debug uldp fsm interface ethernet <IFname>`
 	
В Admin режиме
	Выводить отладочную информацию о работе процесса ULDP для интерфейса `<IFname>`. Команда `no` останавливает вывод

`debug uldp error`
`no debug uldp error`
 	
В Admin режиме
	Выводить отладочную информацию об ошибках в работе ULDP. Команда `no` останавливает вывод

`debug uldp event`
`no debug uldp event`
 	
В Admin режиме
	Выводить отладочную информацию о событиях в работе ULDP. Команда `no` останавливает вывод

`debug uldp packet {receive|send}`
`no debug uldp packet {receive|send}`
В Admin режиме
	Выводить отладочную информацию о пакетах ULDP, `receive` - принятых, `send` - отправленных. Команда `no` останавливает вывод.

`debug uldp {hello|probe|echo|unidir|all} [receive|send] interface ethernet <IFname>`
`no debug uldp {hello|probe|echo|unidir|all} [receive|send] interface ethernet <IFname>`
 	
В Admin режиме
	Выводить отладочную информацию о пакетах ULDP заданного типа `{hello|probe|echo|unidir|all}`, `receive` - принятых, `send` - отправленных, для интерфейса `<IFname>`. Команда `no` останавливает вывод.

8.3 Пример конфигурации ULDP

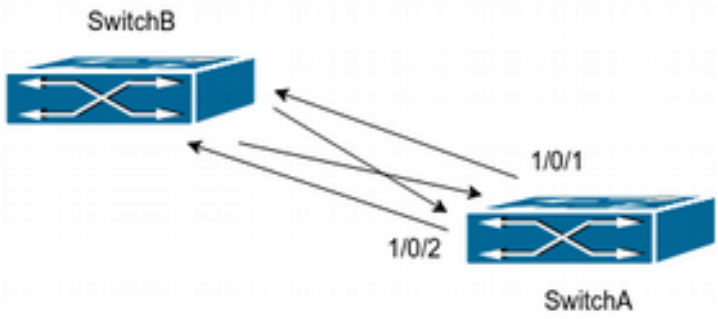


Рисунок 8.1 ULDP

Как показано на рисунке 8.1 коммутаторы соединены между собой двумя отдельными линиями. В результате ошибки при организации связи волокна, предназначенные для передачи трафика от коммутатора SwitchB коммутатору SwitchA оказались перепутаны местами. Физический уровень при этом будет работать нормально, но на канальном уровне будут возникать проблемы. ULDP обнаружит эту ситуацию и переведет порты в статус ошибки.

Конфигурация коммутаторов будет выглядеть следующим образом:

```
SwitchA(config)#uldp enable
SwitchA(config)#interface ethernet 1/0/1
SwitchA(Config-If-Ethernet1/0/1)#uldp enable
SwitchA(Config-If-Ethernet1/0/1)#exit
SwitchA(config)#interface ethernet 1/0/2
SwitchA(Config-If-Ethernet1/0/2)#uldp enable

SwitchB(config)#uldp enable
SwitchB(config)#interface ethernet1/0/3
SwitchB(Config-If-Ethernet1/0/3)#uldp enable
SwitchB(Config-If-Ethernet1/0/3)#exit
SwitchB(config)#interface ethernet 1/0/4
SwitchB(Config-If-Ethernet1/0/4)#uldp enable
```

При обнаружении проблем ULDP выведет следующие сообщения:

```
%Oct 29 11:09:50 2018 A unidirectional link is detected! Port Ethernet1/0/1 need to be shutted down!
%Oct 29 11:09:50 2018 Unidirectional port Ethernet1/0/1 shut down!
%Oct 29 11:09:50 2018 A unidirectional link is detected! Port Ethernet1/0/2 need to be shutted down!
%Oct 29 11:09:50 2018 Unidirectional port Ethernet1/0/2 shutted down!
Port g1/0/3, and port g1/0/4 of SWITCH B are all shut down by ULDP, and there is notification information on the CRT terminal of PC2.
```

```
     %Oct 29 11:09:50 2018 A unidirectional link is detected! Port
Ethernet1/0/3 need to be shutted down!
     %Oct 29 11:09:50 2018 Unidirectional port Ethernet1/0/3 shutted
down!
     %Oct 29 11:09:50 2018 A unidirectional link is detected! Port
Ethernet1/0/4 need to be shutted down!
     %Oct 29 11:09:50 2018 Unidirectional port Ethernet1/0/4 shutted
down!
```

8.4 Решение проблем с конфигурацией ULDP

- UDLP может обнаружить ненормальное состояние, если оба порта работают в дуплексном режиме и имеют одинаковую скорость;
- Интервал отправки сообщений Hello может быть изменен (в интервале от 5 до 100 секунд, по умолчанию - 10 секунд) для увеличения скорости реакции на ошибки. Но рекомендуется, чтобы этот интервал был менее 1/3 от времени сходимости STP, так как большее время может повлечь создание петли коммутации раньше, чем ULDP обнаружит проблему;
- LACP (LAG, Port-channel, Trunk port) прозрачен для ULDP, он работает на каждом линке как на независимом;
- Таймер восстановления отключен по умолчанию и будет включен только после его настройки;

9. LLDP

9.1 Общие сведения о LLDP

LLDP (Link Layer Discovery Protocol, 802.1ab) - протокол канального уровня, позволяющий коммутатору оповещать оборудование, работающее в локальной сети, о своем существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения. Каждое устройство LLDP может отправлять информацию о себе соседям независимо от того, отправляет ли сосед информацию о себе. Устройство хранит информацию о соседях, но не перенаправляет её. Коммутатор может передавать и принимать такую информацию, как: имя порта (Port name), идентификатор порта (PortID), аппаратный адрес (ChassisID), адрес управления (Management address), описание порта (PortDesc), описание устройства (SysDesc).

Полученная информация может быть запрошена с помощью стандартных SNMP MIB и использоваться в NMS для сбора информации и построения топологии сети.

9.2 Конфигурация LLDP

1. Включить функцию LLDP и настроить статус порта;
2. Настроить таймеры;
3. Настроить отправку Trap;
4. Настроить информацию, передаваемую опционально;
5. Настроить таблицу соседей;
6. Вывод информации и отладка.

1. Включить функцию LLDP и настроить статус порта:
2.

Команда	Описание

`lldp enable`
`lldp disable`
 	
В режиме глобальной конфигурации
	Включить LLDP глобально. Команда `no` отключает эту функцию

`lldp enable`
`lldp disable`
 	
В режиме конфигурации порта
	Включить LLDP на порту. Команда `no` отключает эту функцию

`lldp mode (send|receive|both| disable)` В режиме конфигурации порта	Настроить режим LLDP на порту, `send` - только отправка, `receive` - только прием, `both` - оба направления (по умолчанию)

3. Настроить таймеры:

Команда	Описание

`lldp tx-interval <integer>`
`no lldp tx-interval`
 	
В режиме глобальной конфигурации
	Настроить интервал отправки LLDP сообщений в секундах. Команда `no` восстанавливает конфигурацию по-умолчанию - 30 секунд.

`lldp msgTxHold <value>`
`no lldp msgTxHold`
 	
В режиме глобальной конфигурации
	Настроить количество интервалов `tx-interval` - время жизни информации о соседе LLDP с момента последнего обновления. Команда `no` восстанавливает конфигурацию по-умолчанию - 4.

`lldp transmit delay <seconds>`
`no lldp transmit delay`
 	
В режиме глобальной конфигурации
	Задать время в течении которого коммутатор не будет принимать новые LLDP сообщения на порту после получения последнего. Команда `no` восстанавливает конфигурацию по-умолчанию - 2 секунды.

4. Настроить отправку Trap:

Команда	Описание
`lldp trap <enable|disable>` В режиме конфигурации порта	Включить LLDP trap для порта. Команда `no` отключает эту функцию.

`lldp notification interval <seconds>`
`no lldp notification interval`
 	
В режиме глобальной конфигурации
	Задать время отправки trap после изменения LLDP таблицы. Команда `no` восстанавливает конфигурацию по-умолчанию - 5 секунд.

5. Настроить информацию, передаваемую опционально:

Команда	Описание

`lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]`
`no lldp transmit optional tlv`
 	
В режиме конфигурации порта
	Задать LLDP TLV отправляемые опционально:
	`portDesc` - description порта, `sysName` - имя коммутатора (hostname), `sysDesc` - описание коммутатора, `sysCap` - возможности системы. Команда `no` отключает опциональные tlv

`lldp management-address tlv [A.B.C.D]`
`no lldp management-address tlv`
 	
В режиме конфигурации порта
	Передавать в качестве `management-address tlv` адрес `[A.B.C.D]`. Команда `no` отключает эту функцию.

6. Настроить таблицу соседей:

Команда	Описание

`lldp neighbors max-num < value >`
`no lldp neighbors max-num`
 	
В режиме конфигурации порта
	Задать максимальное число соседей на порту. Команда `no` восстанавливает конфигурацию по-умолчанию - 100.

`lldp tooManyNeighbors {discard | delete}` В режиме конфигурации порта	Задать действие при получении информации от нового соседа при превышении максимального числа соседей. `delete` - удалить соседа с наименьшим временем жизни, `discard` - не записывать информацию о новом соседе (по-умолчанию).

7. Вывод информации и отладка:

Команда	Описание
`show lldp` В Admin режиме	Вывести суммарную информацию о конфигурации LLDP на коммутаторе.
`show lldp interface ethernet <IFNAME>` В Admin режиме	Вывести информацию по конфигурации LLDP на порту коммутатора.
`show lldp traffic` В Admin режиме	Вывести суммарную информацию об отправленных и полученных пакетах LLDP.
`show lldp neighbors interface ethernet < IFNAME >` В Admin режиме	Вывести информацию о соседях LLDP на интерфейсе

`debug lldp`
`no debug lldp`
 	
В Admin режиме
	Выводить отладочную информацию о работе протокола LLDP на коммутаторе. Команда **no** останавливает вывод информации.

`debug lldp packets interface ethernet <IFNAME>`
`no debug lldp packets interface ethernet <IFNAME>`
 	
В Admin режиме
	Выводить отладочную информацию о работе протокола LLDP на порту коммутатора. Команда **no** останавливает вывод информации.

`show debugging lldp` В Admin режиме	Вывести информацию о состоянии вывода отладки LLDP на коммутаторе.
`clear lldp remote-table` В режиме конфигурации порта	Очистить информацию о соседях LLDP на интерфейсе.

9.3 Пример конфигурации LLDP

2 коммутатора соединены друг с другом одним линком. Порт коммутатора Switch B настроен только для получение LLDP сообщений. Порт коммутатора Switch A должен передавать информацию о описании порта и возможностях системы.

Конфигурация коммутаторов будет выглядеть следующим образом:

```
SwitchA(config)# lldp enable
SwitchA(config)#interface ethernet 1/0/4
SwitchA(Config-If-Ethernet1/0/4)#lldp transmit optional tlv portDesc
sysCap
SwitchA(Config-If-Ethernet1/0/4)exit

SwitchB(config)#lldp enable
SwitchB(config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)#lldp mode receive
SwitchB(Config-If-Ethernet1/0/1)#exit
```

10. LLDP-MED

10.1 Общие сведения о LLDP-MED

LLDP MED (Link Layer Discovery Protocol-Media Endpoint Discovery) основан на стандарте 802.1AB LLDP и предоставляет расширенные возможности для управления конечными медиа-устройствами, такими как пользовательские маршрутизаторы (CPE) или IP-телефоны - для этого LLDP-MED предусматривает отправку специальных TLV.

10.2 Конфигурация LLDP-MED

1. Настроить передаваемые LLDP MED TLV;
2. Вывод информации и отладка;

1. Настроить передаваемые LLDP MED TLV:

Команда	Описание

`lldp transmit med tlv all`
`no lldp transmit med tlv all`
 	
В режиме конфигурации порта
	Включить на порту функцию отправки всех TLV LLDP-MED. Команда `no` отключает эту функцию.

`lldp transmit med tlv capability`
`no lldp transmit med tlv capability`
 	
В режиме конфигурации порта
	Включить на порту функцию отправки LLDP-MED Capability TLV. Команда `no` отключает эту функцию.

`lldp transmit med tlv networkPolicy`
`no lldp transmit med tlv networkPolicy`
 	
В режиме конфигурации порта
	Включить на порту функцию отправки LLDP-MED Network-Policy TLV. Команда `no` отключает эту функцию.

`lldp transmit med tlv extendPoe`
`no lldp transmit med tlv extendPoe`
 	
В режиме конфигурации порта
	Включить на порту функцию отправки LLDP-MED Extended POE TLV. Команда `no` отключает эту функцию.

`lldp transmit med tlv location`
`no lldp transmit med tlv location`
 	
В режиме конфигурации порта
	Включить на порту функцию отправки LLDP-MED location TLV. Команда `no` отключает эту функцию.

`lldp transmit med tlv inventory`
`no lldp transmit med tlv inventory`
 	
В режиме конфигурации порта
	Включить на порту функцию отправки LLDP-MED Inventory Management TLV. Команда **no** отключает эту функцию.

`network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-`	Настройка сетевой политики порта, передаваемой по LLDP-MED, включающая Vlan ID, поддерживаемые приложения,

video | video-signaling} [status {enable | disable}] [tag {tagged | untagged}] [vid {*<vlan-id>* | dot1p}] [cos *<cos-value>*] [dscp *<dscp-value>*] no network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} В режиме конфигурации порта	приоритет трафика. Команда no отменяет эту конфигурацию.
civic location {dhcp server | switch | endpointDev} *<country-code>* no civic location В режиме конфигурации порта	Задать тип устройства и код страны в соответствии с форматом Civic Address LCI и вход в режим Civic Address LCI. Команда **no** отменяет эту конфигурацию.
ecs location *<tel-number>* no ecs location В режиме конфигурации порта	Задать расположение в соответствии с форматом ECS ELIN. Команда no отменяет эту конфигурацию.
lldp med trap {enable | disable} В режиме конфигурации порта	Включить\отключить отправку trap сообщений при изменении соседей LLDP-MED.
{description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo} *<address>* no {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo} В режиме конфигурации Civic Address LCI	Задать расположение в режиме Civic Address LCI. Команда no отменяет эту конфигурацию.
lldp med fast count *<value>* no lldp med fast count В режиме глобальной конфигурации	Задать число LLDP-MED сообщений, отправляемых в первую секунду после обнаружения LLDP-MED устройства. Команда no возвращает конфигурацию по-умолчанию - 4.

2. Вывод информации и отладка:

Команда	Описание
`show lldp` В Admin режиме	Вывести суммарную информацию о конфигурации LLDP на коммутаторе.
`show lldp interface ethernet <IFNAME>` В Admin режиме	Вывести информацию по конфигурации LLDP на порту коммутатора.
`show lldp traffic` В Admin режиме	Вывести суммарную информацию об отправленных и полученных пакетах LLDP.
`show lldp neighbors interface ethernet < IFNAME >` В Admin режиме	Вывести информацию о соседях LLDP на интерфейсе

`debug lldp`
`no debug lldp`
 	
В Admin режиме
	Выводить отладочную информацию о работе протокола LLDP на коммутаторе. Команда `no` останавливает вывод информации.

`debug lldp packets interface ethernet <IFNAME>`
`no debug lldp packets interface ethernet <IFNAME>`
 	
В Admin режиме
	Выводить отладочную информацию о работе протокола LLDP на порту коммутатора. Команда `no` останавливает вывод информации.

`show debugging lldp` В Admin режиме	Вывести информацию о состоянии вывода отладки LLDP на коммутаторе.
`clear lldp remote-table` В режиме конфигурации порта	Очистить информацию о соседях LLDP на интерфейсе.

10.3 Пример конфигурации LLDP-MED

К порту Eth 1/0/1 оммутатора SwitchA подключен IP телефон, для его автоматической конфигурации используется LLDP-MED.

Конфигурация коммутатора:

```
SwitchA(config)#interface ethernet1/0/1
SwitchA (Config-If-Ethernet1/0/1)# lldp enable
SwitchA (Config-If-Ethernet1/0/1)# lldp transmit med tlv capability
SwitchA (Config-If-Ethernet1/0/1)# lldp transmit med tlv network
policy
SwitchA (Config-If-Ethernet1/0/1)# lldp transmit med tlv inventory
SwitchB (Config-If-Ethernet1/0/1)# network policy voice tag tagged vid
10 cos 5 dscp 15
SwitchA (Config-If-Ethernet1/0/1)# exit
```

Проверка конфигурации:

```
SwitchA# show lldp neighbors interface ethernet 1/0/1
Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :00-03-0f-00-00-02
PortIdSubtype :Local
PortId :1
PortDesc :****
SysName :****
SysDesc :*****

SysCapSupported :4
SysCapEnabled :4

LLDP MED Information :
MED Codes:
(CAP)Capabilities, (NP) Network Policy
(LI) Location Identification, (PSE)Power Source Entity
(PD) Power Device, (IN) Inventory
MED Capabilities:CAP,NP,PD,IN
MED Device Type: Endpoint Class III
Media Policy Type :Voice
Media Policy :Tagged
Media Policy Vlan id :10
Media Policy Priority :3
Media Policy Dscp :5
Power Type : PD
Power Source :Primary power source
Power Priority :low
Power Value :15.4 (Watts)
Hardware Revision:
Firmware Revision:4.0.1
```

```
Software Revision:6.2.30.0
Serial Number:
Manufacturer Name:****
Model Name:Unknown
Assert ID:Unknown
IEEE 802.3 Information :
auto-negotiation support: Supported
auto-negotiation support: Not Enabled
PMD auto-negotiation advertised capability: 1
operational MAU type: 1
```

11. LACP и агрегация портов

11.1 Общие сведения об агрегации портов

Агрегирование портов - это процесс объединения нескольких портов с одинаковой конфигурацией и для использования их логически в качестве одного физического порта (**Port-Channel**), что позволяет суммировать полосу пропускания в одном логическом линке и использовать резервирование. Для агрегации портов на коммутаторах SNR используется **Port-Group**, который должен быть создан и добавлен на порты для работы их как часть одного Port-Channel.

Для создания и корректной работы порты-члены интерфейса Port-Channel должны работать в дуплексном режиме (full-duplex) и иметь одинаковую конфигурацию.

После объединения физические порты могут конфигурироваться одновременно как один логический интерфейс Port-channel. Система автоматически установит порт с наименьшим номером в качестве Master port. Если на коммутаторе включен функционал spanning tree, STP будет рассматривать Port Channel как логический порт и отправлять кадры BPDU через Master port.

Коммутатор позволяет объединять физические порты любых двух коммутаторов, существует ограничение на максимальное число групп - 14, и максимальное число портов в каждой группе - 8.

11.1.1 Статическое агрегирование

Статическое агрегирование производится путем ручного конфигурирования пользователем и не требует использования протокола LACP. При конфигурировании статического агрегирования используется режим “on” для добавления порта в Port-Group.

11.1.2 Динамическое агрегирование LACP

LACP (Link Aggregation Control Protocol) - протокол агрегирования каналов, описанный в стандарте IEEE 802.3ad. LACP использует LACPDU сообщения для обмена информацией с соседней стороной.

После включения LACP порт посылает LACPDU, уведомляя ответную сторону о приоритете и MAC адресе системы, приоритете и адресе порта и ключе операции. Когда ответный порт получает эту информацию, он сравнивает её с информацией о своих портах, настроенных на агрегацию. Таким образом обе стороны достигают соглашения о включении или исключении порта из динамической группы агрегации.

В динамической группе агрегации порты имеют 2 статуса - выбранный (selected) и в ожидании (standby). Порты могут посылать и принимать LACPDU находясь в любом статусе, но в статусе standby порт не может передавать данные.

Поскольку существует ограничение на количество портов в группе, если текущее число членов агрегации превышает это ограничение, коммутатор согласовывает статус порта с другой стороной на основании port ID. Согласование происходит следующим образом:

1. Сравнение ID устройств (приоритет системы + MAC адресе системы). Если приоритет устройств одинаков - сравниваются MAC адреса устройств.

Наименьший номер будет иметь наивысший приоритет;
2. Сравнение ID портов (приоритет порта + идентификатор порта). Для каждого порта на стороне устройства с наивысшим приоритетом системы сравниваются приоритеты портов. Если приоритеты одинаковые - сравниваются ID портов. Порт с наименьшим идентификатором порта становится выбранным (selected), а остальные - в режим ожидания (standby).
3. В данной Port-Group порт с наименьшим идентификатором и статусом standby становится мастер-портом. Другие порты со статусом selected становятся членами группы.

11.2 Конфигурация агрегации портов

1. Создать Port-Group;
2. Добавить порт в Port-Group для агрегации, выбрать режим;
3. Войти в режим конфигурации Port-Channel;
4. Выбрать метод балансировки трафика;
5. Задать приоритет системы для LACP;
6. Задать приоритет порта для LACP;
7. Задать режим тайм-аута для LACP.

1. Создать Port-Group:

Команда	Описание

`port-group <port-group-number>`
`no port-group <port-group-number>`
 	
В режиме глобальной конфигурации
	Создать Port-Group. Команда `no` удаляет Port-Group.

2. Добавить порт в Port-Group для агрегации, выбрать режим:

Команда	Описание

`port-group <port-group-number>`
`mode {active | passive | on}`
`no port-group`
 	
В режиме конфигурации порта
	Добавить данный порт в Port-Group и выбрать режим агрегации. `active` - порт будет посылать сообщения LACPDU независимо от второй стороны; `passive` - порт будет ожидать получения LACPDU от ответной стороны; `on` - режим статической агрегации. Команда `no` удаляет порт из Port-Group.

3. Войти в режим конфигурации Port-Channel:

Команда	Описание
`interface port-channel <port-channel-number>`	Войти в режим конфигурации Port-Channel. `<port-channel-number>` - соответствует

В режиме глобальной конфигурации	`<port-group-number>` созданной Port-Group.

4. Выбрать метод балансировки трафика:

Команда	Описание

`load-balance {src-mac | dst-mac | dst-src-mac | src-ip | dst-ip | dst-src-ip | ingress-port | dst-src-mac-ip }`
`no load-balance`
 	
В режиме глобальной конфигурации
	Выбрать метод балансировки трафика для всех Port-Channel. Команда `no` возвращает метод по-умолчанию - `src-mac`.

5. Задать приоритет системы для LACP:

Команда	Описание

`lacp system-priority <system-priority>`
`no lacp system-priority`
 	
В режиме глобальной конфигурации
	Задать приоритет системы для LACP. Команда `no` возвращает приоритет по-умолчанию - 32768.

6. Задать приоритет порта для LACP:

Команда	Описание

`lacp port-priority <port-priority>`
`no lacp port-priority`
 	
В режиме конфигурации порта
	Задать приоритет порта для LACP. Команда `no` возвращает приоритет по-умолчанию - 32768.

7. Задать режим тайм-аута для LACP:

Команда	Описание

`lacp timeout {short | long}`
`no lacp timeout`
 	
В режиме конфигурации порта
	Выбрать режим таймаута порта для LACP. Команда `no` возвращает конфигурацию по-умолчанию - long.

11.3 Пример конфигурации агрегации портов

Сценарий 1: LACP

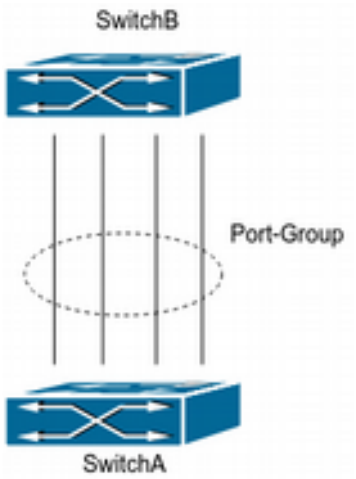


рисунок 11.1 LACP

Коммутаторы SwitchA и SwitchB соединены между собой с помощью 4х линий: порты 1/0/1-1/0/4 коммутатора SwitchA добавлены в port-group 1 в режиме active, порты 1/0/7-1/0/10 коммутатора SwitchB добавлены в port-group 2 в режиме passive. В результате конфигурации и согласований LACP порты 1/0/1-1/0/4 коммутатора SwitchA будут объединены в интерфейс “Port-Channel1”, а порты 1/0/7-1/0/10 коммутатора SwitchB будут объединены в интерфейс “Port-Channel2”.

Конфигурация будет выглядеть следующим образом:

```
SwitchA#config
SwitchA(config)#interface                ethernet                1/0/1-4
SwitchA(Config-If-Port-Range)#port-group       1       mode       active
SwitchA(Config-If-Port-Range)#exit
SwitchA(config)#interface                 port-channel                 1
SwitchA(Config-If-Port-Channel1)#

SwitchB#config
SwitchB(config)#port-group 2
SwitchB(config)#interface ethernet 1/0/7-10
SwitchB(Config-If-Port-Range)#port-group 2 mode passive
SwitchB(Config-If-Port-Range)#exit
SwitchB(config)#interface port-channel 2
SwitchB(Config-If-Port-Channel2)#
```

Сценарий 2: Ручное агрегирование портов

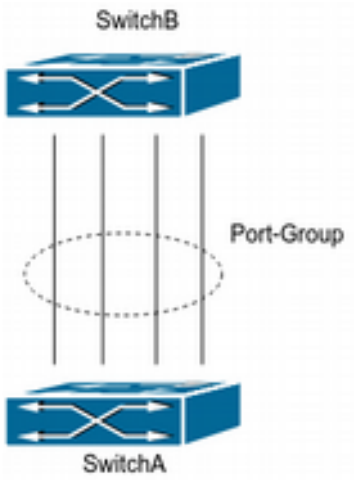


рисунок 11.2 Ручное агрегирование портов

Коммутаторы SwitchA и SwitchB соединены между собой с помощью 4х линий: порты 1/0/1-1/0/4 коммутатора SwitchA добавлены в port-group 1 в режиме on, порты 1/0/7-1/0/10 коммутатора SwitchB добавлены в port-group 2 в режиме on.

```
SwitchA#config
SwitchA(config)#interface                ethernet                1/0/1-4
SwitchA(Config-If-Port-Range)#port-group        1        mode         on
SwitchA(Config-If-Port-Range)#exit
SwitchA(config)#interface                 port-channel                 1
SwitchA(Config-If-Port-Channel1)#

SwitchB#config
SwitchB(config)#port-group 2
SwitchB(config)#interface ethernet 1/0/7-10
SwitchB(Config-If-Port-Range)#port-group 2 mode on
SwitchB(Config-If-Port-Range)#exit
SwitchB(config)#interface port-channel 2
SwitchB(Config-If-Port-Channel2)#
```

В результате выполнения конфигурации описанной выше порты добавляются в Port-Channel сразу, как только выполняется команда , задающая режим on. Обмен LACPDU не требуется.

11.4 Решение проблем при конфигурации агрегации портов

- Убедитесь , что все порты в группе имеют одинаковую конфигурацию, используются в режиме полного дуплекса и имеют одинаковую скорость.
- Некоторые команды, такие как arp, bandwidth, ip и ip-forward, не могут быть использованы на портах в Port-Group.

12. Настройка MTU

12.1 Общие сведения об MTU

MTU (Maximal Transmition Unit) означает максимальный размер кадра данных, который может быть передан без фрагментации. По умолчанию коммутатор отправляет\принимает кадры данных размером не более 1500 байт. Существует возможность разрешения работы с кадрами данных 1501-12270 байт.

12.2 Конфигурация MTU

Команда	Описание

`mtu [<mtu-value>]`
`no mtu`
 	
В режиме глобальной конфигурации
	Задать максимальный размер MTU пакетов в диапазоне 1500-12270 байт, принимаемых\отправляемых коммутатором. Команда `no` восстанавливает значение по-умолчанию - 1500байт.

13. EFM OAM

13.1 Общие сведения о EFM OAM

EFM OAM (Ethernet in the First Mile Operation, Administration and Maintenance) позволяет своевременно обнаруживать неисправности в канале данных, за счет чего повышая его надежность. Для своей работы использует канальный уровень: для обмен OAMPDU используется MAC-адрес назначения 01-80-c2-00-00-02.

Мониторинг канала.

В сети Ethernet затруднено обнаружение неисправности, когда соединение не разрывается, но работоспособность сети нарушена. EFM OAM обеспечивает мониторинг канала с помощью уведомлений OAMPDU. При обнаружении неисправности в канале модуль OAM посылает уведомление удаленному устройству, записывает это событие в лог и посылает SNMP Trap системе мониторинга. При получении уведомления о проблеме, удаленное устройство он так же записывает информацию в лог и отправляет уведомление системе мониторинга. Анализируя информацию в логах, сетевой администратор может отследить состояние канала в определенный период времени.
Мониторинг канала с помощью EFM OAM отслеживает следующие события:

- **Errored symbol period event**: количество ошибочных символов не может быть меньше нижнего порога ошибок (здесь символ — минимальный блок передачи информации в физической среде. Он уникален для системы кодировки, символы могут отличаться в разных физических средах. Скорость передачи символа определяется физической скоростью передачи в данной среде);
- **Errored frame event**: Определяет N как период фреймов, число ошибочных фреймов за период приема N фреймов не должно быть меньше нижнего порога ошибок (ошибочный фрейм определяется по CRC).
- **Errored frame period event**: количество определенных ошибочных фреймов за M секунд не должно быть меньше нижнего порога ошибок;
- **Errored frame seconds event**: количество секунд приема ошибочных фреймов зафиксированных за M секунд не может быть ниже порога ошибок.

Удаленное определение неисправностей

Когда в сети прерывается передача трафика из-за сбоя в работе устройства или его недоступности, Ethernet OAM модуль устанавливает соответствующий флаг в OAMPDU сообщениях, сообщая информацию о проблеме удаленному концу. Так как при активном соединении модули обмениваются пакетами OAMPDU постоянно, администратор по логам может отследить состояние канала и вовремя устранить неисправность.

Loopback-тестирование линии

После активации режима loopback-тестирования, работающий в активном режиме OAM порт посылает запрос loopback-тестирования соседу, в этом случае он возвращает все пакеты, за исключением Ethernet OAMPDU, отправителю по тому же каналу.
Периодическое выполнение тестирования помогает вовремя определить сетевые проблемы и локализовать их.

Важно: нормальная работа канала в режиме loopback-тестирования невозможна.

13.2 Конфигурация EFM OAM

1. Включить EFM OAM на порту;
2. Настроить мониторинг соединения;
3. Настроить обнаружение удаленных неисправностей;

1. Включить EFM OAM на порту:

Команда	Описание

`ethernet-oam`
`no ethernet-oam`
 	
В режиме конфигурации порта
	Включить функцию EFM OAM на порту. Команда `no` отключает эту функцию.

`ethernet-oam mode {active | passive}` В режиме конфигурации порта	Выбрать режим работы EFM OAM на порту: `active` (по-умолчанию) - коммутатор будет пытаться установить соединение на данном порту; `passive` - коммутатор будет ждать запроса на установление соединения.

`ethernet-oam period <seconds>`
`no ethernet-oam period`
 	
В режиме конфигурации порта
	Задать интервал отправки пакетов OAMPDU. Команда `no` восстанавливает значение по-умолчанию - 1 секунда.

`ethernet-oam timeout <seconds>`
`no ethernet-oam timeout`
 	
В режиме конфигурации порта
	Задать тайм-аут OAM сессии. Команда `no` восстанавливает значение по-умолчанию - 5 секунд.

2. Настроить мониторинг соединения:

Команда	Описание

`ethernet-oam link-monitor`
`no ethernet-oam link-monitor`
 	
В режиме конфигурации порта
	Включить отслеживание локальных ошибок в канале (по-умолчанию включено). Команда `no` отключает эту функцию.

`ethernet-oam errored-symbol-period {threshold low <low-symbols> | window <seconds>}` `no ethernet-oam errored-symbol-period`	Задать нижний порог ошибок и окно фиксации ошибочных символов. Команда `no` возвращает значение по-умолчанию (`<low-symbols>` - 1,

`{threshold low | window }` В режиме конфигурации порта	`window` - 5).

`ethernet-oam errored-frame-period {threshold low <low-frames> | window <seconds>}`
`no ethernet-oam errored-frame-period {threshold low | window }`
 	
В режиме конфигурации порта
	Задать нижний порог ошибок и окно фиксации периода ошибочных кадров. Команда `no` возвращает значение по-умолчанию (`<low-symbols>` - 1, `window` - 5).

`ethernet-oam errored-frame {threshold low <low-frames> | window <seconds>}`
`no ethernet-oam errored-frame {threshold low | window }`
 	
В режиме конфигурации порта
	Задать нижний порог ошибок и окно фиксации ошибочных кадров. Команда **no** возвращает значение по-умолчанию (`<low-symbols>` - 1, `window` - 5).

`ethernet-oam errored-frame-seconds {threshold low <low-frame-seconds> | window <seconds>}`
`no ethernet-oam errored-frame-seconds {threshold low | window }`
 	
В режиме конфигурации порта
	Задать нижний порог ошибок и окно фиксации секунд ошибочных кадров. Команда `no` возвращает значение по-умолчанию (`<low-symbols>` - 1, `window` - 300).

3. Настроить обнаружение удаленных неисправностей:

Команда	Описание

`ethernet-oam remote-failure`
`no ethernet-oam remote-failure`
 	
В режиме конфигурации порта
	Выключить режим отправки критических событий OAM (превышен `threshold high`) на порту через OAMPDU (по-умолчанию включено). Команда **no** отключает эту функцию.

`ethernet-oam errored-symbol-period threshold high {high-symbols | none}`
`no ethernet-oam errored-symbol-period threshold high`
 	
В режиме конфигурации порта
	Задать верхний порог ошибок приема символов за период. Команда `no` отключает этот порог.

`ethernet-oam errored-frame-period threshold high {high-frames | none}` `no ethernet-oam errored-frame-period`	Задать верхний порог ошибок приема кадров за период. Команда `no` отключает этот порог.

`threshold high` В режиме конфигурации порта	

`ethernet-oam errored-frame threshold high {high-frames | none}`
`no ethernet-oam errored-frame threshold high`
 	
В режиме конфигурации порта
	Задать верхний порог ошибок приема кадров. Команда `no` отключает этот порог.

`ethernet-oam errored-frame-seconds threshold high {high-frame-seconds | none}`
`no ethernet-oam errored-frame-seconds threshold high`
 	
В режиме конфигурации порта
	Задать верхний порог секунд ошибок приема кадров. Команда `no` отключает этот порог.

`ethernet-oam remote-loopback`
`no ethernet-oam remote-loopback`
 	
В режиме конфигурации порта
	Включить режим loopback-тестирования. Команда `no` отключает эту функцию

`ethernet-oam remote-loopback supported`
`no ethernet-oam remote-loopback supported`
 	
В режиме конфигурации порта
	Включить режим поддержки удаленного loopback-тестирования. Команда `no` отключает эту функцию.

13.3 Пример конфигурации EFM OAM

Коммутаторы оператора (PE) и клиента (CE) подключены друг к другу линией с использованием EFM OAM. При возникновении аварийных ситуаций информация о линии передается в систему мониторинга. Также при необходимости используется loopback-тестирование.

Конфигурация коммутатора клиента (CE):

```
CE(config)#interface ethernet 1/1
CE(config-if-ethernet1/1)#ethernet-oam mode passive
CE(config-if-ethernet1/1)#ethernet-oam
CE(config-if-ethernet1/1)#ethernet-oam remote-loopback supported
```

Конфигурация коммутатора оператора (PE):

```
PE(config)#interface ethernet 1/1
PE(config-if-ethernet1/1)#ethernet-oam
```

13.4 Решение проблем с конфигурацией EFM OAM

- Удостоверьтесь, что хотя бы один из соседей OAM находится в активном режиме;
- Для корректной доставки информации об аварии убедитесь, что SNMP настроен корректно;
- Соединение в режиме loopback-тестирования не работает. После проверки состояния линии необходимо отключить этот режим;
- Для корректной работы loopback-тестирования убедитесь, что на портах не сконфигурированы STP, MRPP, ULPP, flow control, loopback-detection, а оба устройства поддерживают функцию loopback-тестирования.

14. Port security

14.1 Общие сведения о Port-Security

Port-Security - механизм обеспечения безопасности и контроля доступа основанный на контроле изучаемых MAC-адресов. Может использоваться как дополнение существующей аутентификации 802.1x и аутентификации MAC. Port-security контролирует доступ неавторизованных устройств к сети, проверяя MAC-адрес источника принятого кадра и доступ к неавторизованным устройствам, проверяя MAC-адрес назначения отправленного кадра.
Если функционал port-security настроен на портах коммутатора, при получении кадра с неверным MAC-адресом, коммутатор запускает заданную пользователем функцию защиты порта и автоматически выполняет заданное действие.

14.2 Конфигурация Port-Security

1. Настроить port-security на порту;
2. Просмотр и очистка информации.

1. Настроить port-security на порту:

Команда	Описание

`switchport port-security`
`no switchport port-security`
 	
В режиме конфигурации порта
	Включить функцию port-security на порту. Команда no отключает эту функцию.

`switchport port-security mac-address {sticky | <mac-address> [vlan <vlan-id>]}`
`no switchport port-security {sticky | <mac-address> [vlan <vlan-id>]}`
 	
В режиме конфигурации порта
	Задать MAC адрес для текущего порта и VLAN (необязательно) ***<vlan-list>*** вручную. `sticky` - добавить следующий изученный адрес как статический. Команда `no` удаляет это соответствие.

`switchport port-security maximum <value> [vlan <vlan-list>]`
`no switchport port-security maximum <value> [vlan <vlan-list>]`
 	
В режиме конфигурации порта
	Задать максимальное количество MAC для текущего порта. Если применена команда `vlan <vlan-list>`, порог будет распространяться на указанные VLAN**.** Команда `no` восстанавливает конфигурацию по-умолчанию - 1 MAC для порта.

`switchport port-security violation {protect | recovery | restrict | shutdown}`	Выбрать действие при изучении нового MAC-адреса, если превышено заданное

`no switchport port-security violation` В режиме конфигурации порта	максимальное число адресов. `protect` - не изучать новый MAC, не отправлять уведомление; `recovery` - изучить новый MAC; `restrict` - не изучать новый MAC, отправить уведомление trap и запись в syslog; `shutdown` - выключить порт. Команда no восстанавливает конфигурацию по-умолчанию - shutdown.

2. Просмотр и очистка информации:

Команда	Описание
`clear port-security {all | configured | dynamic | sticky} [[address <mac-addr> | interface <interface-id>] [vlan <vlan-id> ]]` В Admin режиме	Очистить таблицу изученных MAC адресов: `all` - все, `dynamic` - изученных динамически; `configured` - добавленных вручную; добавленных функцией `sticky`.
`show port-security [interface <interface-id>] [address | vlan]` В Admin режиме	Отобразить информацию о конфигурации port-security

14.3 Пример конфигурации Port-Security

Сценарий

Оператор связи предоставляет пользователям услуги выхода в сеть, авторизация и ограничение полосы происходит на BRAS. Для предотвращения подмены MAC одного пользователя другими, на портах коммутатора доступа используется port-security. Функционал будет разрешать доступ только авторизованным устройствам и отправлять оповещение администратору при попытке изучения неизвестного адреса.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#interface Ethernet 1/0/1-1/0/24
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#exit
```

15. DDM

15.1 Общие сведения о DDM

DDM (Digital Diagnostic Monitor) реализует функцию диагностики по стандарту SFF-8472 MSA. DDM контролирует параметры сигнала и оцифровывает их на печатной плате оптического модуля. После чего информация может быть считана коммутаторов для мониторинга.

Обычно оптические модули поддерживают функцию DDM аппаратно, но её использование может быть ограничено программным обеспечением модуля. Устройства сетевого управления имеют возможность контролировать параметры (температура, напряжение, ток, мощности tx и rx) оптических модулей для получения их пороговых значений в режиме реального времени на оптическом модуле. Это помогает им обнаруживать неисправности в оптической линии, сокращать эксплуатационную нагрузку и повышать надежность сетевой системы в целом.

DDM предоставляет следующие возможности:

1. **Просмотр информации мониторинга на трансивере.**

Администратор может наблюдать за текущим состоянием линии и находить потенциальные проблемы с помощью проверки параметров трансивера и получать информацию мониторинга. Это позволит быстро обнаружить неисправную линию и сократить время восстановления.

2. **Определение значения порога пользователем.**

Для параметров реального времени (Tx мощности, Rx мощности, температуры, напряжения и тока) существуют заданные производителем значения порогов. В зависимости от среды, пользователь самостоятельно может определить значение порогов разного приоритета, гибко контролировать рабочее состояние трансивера и быстро обнаружить неисправность. Приоритет оповещений распределяется следующим образом (от низкого к высокому): high alarm - high warn - low warn - low alarm.

3. **Контроль трансивера.**

Пользователь может отслеживать информацию об истории состояния трансивера, такой как последнее время неисправности и ее тип. Контроль трансивера помогает найти последнее состояние неисправности через проверку логов и запросить последнее состояние неполадки через выполнение команд.

15.2 Конфигурация DDM

1. Отобразить текущую информацию о трансивере;
2. Настроить пороги alarm или warning для каждого параметра трансивера;
3. Настроить функцию transceiver monitoring:
    a. Включить функцию transceiver monitoring и настроить интервал;
    b. Вывести и очистить информацию transceiver monitoring;

1. Отобразить текущую информацию мониторинге состояния трансивера:

Команда	Описание
`show transceiver [interface ethernet interface-list>][detail]` В Admin режиме	Просмотр текущей информацию мониторинге состояния трансивера. При указании параметра `interface ethernet <interface-list>` информация будет отображена только для указанного интерфейса. `[detail]` - отобразить детальную информаци.

2. Настроить пороги alarm или warning для каждого параметра трансивера:

Команда	Описание
`transceiver threshold {default | {temperature | voltage | bias | rx-power | tx-power} {high-alarm | low-alarm | high-warn | low-warn} {<value> | default}}` В режиме конфигурации порта	Настроить пороги для каждого параметра трансивера. `default` - устанавливает порог, заданный производителем трансивера (по-умолчанию).

3. Настроить функцию transceiver monitoring:
   a. Включить функцию transceiver monitoring и настроить интервал:

Команда	Описание

`transceiver-monitoring interval <minutes>`
`no transceiver-monitoring interval`
 	
В режиме глобальной конфигурации
	Задать интервал мониторинга трансивера в минутах. Команда `no` восстанавливает значение по-умолчанию - 15 минут.

`transceiver-monitoring {enable | disable}` В режиме конфигурации порта	Включить\выключить функцию transceiver monitoring на порту.

   b. Вывести и очистить информацию transceiver monitoring:

Команда	Описание
`show transceiver threshold-violation [interface ethernet <interface-list>]`	Отобразить информацию о превышении порогов transceiver monitoring. При

В Admin режиме	указании параметра `interface ethernet <interface-list>` информация будет отображена только для указанного интерфейса.
`clear transceiver threshold-violation [interface ethernet <interface-list>]` В Admin режиме	Очистить информацию о превышении порогов transceiver monitoring. При указании параметра `interface ethernet <interface-list>` информация будет удалена только для указанного интерфейса.

15.3 Пример конфигурации DDM

Пример 1: В порты Ethernet 1/0/21 и Ethernet 1/0/23 подключен оптический трансивер с поддержкой функции DDM, в порт Ethernet 1/0/24 трансивер без DDM, а в порт Ethernet 1/0/22 трансивер не подключен.

1. Отобразить информацию о всех интерфейсах, с который возможно прочитать параметры DDM (порты 1/0/22 и 1/0/24 не отобразятся):

```
Switch#show transceiver
Interface Temp (℃)  Voltage (V)  Bias (mA)  RX Power (dBM)  TX
Power (dBM)
1/0/21 33 3.31 6.11 -30.54(A-) -6.01
1/0/23 33 5.00 (W+)  6.11 -20.54(W-) -6.02
```

2. Отобразить информацию об определенном интерфейсе (N/A означает отсутствие информации):

```
Switch#show transceiver interface ethernet 1/0/21-22;23
Interface Temp (℃)  Voltage (V)  Bias (mA)  RX Power (dBM)  TX
Power (dBM)
1/0/21 33 3.31 6.11 -30.54(A-) -6.01
1/0/22 N/A N/A N/A N/A N/A
1/0/23 33 5.00 (W+)  6.11 -20.54(W-) -6.02
```

3. Отобразить детальную информацию:

```
Switch#show transceiver interface ethernet 1/0/21-22;24 detail
Ethernet 1/0/21 transceiver detail information:
Base information:
SFP found in this port, manufactured by company, on Sep 29 2010.
Type is 1000BASE-SX. Serial Number is 1108000001.
Link length is 550 m for 50um Multi-Mode Fiber.
```

```
Link length is 270 m for 62.5um Multi-Mode Fiber.
Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.
Brief alarm information:
RX loss of signal
Voltage high
RX power low
Detail diagnostic and threshold information:
Diagnostic Threshold
Realtime Value High Alarm Low Alarm High Warn Low Warn
-------------- ----------- ----------- ------------ ---------
Temperature (℃)  33 70 0 70 0
Voltage (V)  7.31(A+) 5.00 0.00 5.00 0.00
Bias current (mA)  6.11(W+) 10.30 0.00 5.00 0.00
RX Power (dBM)  -30.54(A-) 9.00 -25.00 9.00 -25.00
TX Power (dBM)  -6.01 9.00 -25.00 9.00 -25.00

Ethernet 1/0/22 transceiver detail information: N/A

Ethernet 1/0/24 transceiver detail information:
Base information:
SFP found in this port, manufactured by company, on Sep 29 2010.
Type is 1000BASE-SX. Serial Number is 1108000001.
Link length is 550 m for 50um Multi-Mode Fiber.
Link length is 270 m for 62.5um Multi-Mode Fiber.
Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.
Brief alarm information: N/A
Detail diagnostic and threshold information: N/A

Explanation: If the serial number is 0, it means that it is not
specified as bellow:
SFP found in this port, manufactured by company, on Sep 29 2010.
Type is 1000BASE-SX. Serial Number is not specified.
Link length is 550 m for 50um Multi-Mode Fiber.
Link length is 270 m for 62.5um Multi-Mode Fiber.
Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.
```

Пример 2: В порт Ethernet 1/0/21 подключен оптический модуль с поддержкой DDM. Необходимо настроить пороговое значение после просмотра информации о DDM.

1. Отобразить информацию о DDM:

```
Switch#show transceiver interface ethernet 1/0/21 detail
Ethernet 1/0/21 transceiver detail information:
Base information:
……
Brief alarm information:
```

```
RX loss of signal
Voltage high
RX power low
Detail diagnostic and threshold information:
Diagnostic Threshold
Realtime Value High Alarm Low Alarm High Warn Low Warn
------------- ----------- ----------- ------------ ---------
Temperature (℃)  33 70 0 70 0
Voltage (V)  7.31(A+) 5.00 0.00 5.00 0.00
Bias current (mA)  6.11(W+) 10.30 0.00 5.00 0.00
RX Power (dBM)  -30.54(A-) 9.00 -25.00 9.00 -25.00
TX Power (dBM)  -13.01 9.00 -25.00 9.00 -25.00
```

2. Сконфигурировать порог tx-power для оптического модуля: low-warning - минус 12, low-alarm - минус 10.00

```
Switch#config
Switch(config)#interface ethernet 1/0/21
Switch(config-if-ethernet1/0/21)#transceiver threshold tx-power low-
warning -12
Switch(config-if-ethernet1/0/21)#transceiver threshold tx-power low-
alarm -10.00
```

3. Отобразить детальную информацию о DDM оптического модуля:

```
Switch#show transceiver interface ethernet 1/0/21 detail
Ethernet 1/0/21 transceiver detail information:
Base information:
……
Brief alarm information:
RX loss of signal
Voltage high
RX power low
TX power low
Detail diagnostic and threshold information:
Diagnostic Threshold
Realtime Value High Alarm Low Alarm High Warn Low Warn
------------- ----------- ----------- ---------- ---------
Temperature (℃)  33 70 0 70 0
Voltage (V)  7.31(A+) 5.00 0.00 5.00 0.00
Bias current (mA)  6.11(W+) 10.30 0.00 5.00 0.00
RX Power (dBM)  -30.54(A-) 9.00 -25.00 9.00 -25.00
TX Power (dBM)  -13.01(A-) 9.00 -12.00(-25.00) 9.00 -10.00(-25.00)
```

Пример 3: В порт Ethernet 1/0/21 подключен оптический модуль с поддержкой DDM. Необходимо включить функцию transceiver monitoring.

1. Включить функцию transceiver monitoring для порта:

```
Switch(config)#interface ethernet 1/0/21
Switch(config-if-ethernet1/0/21)#transceiver-monitoring enable
```

2. Отобразить информацию о мониторинге оптического модуля:

```
Switch#show transceiver threshold-violation interface ethernet 1/0/21-
22
Ethernet 1/0/21 transceiver threshold-violation information:
Transceiver monitor is enabled. Monitor interval is set to 30 minutes.
The current time is Jan 15 12:30:50 2018.
The last threshold-violation time is Jan 15 11:00:50 2018.
Brief alarm information:
RX loss of signal
RX power low
Detail diagnostic and threshold information:
Diagnostic Threshold
Realtime Value High Alarm Low Alarm High Warn Low Warn
------------ ----------- ----------- ------------ ---------
Temperature (℃)  33 70 0 70 0
Voltage (V)  7.31 10.00 0.00 5.00 0.00
Bias current (mA)  3.11 10.30 0.00 5.00 0.00
RX Power (dBM)  -30.54(A-) 9.00 -25.00(-34) 9.00 -25.00
TX Power (dBM)  -1.01 9.00 -12.05 9.00 -10.00

Ethernet 1/0/22 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30
minutes.
The last threshold-violation doesn’t exist.
```

15.4 Решение проблем при использовании DDM

При возникновении проблем с использованием DDM, пожалуйста, проверьте следующие причины:

- Убедитесь, что трансивер включен в порт, и поддерживает DDM;
- Убедитесь, что оптическая линия включена в трансивер;
- При отсутствии оповещения по SNMP, убедитесь, что SNMP корректно сконфигурирован на коммутаторе;
- Использование команд **show transceiver** или **show transceiver detail** в некоторых случаях может занять длительное время, поэтому рекомендуется использовать данные команды только для определенных портов в отдельности;

16. BPDU-Tunnel

16.1 Общие сведения о BPDU-Tunnel

BPDU-Tunnel - это функционал, позволяющий передавать служебный трафик протоколов канального уровня без изменений.

Функционал может быть полезен, например, при подключении географически распределенной корпоративной сети через L2-каналы оператора. В этом случае трафик служебных протоколов, таких как STP, может помешать нормальной работе коммутаторов оператора и наоборот. BPDU-Tunnel позволяет передавать такие кадры прозрачно для коммутатора оператора.

16.2 Конфигурация BPDU-Tunnel

1. Настроить MAC-адреса кадров для BPDU-tunnel;
2. Настроить порты для BPDU-tunnel.

1. Настроить MAC-адреса кадров для BPDU-tunnel:

Команда	Описание

`bpdu-tunnel-protocol {stp| gvrp| dot1x} {group-mac <mac> | default-group-mac}`
`no bpdu-tunnel-protocol {stp| gvrp| dot1x}`
 	
В режиме глобальной конфигурации
	Включить BPDU-Tunnel на коммутаторе для протоколов STP, GVRP, Dot1x. Команда позволяет выбрать MAC-адрес группы, на который будет заменен оригинальный адрес, по-умолчанию `default-group-mac` (01-00-0c-cd-00-02), либо назначить MAC-адрес группы вручную `group-mac <mac>` (в диапазоне от 01-80-c2-00-00-00 до 01-80-c2-00-00-30). Команда `no` выключает эту функцию.

`bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> {group-mac <mac> | default-group-mac}`
`no bpdu-tunnel-protocol user-defined-protocol <name>`
 	
В режиме глобальной конфигурации
	Включить BPDU-Tunnel на коммутаторе для протокола, задаваемого пользователем. `protocol-mac <mac>` - оригинальный MAC-адрес протокола. Команда позволяет выбрать MAC-адрес группы, на который будет заменен оригинальный адрес, по-умолчанию `default-group-mac` (01-00-0c-cd-00-02), либо назначить MAC-адрес группы вручную `group-mac <mac>` (в диапазоне от 01-80-c2-00-00-00 до 01-80-c2-00-00-30). Команда `no` выключает эту функцию.

`bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> encape-type ethernetii protocol-type <type> {group-mac <mac> | default-group-mac}`
`no bpdu-tunnel-protocol user-defined-protocol <name>`
 	
В режиме глобальной конфигурации
	Включить BPDU-Tunnel на коммутаторе для протокола, задаваемого пользователем, имеющего инкапсуляцию Ethernet II. `protocol-mac <mac>` - оригинальный MAC-адрес протокола. Команда позволяет выбрать MAC-адрес группы, на который будет заменен оригинальный адрес, по-умолчанию `default-group-mac` (01-00-0c-cd-00-02), либо назначить MAC-адрес группы вручную `group-mac <mac>` (в диапазоне от 01-80-c2-00-00-00 до 01-80-c2-00-00-30). Команда `no` выключает эту функцию.

`bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> encape-type snap {oui <oui>| }protocol-type <type> {group-mac <mac> | default-group-mac}`
`no bpdu-tunnel-protocol user-defined-protocol <name>`
 	
В режиме глобальной конфигурации
	Включить BPDU-Tunnel на коммутаторе для протокола, задаваемого пользователем, имеющего инкапсуляцию SNAP. `protocol-mac <mac>` - оригинальный MAC-адрес протокола. Команда позволяет выбрать MAC-адрес группы, на который будет заменен оригинальный адрес, по-умолчанию `default-group-mac` (01-00-0c-cd-00-02), либо назначить MAC-адрес группы вручную `group-mac <mac>` (в диапазоне от 01-80-c2-00-00-00 до 01-80-c2-00-00-30). Команда `no` выключает эту функцию.

`bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> encape-type llc dsap <dsap> ssap <ssap> {group-mac <mac> | default-group-mac}` **`no bpdu-tunnel-protocol user-defined-protocol <name>`** В режиме глобальной конфигурации	Включить BPDU-Tunnel на коммутаторе для протокола, задаваемого пользователем, имеющего инкапсуляцию LLC. `protocol-mac <mac>` - оригинальный MAC-адрес протокола. Команда позволяет выбрать MAC-адрес группы, на который будет заменен оригинальный адрес, по-умолчанию `default-group-mac` (01-00-0c-cd-00-02), либо назначить MAC-адрес группы вручную `group-mac <mac>` (в диапазоне от 01-80-c2-00-00-00 до 01-80-c2-00-00-30). Команда `no` выключает эту функцию.

2. Настроить порты для BPDU-tunnel.

Команда	Описание

`bpdu-tunnel-protocol {stp| gvrp| dot1x| user-defined-protocol <name>}`
`no bpdu-tunnel-protocol {stp| gvrp| dot1x| user-defined-protocol <name>}`
 	
В режиме конфигурации порта
	Включить на порту заранее сконфигурированный BPDU-tunnel. Команда `no` выключает эту функцию на порту.

16.3 Пример конфигурации BPDU-Tunnel

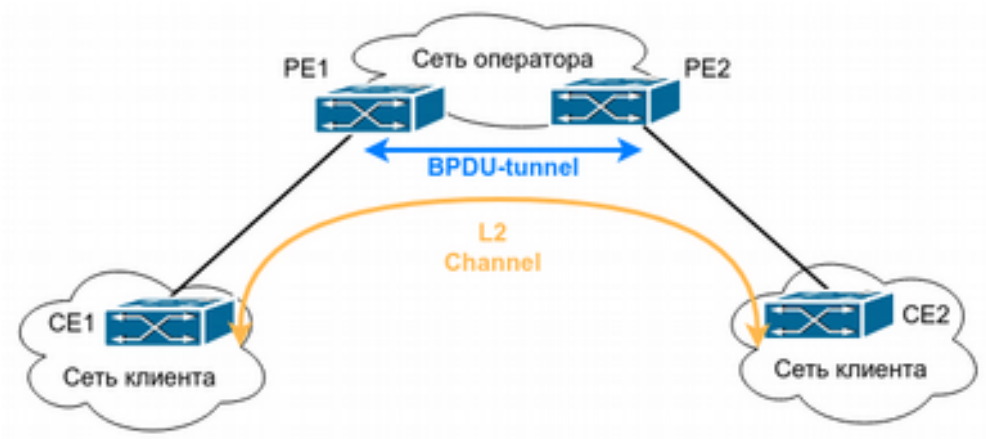


Рисунок 16.1 BPDU-Tunnel

Как показано на рисунке 16.1, оператор предоставляет клиенту L2 VLAN для соединения географически удаленных филиалов через коммутаторы PE1 и PE2. В свою очередь, клиент использует коммутаторы CE1 и CE2 для подключения к сети оператора. В своей сети клиент использует для резервирования протокол STP. Необходимо настроить BPDU-tunnel для корректной передачи BPDU STP из сети клиента по сети оператора.

Конфигурация коммутатора PE1:

```
PE1(config)# bpdu-tunnel-protocol stp default-group-mac
PE1(config-if-ethernet1/0/1)# bpdu-tunnel-protocol stp
```

Конфигурация коммутатора PE2:

```
PE2(config)# bpdu-tunnel-protocol stp default-group-mac
PE2(config-if-ethernet1/0/1)# bpdu-tunnel-protocol stp
```

После проведения этой конфигурации будет происходит следующее:

1. При получении кадра протокола канального уровня коммутатор инкапсулирует пакет, а именно заменяет MAC-адрес назначения на конкретный multicast MAC-адрес (по умолчанию 01-00-0c-cd-00-02) и посылает по сети;
2. На другом конце сети кадр деинкапсулируется: MAC-адрес назначения 01-00-0c-cd-00-02 меняется на оригинальный.

16.4 Решение проблем при конфигурации BPDU-Tunnel

- BPDU-tunnel может работать только на портах, протоколы stp, gvrp и dot1x на которых не задействованы.

17. EEE Energy saving

17.1 Общие сведения о функции EEE

EEE (Energy Efficient Ethernet) - функция, позволяющая экономить энергию при использовании медных портов коммутатора. После активации функции на порту, коммутатор автоматически определяет статус порта: если данные на порту не передаются и порт простаивает, коммутатор отключает питание порта для экономии энергии.

17.2 Конфигурация функции EEE

Команда	Описание

`eee enable`
`no eee enable`
 	
В режиме конфигурации порта
	Включить на порту функцию EEE на порту. Команда `no` отключает эту функцию.

18. Отключение LED портов

18.1 Общие сведения о функции отключения LED портов

Функция отключения светодиода (LED) порта может выключить все светодиоды в соответствии с заданным временем независимо от наличия соединения на физическом уровне. По истечении заданного времени LED портов могут быть включены и работать в зависимости от наличия линка как обычно. Функция может быть полезна при установке коммутатора в жилых или общественных помещениях, а также для экономии энергии.

18.2 Конфигурация функции отключения LED портов

Команда	Описание

`port-led shutoff time-range <time-range-name>`
`no port-led shutoff`
 	
В режиме глобальной конфигурации
	Настроить время отключения LED портов. Команда `no` отменяет выключение LED портов.

18.3 Пример конфигурации функции отключения LED портов

Настроить отключение светодиодов с 14:30 понедельника по 18:30 пятницы.
Конфигурация коммутатора будет выглядеть следующим образом:

```
switch(config)#time-range t1
switch(config-time-t1)#periodic Monday Friday 14:30:00 to 18:30:00
switch(config)#port-led shutoff time-range t1
```

19. VLAN

19.1 Общие сведения о технологии VLAN

VLAN (Virtual Local Area Network) - это технология, позволяющая объединять устройства в сети в сегменты на основе функций, приложений или требований управления. Виртуальные сегменты могут формироваться в независимости от физического расположения устройств. VLAN имеют те же свойства, что и физические LAN, за исключением того, что VLAN представляет собой логическое объединение, а не физическое. Поэтому во VLAN можно объединять устройства, независимо от того, где они находятся физически, а широковещательный, многоадресный и одноадресный трафик в одном VLAN отделен от других VLAN.
Стандарт IEEE 802.1Q определяет процедуру передачи трафика VLAN.
Основная идея технологии VLAN заключается в том, что большая локальная сеть может быть динамически разделена на отдельные широковещательные области, удовлетворяющие различным требованиям, каждый VLAN представляет собой отдельный широковещательный домен.

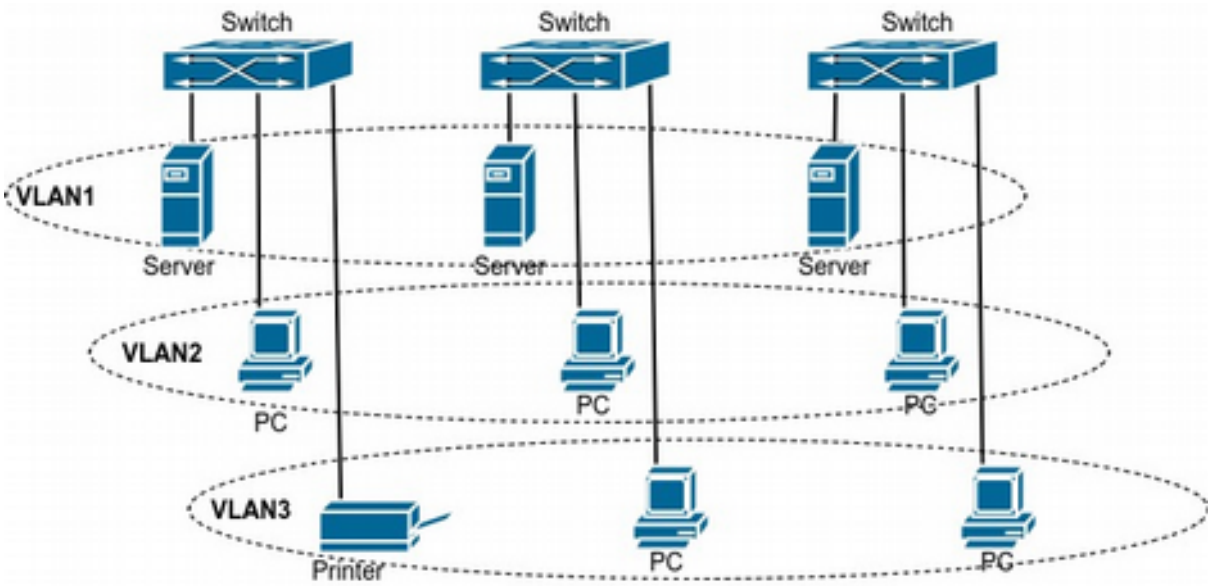


Рисунок 19.1 логическое разделение сети на VLAN

Благодаря этим функциям технология VLAN предоставляет следующие возможности:
- Повышение производительности сети;
- Сохранение сетевых ресурсов;
- Оптимизация сетевого управления;
- Снижение стоимости сети;
- Повышение безопасности сети;

Ethernet-порт коммутатора может работать в трех режимах: Access, Trunk и Hybrid, каждый режим имеет различный метод обработки при передаче кадров с тэгом или без.

Порт в режиме Access относится только к одному VLAN, обычно используется для подключения конечных устройств, таких как персональный компьютер или wi-fi маршрутизатор в квартире или офисе.
Порт в режиме Trunk относится к нескольким VLAN и может принимать и отправлять кадры одновременно в нескольких VLAN. Обычно используется для соединения коммутаторов.
Порт в режиме Hybrid, также как и Trunk, относится к нескольким VLAN и может принимать и отправлять кадры одновременно в нескольких VLAN. Может использоваться как для подключения персональных компьютеров, так и для соединения коммутаторов.
Ethernet-порты в режимах Hybrid и Trunk могут принимать данные одним, но отправляют разными способами: Hybrid порт может отправлять пакеты в нескольких VLAN в нетэгированном виде, в то время как Trunk может отправлять трафик в нескольких VLAN только с тэгом, за исключением native VLAN.
Коммутатор Поддерживает VLAN и GVRP (протокол регистрации VLAN GARP), которые определены 802.1Q. В главе подробно рассказывается об использовании и конфигурации VLAN и GVRP.

19.2 Конфигурация VLAN

1. Создание и удаление VLAN
2. Назначение и удаление имени VLAN
3. Назначение портов коммутатора для VLAN
4. Выбор типа порта коммутатора
5. Настройка порта в режиме Trunk
6. Настройка порта в режиме Access
7. Настройка порта в режиме Hybrid
8. Включение/выключение vlan ingress rules глобально
9. Настройка private vlan
10. Настройка ассоциаций private vlan

1. Создание и удаление VLAN

Команда	Описание

`vlan <Vlan-id>`
`no vlan <Vlan-id>`
В режиме глобальной конфигурации
	Создание VLAN, вход в режим конфигурирования VLAN
	Удаление VLAN

2. Назначение и удаление имени VLAN

Команда	Описание
`name <Vlan-name>` `no name <Vlan-name>`	Назначение имени VLAN Удаление имени VLAN

в режиме конфигурации VLAN	

3. Назначение портов коммутатора для VLAN

Команда	Описание

`switchport interface <interface-list>`
`no switchport interface <interface-list>`
в режиме конфигурации VLAN
	Добавление портов коммутатора во VLAN
	
	Удаление портов коммутатора из VLAN

4. Выбор типа порта коммутатора

Команда	Описание
`switchport mode <trunk|access|hybrid>` в режиме конфигурации порта	Установка текущего порта в режим Trunk, Access или Hybrid

5. Настройка порта в режиме Trunk

Команда	Описание

`switchport trunk allowed vlan {WORD|all|add WORD|except WORD|remove WORD}`
 	
`no switchport trunk allowed vlan`
 	
в режиме конфигурации порта
	Добавление VLAN в Trunk
	
	Вернуть значение по-умолчанию

`switchport trunk native vlan <vlan-id>`
`no switchport trunk native vlan`
 	
в режиме конфигурации порта
	установка PVID для интерфейса
	
	возвращение значений по-умолчанию

6. Настройка порта в режиме Access

Команда	Описание
`switchport access vlan <Vlan-id>` `no switchport access vlan <Vlan-`	Добавление текущего порта в определенный VLAN.

id> в режиме конфигурации порта	Вернуть значение по-умолчанию

7. Настройка порта в режиме Hybrid

Команда	Описание
switchport hybrid allowed vlan <WORD| all| add WORD><tag|untag> no switchport hybrid allowed vlan в режиме конфигурации порта	Создание/удаление VLAN, вход в режим конфигурирования VLAN
switchport hybrid native vlan <vlan-id> в режиме конфигурации порта	установка PVID для интерфейса возвращение значений по-умолчанию

8. Включение/выключение vlan ingress rules глобально

Команда	Описание
vlan ingress enable <Vlan-id> no ingress disable <Vlan-id> в режиме конфигурации порта	Включение VLAN ingress rules выключение VLAN ingress rules

9. Настройка private vlan

Команда	Описание
private-vlan {primary| isolated| community} no private vlan В режиме конфигурации VLAN	Настройка текущего vlan в качестве Private VLAN. Возвращение настроек по-умолчанию

10. Настройка ассоциаций private vlan

Команда	Описание
private vlan association <secondary-vlan-list> no private vlan association	Выбрать vlan для ассоциации с private vlan Удалить ассоциацию

<Vlan-id> В режиме конфигурации VLAN	

19.3 Пример конфигурации VLAN

Сценарий:

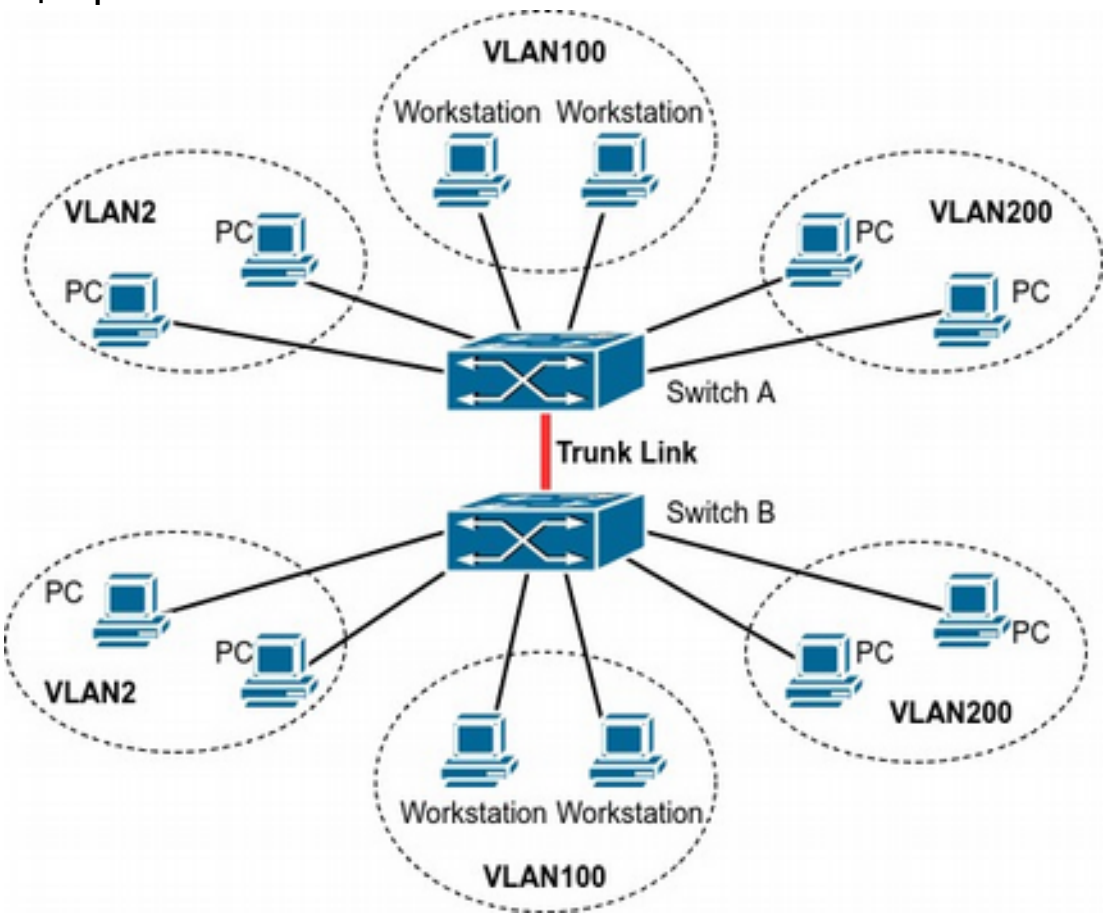


Рисунок 19.2 Топология для примера настройки VLAN

Представленная на рисунке 19.2, сеть разделена на 3 VLAN: VLAN2, VLAN100, VLAN100, VLAN200 по используемым приложениям, а также по соображениям безопасности. Эти VLAN расположены в разных локациях: A и B. Каждый из двух коммутаторов размещен в своей локации. Устройства в разных локациях могут быть объединены виртуальную локальную сеть, если трафик будет передаваться между коммутаторами A и B.

пункт конфигурации	описание
VLAN2	Коммутатор A и B: порт 2-4
VLAN100	Коммутатор A и B: порт 5-7

VLAN200	Коммутатор A и B: порт 8-10
Trunk port	Коммутатор A и B: порт 11

Соедините порты в режиме trunk на коммутаторах A и B друг с другом, подключите остальные сетевые устройства к соответствующим портам.

Коммутатор A:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/0/2-4
Switch (Config-Vlan2)#exit
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/0/5-7
Switch (Config-Vlan100)#exit
Switch (config)#vlan 200
Switch (Config-Vlan200)#switchport interface ethernet 1/0/8-10
Switch (Config-Vlan200)#exit
Switch (config)#interface ethernet 1/0/11
Switch (Config-If-Ethernet1/0/11)#switchport mode trunk
Switch (Config-If-Ethernet1/0/11)#exit
```

Коммутатор B:

```
Switch (config)#vlan 2
Switch (Config-Vlan2)#switchport interface ethernet 1/0/2-4
Switch (Config-Vlan2)#exit
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/0/5-7
Switch (Config-Vlan100)#exit
Switch (config)#vlan 200
Switch (Config-Vlan200)#switchport interface ethernet 1/0/8-10
Switch (Config-Vlan200)#exit
Switch (config)#interface ethernet 1/0/11
Switch (Config-If-Ethernet1/0/11)#switchport mode trunk
Switch (Config-If-Ethernet1/0/11)#exit
```

19.3.1 Пример конфигурации Hybrid порта

Сценарий:

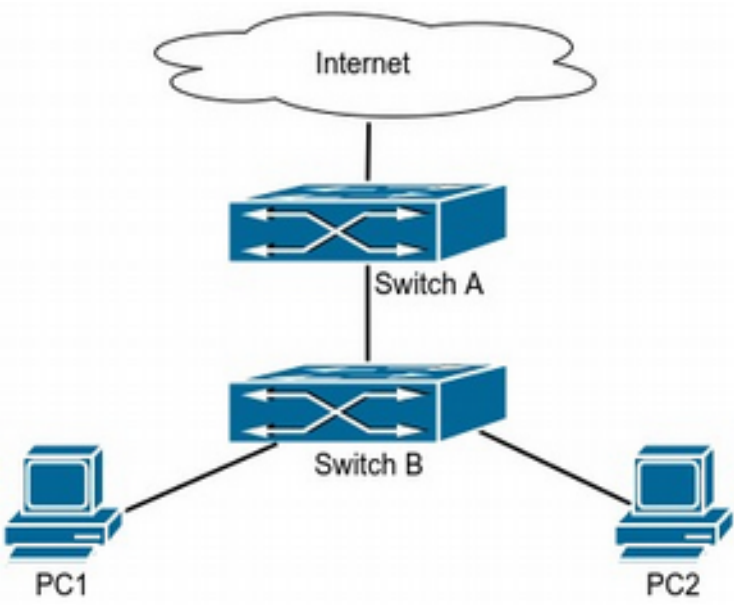


Рисунок 19.3 Пример применения Hybrid Port

ПК 1 подключен к интерфейсу Ethernet 1/0/7 Коммутатора “Switch B”, ПК2 подключен к интерфейсу Ethernet 1/0/9 коммутатора “Switch B”, интерфейс Ethernet 1/0/10 “Switch A” подключен к порту Ethernet 1/0/10 коммутатора “Switch B”
Для безопасности ПК1 и ПК2 не должны иметь возможность взаимодействовать друг с другом, но должны иметь доступ к сетевым ресурсам, находящимся за “Switch A”.

Необходимо настроить коммутаторы следующим образом:

Порт	Тип	PVID	VLAN, которые может пропускать
1/0/10 на “Switch A”	Access	10	пакеты VLAN 10 без тэга
1/0/10 на “Switch B”	Hybrid	10	пакеты VLAN 7,9,10 без тэга
1/0/7 на “Switch B”	Hybrid	7	пакеты VLAN 7,10 без тэга
1/0/9 на “Switch B”	Hybrid	9	пакеты VLAN 9,10 без тэга

Switch A:

```
Switch(config)#vlan 10
Switch(Config-Vlan10)#switchport interface ethernet 1/0/10
```

Switch B:

```
Switch(config)#vlan 7;9;10
Switch(config)#interface ethernet 1/0/7
Switch(Config-If-Ethernet1/0/7)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/7)#switchport hybrid native vlan 7
Switch(Config-If-Ethernet1/0/7)#switchport hybrid allowed vlan 7;10
untag
```

```
Switch(Config-If-Ethernet1/0/7)#exit
Switch(Config)#interface Ethernet 1/0/9
Switch(Config-If-Ethernet1/0/9)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/9)#switchport hybrid native vlan 9
Switch(Config-If-Ethernet1/0/9)#switchport hybrid allowed vlan 9;10
untag
Switch(Config-If-Ethernet1/0/9)#exit
Switch(Config)#interface Ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/10)#switchport hybrid native vlan 10
Switch(Config-If-Ethernet1/0/10)#switchport hybrid allowed vlan 7;9;10
untag
Switch(Config-If-Ethernet1/0/10)#exit
```

20. Dot1q-tunnel

20.1 Общие сведения о Dot1q-tunnel

Dot1q-tunnel, также известный как QinQ (802.1Q-in-802.1Q), является расширением стандарта 802.1Q. Его идея заключается в инкапсуляции тега VLAN клиента (тег CVLAN) в тег VLAN поставщика услуг (тег SPVLAN). Имея 2 тэга, трафик передается в сети поставщика услуг, чем обеспечивает l2-канал для пользователя.

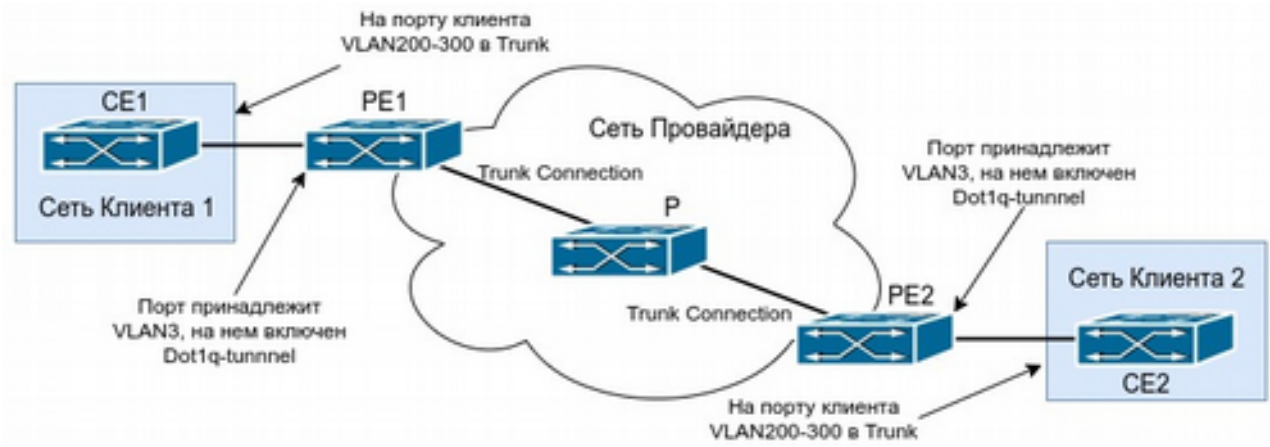


Рисунок 20.1 Режим обмена трафиком dot1q-tunnel

Как показано выше, после включения на порту подключения пользователя dot1q-tunnel, коммутатор назначает идентификатор SPVLAN (SPVID) VLAN 3. Для одного и того же пользователя сети на разных PE должны быть назначены одинаковые SPVID. Когда пакет из CE достигает PE, он несет тег VLAN 200-300 внутренней сети пользователя. Поскольку функция dot1q-tunnel включена, порт на PE1 добавит в пакет другой тег VLAN, идентификатором которого является SPVID, назначенный пользователю. После этого пакет будет передаваться только во VLAN 3 по сети Интернет-провайдера с двумя тегами VLAN одновременно (внутренний тег добавляется при входе на PE1, а внешний - SPVID). На порту подключения пользователя коммутатора PE2 перед отправкой кадров в CE2, внешний тег VLAN удаляется, - CE2 принимает пакет абсолютно идентичный тому, который был отправлен CE1.

Технология Dot1q-tunnel предоставляет операторам возможность передачи трафика разных клиентов в только одном собственном VLAN. При этом и Интернет-оператор и его клиент могут настроить свои собственные VLAN.

Dot1q-tunnel имеет следующие преимущества:

- Обеспечивает простой L2-канал для пользователя, требующий небольших ресурсов как со стороны настройки\обслуживания, так и со стороны аппаратных возможностей оборудования
- Расширяет количество доступных к использованию VLAN
- Позволяет пользователям самостоятельно выбирать номер тэга VLAN в не зависимости от тега VLAN в сети Интернет-провайдера

В данном разделе представлено детальное описание настройки технологии Dot1q-tunnel.

20.2 Конфигурация Dot1q-tunnel

1. Настройка dot1q-tunnel на ethernet-интерфейсе
2. Настройка в TPID (Tag Protocol Identifier)

1. Настройка dot1q-tunnel на ethernet-интерфейсе

Команда	Описание

`dot1q-tunnel enable`
 	
`no dot1q-tunnel enable`
В режиме конфигурации интерфейса
	Включить на интерфейсе функцию dot1q-tunnel
	
	Выключить на интерфейсе функцию dot1q-tunnel

2. Настройка TPID (Tag Protocol Identifier)

Команда	Описание
`dot1q-tunnel tpid {0x8100|0x9100|0x9200|<1-65535>}` в режиме глобальной конфигурации	Настроить TPID глобально

20.3 Пример конфигурации dot1q-tunnel

Сценарий:

Пограничные коммутаторы PE1 и PE2 сети Интернет провайдера передают во VLAN 3 трафик VLAN 200~300 между коммутаторами сети клиента CE1 и CE2. Порт 1/0/1 коммутатора PE1 подключен к CE1, порт 1/0/10 подключен к публичной сети. TPID подключенного оборудования - 9100. Порт 1/0/1 коммутатора PE2 подключен к CE2, порт 1/0/10 подключен к публичной сети

Необходимо настроить коммутаторы следующим образом:

Объект	Описание конфигурации
VLAN3	Port 1/0/1 на PE1 и PE2
dot1q-tunnel	Port 1/0/1 на PE1 и PE2
tpid	9100

Конфигурация будет выглядеть следующим образом:

PE1:

```
Switch(Config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/0/1
Switch(Config-Vlan3)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(Config-Ethernet1/0/1)# dot1q-tunnel enable
Switch(Config-Ethernet1/0/1)# exit
Switch(Config)#interface ethernet 1/0/10
Switch(Config-Ethernet1/0/10)#switchport mode trunk
Switch(Config-Ethernet1/0/10)#exit
Switch(config)#dot1q-tunnel tpid 0x9100
Switch(Config)#
```

PE2:

```
Switch(Config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/0/1
Switch(Config-Vlan3)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(Config-Ethernet1/0/1)# dot1q-tunnel enable
Switch(Config-Ethernet1/0/1)# exit
Switch(Config)#interface ethernet 1/0/10
Switch(Config-Ethernet1/0/10)#switchport mode trunk
Switch(Config-Ethernet1/0/10)#exit
Switch(config)#dot1q-tunnel tpid 0x9100
Switch(Config)#
```

20.4 Решение проблем при конфигурации Dot1q-tunnel

- Включение dot1q-tunnel на интерфейсе в режиме Trunk сделает тэг кадра данных непредсказуемым, поэтому включать dot1q-tunnel на интерфейсе в режиме trunk не рекомендуется;
- Не поддерживается настройка dot1q-tunnel на Port-channel;
- Не поддерживается включение dot1q-tunnel на интерфейсе вместе с STP/MSTP;
- Не поддерживается использование в Private VLAN.

21. Selective QinQ

21.1 Общие сведения о Selective QinQ

Selective QinQ - это расширение функции dot1q-tunnel, позволяющая тегировать пакеты разным внешним тэгом VLAN в зависимости от разного внутреннего тэга VLAN в соответствии с требованиями пользователя. Это позволяет выбирать каналы передачи для разных типов трафика с разным тэгом VLAN.

21.2 Конфигурация Selective QinQ

1. Настройка соответствия между внутренним и внешним тэгом на порту коммутатора;
2. Включение Selective QinQ на порту коммутатора.

1. Настройка правил сопоставления внешнего тэга внутреннему;

Команда	Описание
`dot1q-tunnel selective s-vlan <s-vid> c-vlan <c-vid-list>`	Применение правила сопоставления внешнего тега внутреннему(внутренним) `s-vlan` - внешний тэг `c-vlan` - внутренний тэг
`no dot1q-tunnel selective s-vlan <s-vid> c-vlan <c-vid-list>` В режиме конфигурации интерфейса	Удаление правила сопоставления внешнего тега внутреннему(внутренним)

2. Включение функции Selective QinQ.

Команда	Описание
`dot1q-tunnel selective enable`	Включить на интерфейсе функцию dot1q-tunnel selective
`no dot1q-tunnel selective enable` В режиме конфигурации порта	Выключить на интерфейсе функцию dot1q-tunnel selective

21.3 Пример применения Selective QinQ

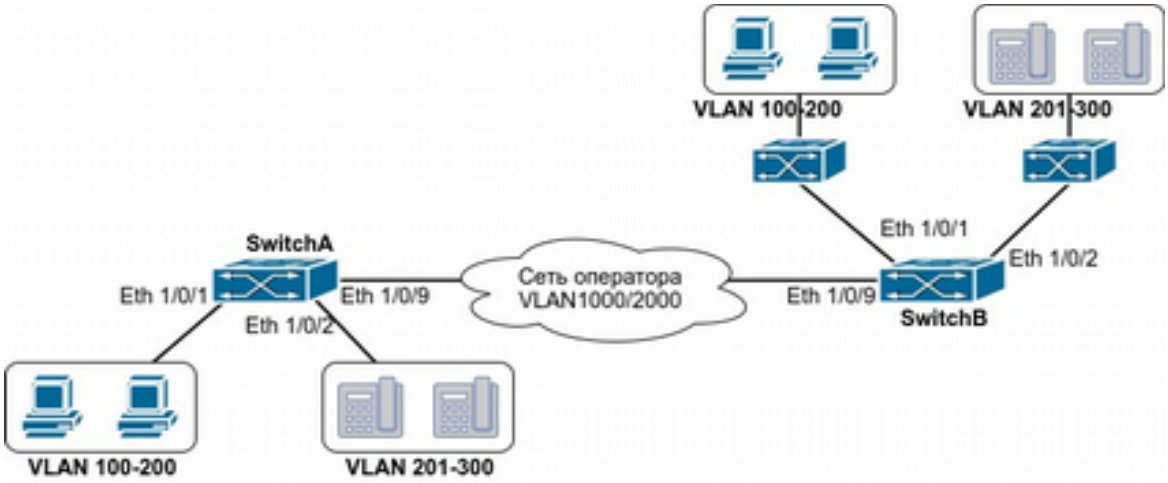


Рисунок 21.1 применение Selective QinQ

1. Порт Ethernet 1/0/1 коммутатора “SwitchA” предоставляет доступ в публичную сеть пользователям PC, а Ethernet 1/0/2 коммутатора “SwitchA” предоставляет доступ в публичную сеть пользователям IP-телефонии. Пользователи PC используют VLAN из диапазона от 100 до 200, а пользователи IP-телефонии используют VLAN из диапазона от 201 до 300. Ethernet 1/0/9 подключен к публичной сети.
2. Ethernet 1/0/1 и Ethernet 1/0/2 коммутатора “SwitchB” предоставляют доступ в публичную сеть для пользователей PC в диапазоне VLAN от 100 до 200, и пользователям IP-телефонии в диапазоне VLAN от 201 до 300 соответственно. Ethernet 1/0/9 подключен к публичной сети.
3. Публичная сеть пропускает пакеты VLAN 1000 и VLAN 2000.
4. Selective QinQ включен на портах Ethernet 1/0/1 и Ethernet 1/0/2 коммутатора “SwitchA” и коммутатора “SwitchB” соответственно. К пакетам во VLAN из диапазона от 100 до 200 добавляется внешний тэг 1000, а к пакетам во VLAN из диапазона от 201 до 300 добавляется внешний тэг 2000.

Настройка может быть разбита на следующие шаги:

Создать VLAN 1000 и VLAN 2000 на коммутаторе “SwitchA”.

```
switch(config)#vlan 1000;2000
```

Настроить Ethernet1/0/1 в режим Hybrid и настроить его для снятия тэга при передаче пакета vlan 1000.

```
switch(config-if-ethernet1/0/1)#switchport hybrid allowed vlan 1000
untag
```

Настроить правило сопоставления selective QinQ на Ehernet1/0/1 для добавления тэга VLAN 1000 как внешней метки в пакетах с тэгами из диапазона VLAN от 100 до 200.

```
switch(config-if-ethernet1/0/1)#dot1q-tunnel selective s-vlan 1000 c-
vlan 100-200
```

Включить selective QinQ на Ethernet1/0/1.

```
switch(config-if-ethernet1/0/1)#dot1q-tunnel selective enable
```
Настроить порт Ethernet 1/0/2 в режим Hybrid, настроить его для удаления тэга VLAN при приеме пакета с тэгом VLAN 2000.
```
switch(config-if-ethernet1/0/2)#switchport mode hybrid
switch(config-if-ethernet1/0/2)#switchport hybrid allowed vlan 2000
untag
```
Настроить правило сопоставления selective QinQ на Ehernet1/0/2 для добавления тэга VLAN 2000 как внешней метки в пакетах с тэгами из диапазона VLAN от 201 до 300.
```
switch(config-if-ethernet1/0/2)#dot1q-tunnel selective s-vlan 2000 c-
vlan 201-300
```
Включить selective QinQ на Ethernet1/0/2.
```
switch(config-if-ethernet1/0/2)#dot1q-tunnel selective enable
```
Настроить порт Ethernet 1/0/9 в режим Hybrid, настроить его для удаления тэга VLAN при приеме пакета с тэгом VLAN 1000 и VLAN 2000.
```
switch(config-if-ethernet1/0/2)#interface ethernet 1/0/9
switch(config-if-ethernet1/0/9)#switchport mode hybrid
switch(config-if-ethernet1/0/9)#switchport hybrid allowed vlan
1000;2000 tag
```

После настройки коммутатора “SwitchA” пакеты с VLAN из диапазона от 100 до 200 из порта Ethernet1/0/1 будут автоматически тегироваться VLAN 1000 в качестве внешней метки, пакеты с VLAN из диапазона от 200 до 301 из порта Ethernet1/0/1 будут автоматически тегироваться VLAN 2000 в качестве внешней метки.

Конфигурация коммутатора “SwitchB” похожа на конфигурацию коммутатора “SwitchA” и выглядит следующим образом:

```
switch(config)#vlan 1000;2000
switch(config)#interface ethernet 1/0/1
switch(config-if-ethernet1/0/1)#switchport mode hybrid
switch(config-if-ethernet1/0/1)#switchport hybrid allowed vlan 1000
untag
switch(config-if-ethernet1/0/1)#dot1q-tunnel selective s-vlan 1000 c-
vlan 100-200
switch(config-if-ethernet1/0/1)#dot1q-tunnel selective enable
switch(config-if-ethernet1/0/1)#interface ethernet 1/0/2
switch(config-if-ethernet1/0/2)#switchport hybrid allowed vlan 2000
untag
switch(config-if-ethernet1/0/2)#dot1q-tunnel selective s-vlan 2000 c-
vlan 201-300
switch(config-if-ethernet1/0/2)#dot1q-tunnel selective enable
switch(config-if-ethernet1/0/9)#switchport mode hybrid
switch(config-if-ethernet1/0/9)#switchport hybrid allowed vlan
1000;2000 tag
```

21.4. Решение проблем при настройке Selective QinQ

- Функции Selective QinQ и dot1q-tunnel не должны настраиваться одновременно на одном и том же порту.

22. Flexible QinQ

22.1 Общие сведения о Flexible QinQ

Flexible QinQ принимает решение добавлять внешний тэг VLAN (SPVLAN tag) или нет, основываясь на потоке кадров данных. Например, Гибкий QinQ может быть реализован на основе тэга VLAN пользователя, MAC-адреса, IPv4/IPv6 адреса, протокола IPv4/IPv6, номером порта приложения и т.д. Таким образом эта технология позволяет гибко инкапсулировать поток данных пользователя по различным схемам и различными методами.

22.2 Конфигурация Flexible QinQ

Соответствие потока данных Flexible QinQ реализовано на основе правил карты политик (policy-map):

1. Создать карту класса (class-map) для классификации различных поток данных;
2. Создать карту политик (policy-map) Flexible QinQ для связи с картой класса (class-map) и выбора операции;
3. Применить Flexible QinQ на порт;
4. Проверка текущей конфигурации Flexible QinQ.

1. Создать карту класса (class-map) для классификации различных поток данных;

Команда	Описание

`class-map <class-map-name>`
 	
`no class-map <class-map-name>`
 	
В режиме глобальной конфигурации
	Создание карты классов с именем `<class-map-name>` и вход в режим конфигурирования этой карты классов.
	
	Команда `no` удаляет карты классов с именем `<class-map-name>`

`match {access-group <acl-index-or-name> | ip dscp <dscp-list>| ip precedence <ip-precedence-list> | ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <cos-list>}`
 	
`no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6`
	Настройка критерия соответствия данных карте классов. Команда `no` отменяет конфигурацию соответствия.

`flowlabel | vlan | cos }` В режиме глобальной конфигурации	

2. Создать карту политик (policy-map) Flexible QinQ для связи с картой класса (class-map) и выбора операции;

Команда	Описание

`policy-map <policy-map-name>`
`no policy-map <policy-map-name>`
 	
В режиме глобальной конфигурации
	Создание карты политик с именем и вход в режим её конфигурирования `<policy-map-name>`. Команда `no` удаляет карту политик

`class <class-map-name> [insert-before <class-map-name>]`
 	
`no class <class-map-name>`
 	
В режиме глобальной конфигурации
	Задать для текущей карты политик ассоциацию с картой классов с именем `<class-map-name>`.
	`insert-before <class-map-name>` - позволяет добавить карту классов для ассоциации раньше, чем с именем `<class-map-name>`.
	
	Команда `no` отменяет эту ассоциацию.

`set {ip dscp <new-dscp> | ip precedence <new-precedence> | internal priority <new-inp> | drop precedence <new-dp> | cos <new-cos> | s-vid<new-vid>}`
 	
`no set {ip dscp | ip precedence | internal priority | drop precedence | cos|s-vid }`
 	
В режиме глобальной конфигурации
	Присвоить классифицированному трафику новое значение dscp (`ip dscp <new-dscp>`), значение ip presedence (`ip precedence <new-precedence>`), значение приоритета сброса (`drop precedence <new-dp>`), значение поля cos (`cos <new-cos>`), внешний тег vlan (`s-vid <new-vid>`)
	
	Команда `no` отменяет присвоение.

3. Применить Flexible QinQ на порт.

Команда	Описание

`service-policy input <policy-map-name>`
 	
`no service-policy input {<policy-map-name>}`
	Применить карту политик с именем `<policy-map-name>` для входящего трафика на порту
	
	Команда `no` удаляет карту политик с именем `<policy-map-name>` с порта.

в режиме конфигурирования интерфейса	

4. Просмотр конфигурации Flexible QinQ

Команда	Описание
`show mls qos {interface [<interface-id>]` В привилегированном режиме	Просмотр текущей конфигурации Flexible QinQ на порту `<interface-id>`

22.3 Пример конфигурации Flexible QinQ

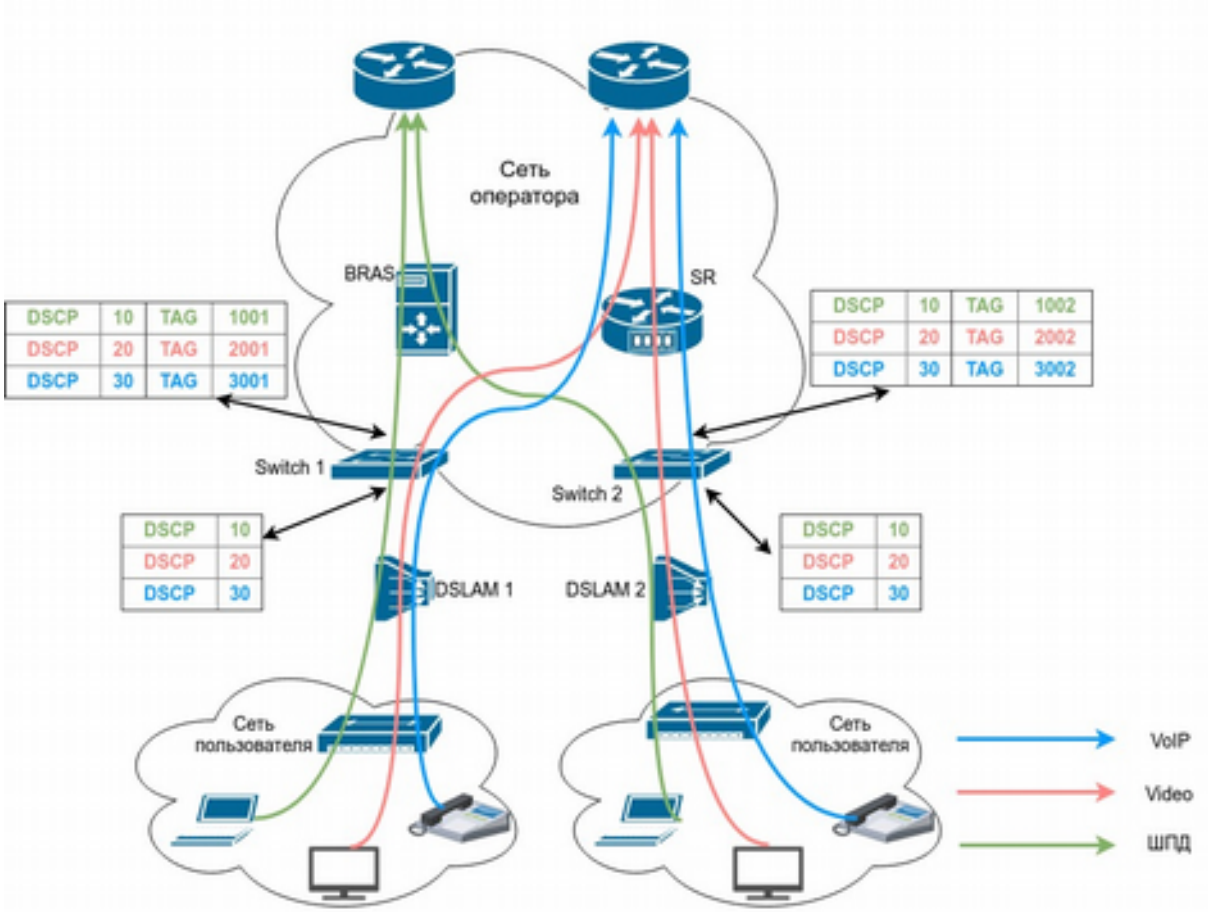


Рис. 22-1 Пример использования Flexible QinQ

Как показано на рисунке 22-1, первый пользователь, подключенный к DSLAM1, назначает метки DSCP 10, 20 и 30 для исходящего трафика в своей сети. DSCP10 соответствует Широкополосному доступу, DSCP20 соответствует VoIP, DSCP соответствует VOD. После того, как на портах коммутаторов в сторону клиентов будет включен Гибкий QinQ, пакетам с разным значением DSCP будут добавлены различные внешние тэги VLAN, уникальные в публичной сети оператора. Пакетам с DSCP10 будет добавлен тег 1001, трафик будет отправлен на BRAS. Пакетам с DSCP20 (DSCP30) будет

добавлен внешний тег VLAN 2001 (3001 соответственно), трафик будет отправлен на SR. Второй пользователь, подключенный к DSLAM2, также добавляет различные метки DSCP, метки внешнего тега будут добавлены аналогичным образом. На приведенном выше рисунке внешний тег второго пользователя отличается от первого пользователя для различия DSLAM и местонахождения пользователей.
Предположим, что DSLAM подключены к портам ethernet 1/0/1 обоих коммутаторов соответственно.

Конфигурация будет выглядеть следующим образом:

Switch1:

```
Switch(config)#class-map c1
Switch(config-classmap-c1)#match ip dscp 10
Switch(config-classmap-c1)#exit
Switch(config)#class-map c2
Switch(config-classmap-c2)#match ip dscp 20
Switch(config-classmap-c2)#exit
Switch(config)#class-map c3
Switch(config-classmap-c3)#match ip dscp 30
Switch(config-classmap-c3)#exit
Switch(config)#policy-map p1
Switch(config-policymap-p1)#class c1
Switch(config-policymap-p1-class-c1)# set s-vid 1001
Switch(config-policymap-p1)#class c2
Switch(config-policymap-p1-class-c2)# set s-vid 2001
Switch(config-policymap-p1)#class c3
Switch(config-policymap-p1-class-c3)# set s-vid 3001
Switch(config-policymap-p1-class-c3)#exit
Switch(config-policymap-p1)#exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#dot1q-tunnel enable
Switch(config-if-ethernet1/0/1)#service-policy p1 in
```

Switch2:

```
Switch(config)#class-map c1
Switch(config-classmap-c1)#match ip dscp 10
Switch(config-classmap-c1)#exit
Switch(config)#class-map c2
Switch(config-classmap-c2)#match ip dscp 20
Switch(config-classmap-c2)#exit
Switch(config)#class-map c3
Switch(config-classmap-c3)#match ip dscp 30
Switch(config-classmap-c3)#exit
Switch(config)#policy-map p1
Switch(config-policymap-p1)#class c1
Switch(config-policymap-p1-class-c1)# set s-vid 1002
```

```
Switch(config-policymap-p1)#class c2
Switch(config-policymap-p1-class-c2)# set s-vid 2002
Switch(config-policymap-p1)#class c3
Switch(config-policymap-p1-class-c3)# set s-vid 3002
Switch(config-policymap-p1-class-c3)#exit
Switch(config-policymap-p1)#exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#dot1q-tunnel enable
Switch(config-if-ethernet1/0/1)# service-policy p1 in
```

22.4 Решение проблем с конфигурацией Flexible QinQ

В случае, если Flexible QinQ не может быть применен к порту, проверьте не вызвана ли проблема следующими причинами:

- Убедитесь, что в настроенною карту классов и карту политик добавлен Flexible QinQ;
- Убедитесь, что ACL содержит правило permit, а карта классов настроена на соответствие правилу ACL;
- Убедитесь, что коммутатору достаточно ресурса TCAM для работы правила.

23. VLAN-translation

23.1 Общие сведения о VLAN-translation

VLAN-translation - это функция, которая позволяет преобразовать тэг VLAN пакета в новый в соответствии с требованиями. Это позволяет обмениваться данными в разных VLAN.
VLAN-translation может быть использован на обоих направлениях трафика. Конфигурация VLAN-translation описана в этой главе.

23.2 Настройка VLAN-translation

1. Включение функции VLAN-translation на порту
2. Создание соответствия VLAN-translation на порту
3. Конфигурирование сброса пакетов при возникновении ошибок трансляции VLAN
4. Просмотр сконфигурированных соответствий VLAN-translation

1. Включение функции VLAN-translation на порту

Команда	Описание
`vlan-translation enable`	Включить функцию VLAN-translation на порту
`no vlan-translation enable`	Выключить функцию VLAN-translation на порту
В режиме конфигурации порта	

2. Создание соответствия VLAN-translation на порту

Команда	Описание
`vlan-translation <old-vlan-id> to <new-vlan-id> {in | out}`	Задать соответствие VLAN-translation
`no vlan-translation old-vlan-id {in | out}`	Удалить соответствие VLAN-translation
В режиме конфигурации порта	

3. Конфигурирование сброса пакетов при возникновении ошибок трансляции VLAN

Команда	Описание

`vlan-translation miss drop {in | out | both}`
 	
`no vlan-translation miss drop {in | out | both}`
 	
В режиме конфигурации порта
	Сконфигурировать сброс пакетов
	
	Отменить сброс пакетов

4. Просмотр сконфигурированных соответствий VLAN-translation

Команда	Описание
`show vlan-translation` В Admin режиме	Просмотр сконфигурированных соответствий трансляции VLAN

23.3 Конфигурация VLAN-translation

Сценарий:

Пограничные коммутаторы PE1 и PE2 Интернет-провайдера поддерживают VLAN 20 для передачи трафика между CE1 и CE2 из клиентской сети через собственный VLAN 3. Порт 1/0/1 PE1 Подключен к CE1, порт 1/0/10 подключен к публичной сети, порт 1/0/1 PE2 подключен к CE2, порт 1/0/10 подключен к публичной сети.

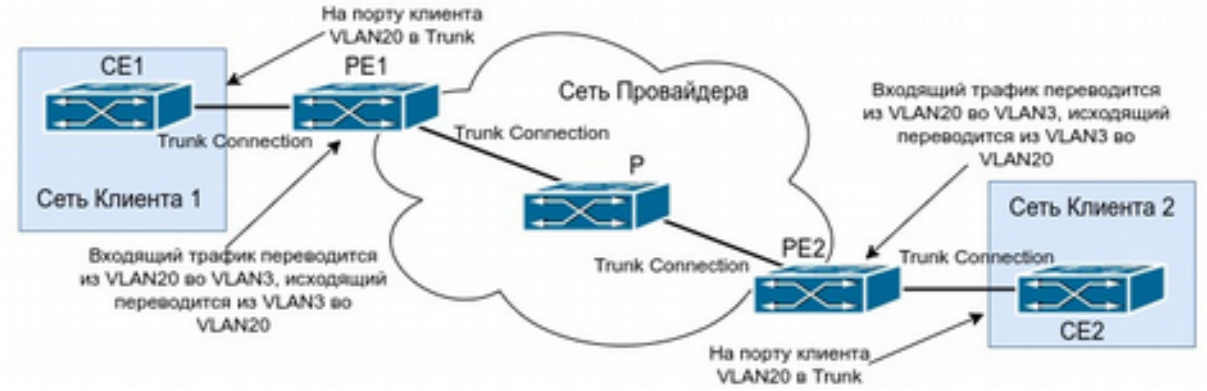


Рисунок 23.1 Топология с применением VLAN-translation

Объект	Описание конфигурации
VLAN-translation	Ethernet1/0/1 of PE1 and PE2.
Trunk Port	Ethernet1/0/1 and Ethernet1/0/10 of PE1 and PE2.

Конфигурация будет выглядеть следующим образом:

```
switch(Config)#interface ethernet 1/0/1
switch(Config-Ethernet1/0/1)#switchport mode trunk
switch(Config-Ethernet1/0/1)# vlan-translation enable
switch(Config-Ethernet1/0/1)# vlan-translation 20 to 3 in
switch(Config-Ethernet1/0/1)# vlan-translation 3 to 20 out
switch(Config-Ethernet1/0/1)# exit
switch(Config)#interface ethernet 1/0/10
switch(Config-Ethernet1/0/10)#switchport mode trunk
switch(Config-Ethernet1/0/10)#exit
switch(Config)#
```

22.4 Решение проблем с конфигурацией VLAN-translation

- VLAN-translation используется только на портах в режиме Trunk;
- При включенной функции VLAN-translation правила QoS применяются на Vlan после изменения тэга.

24. Multi-to-One VLAN-translation

24.1 Общие сведения о Multi-to-One VLAN-translation

Функция Multi-to-One VLAN-translation позволяет изменять тег пакетов нескольких VLAN одновременно на тэг нового VLAN на линиях uplink и возвращать оригинальный тэг в портах downlink.

В этой главе подробно описана функция Multi-to-One VLAN-translation и её настройка.

24.2 Конфигурация Multi-to-One VLAN-translation

1. Настройка соответствия VLAN
2. Просмотр сконфигурированных соответствий

1. Настройка соответствия VLAN

Команда	Описание

`vlan-translation n-to-1 <WORD> to <new-vlan-id> in`
 	
`no vlan-translation n-to-1 <WORD> to <new-vlan-id> in`
 	
В режиме конфигурации порта
	Задать соответствие VLAN
	`<WORD>`
	`<new-vlan-id>`
	
	Удалить соответствие VLAN

2. Просмотр сконфигурированных соответствий

Команда	Описание
`show vlan-translation` В Admin режиме	Просмотр сконфигурированных соответствий трансляции VLAN

24.3 Пример конфигурации Multi-to-One VLAN-translation

Сценарий:

Пользователи UserA, UserB и userC принадлежат VLAN1, VLAN2, VLAN3 соответственно. До выхода в сеть оператора, трафик пользователей UserA, UserB и UserC преобразовывается по VLAN 100 на порту Ethernet 1/0/1 пограничного коммутатора “switch1”. Трафик из сети оператора во VLAN 100, предназначенный пользователям UserA, UserB и userC будет преобразован во VLAN1, VLAN2, VLAN3. Точно такая же

операция будет выполнена на порту Ethernet 1/0/1 пограничного коммутатора “switch2” для трафика пользователей UserD, UserE и userF.

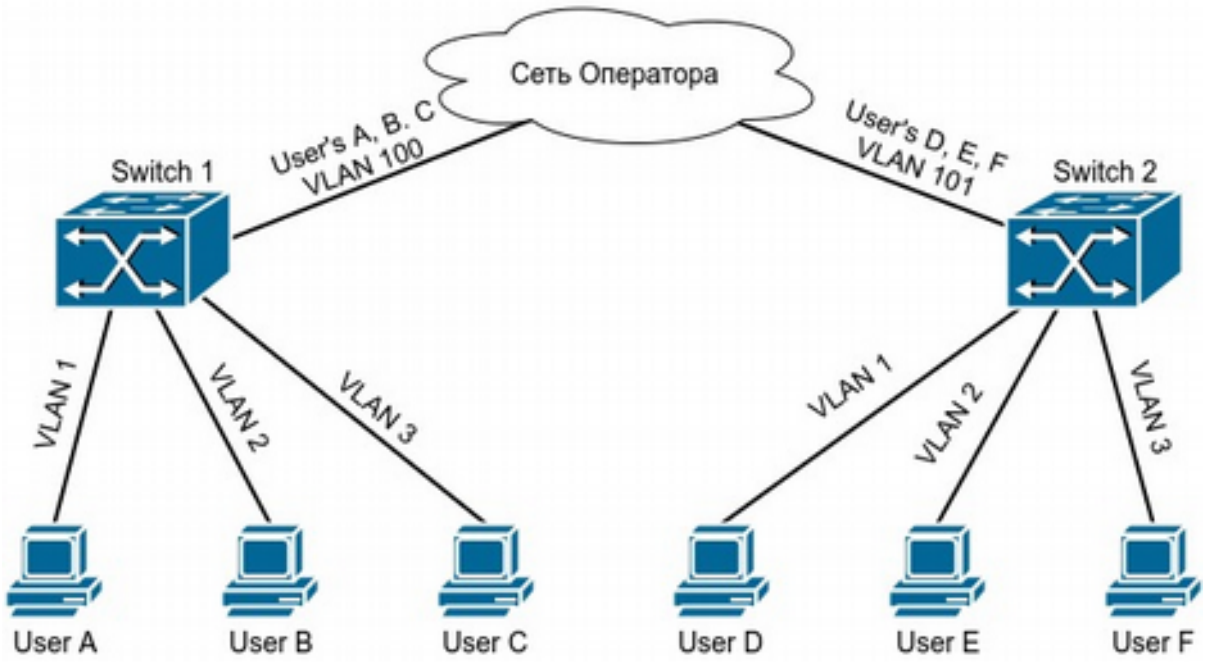


Рисунок 24.1 топология Multi-to-One VLAN-translation

Объект	Описание конфигурации
VLAN	Switch1、Switch2
Trunk Port	Downlink port 1/0/1 and uplink port 1/0/5 of Switch1 and Switch 2
Multi-to-One VLAN-translation	Downlink port 1/0/1 of Switch1 and Switch2

Конфигурация будет выглядеть следующим образом:

Switch1、Switch2:

```
switch(Config)# vlan 1-3;100
switch(Config-Ethernet1/0/1)#switchport mode trunk
switch(Config-Ethernet1/0/1)# vlan-translation n-to-1 1-3 to 100
switch(Config)#interface ethernet 1/0/5
switch(Config-Ethernet1/0/5)#switchport mode trunk
switch(Config-Ethernet1/0/5)#exit
```

24.4 Решение проблем с Multi-to-One VLAN-translation

- не используйте Multi-to-One VLAN-translation одновременно с Dot1q-tunnel;
- не используйте Multi-to-One VLAN-translation одновременно с VLAN-translation;
- одинаковые MAC-адреса не должны находиться в оригинальном и транслируемом VLAN.

25. Динамический VLAN

25.1 Общие сведения о Динамическом VLAN

Динамический VLAN - это обобщенное понятие, названное так в противопоставление статическому VLAN (применяемому статически на порт). Динамический VLAN включает в себя VLAN основанный на MAC-адресах, VLAN подсетей и протокольный VLAN.

VLAN, основанный на MAC-адресах (MAC VLAN) - это технология, позволяющая распределять трафик по VLAN на основе MAC-адреса: каждый хост с различным MAC-адресом может быть назначен определенному VLAN, в зависимости от обозначенных требований. Это дает возможность отказаться от настройки VLAN при изменении местоположения пользователя: в не зависимости от местоположения, трафик пользователя будет определен в свой VLAN.

VLAN подсетей (IP-subnet VLAN) - технология, позволяющая распределять трафик по различным VLAN на основе IP-адреса источника и маске его подсети. Его преимущество такое же, как у VLAN на основе MAC: пользователю не нужно изменять конфигурацию при изменении своего местоположения.

Разделение **VLAN на основе протокола сетевого уровня (Protocol VLAN)** будет удобен для тех администраторов, которые хотят разделять пользователей по приложениям или сервисам. Его удобство состоит в том, что пользователь может изменять свое местоположение в сети, сохраняя при этом свое членство во VLAN.

Важно! Использование динамических VLAN требует настройку порта в режим Hybrid.

25.2 Конфигурация динамических VLAN

1. Включение функции Динамических VLAN на интерфейсе
2. Выбор VLAN в качестве MAC VLAN
3. Настройка соответствия между MAC-адресом и VLAN
4. Включение IP-subnet VLAN на интерфейсе
5. Настройка соответствия между IP маской и VLAN
6. Настройка соответствия между протоколом сетевого уровня и VLAN
7. Настройка приоритета для Динамических VLAN

1. Включение функции Динамического VLAN на интерфейсе

Команда	Описание
`switchport mac-vlan enable`	Включить функцию динамических VLAN на интерфейсе
`no switchport mac-vlan enable`	Выключить функцию динамических VLAN на интерфейсе

В режиме конфигурации порта	

2. Выбор VLAN в качестве MAC VLAN

Команда	Описание

`mac-vlan vlan <vlan-id>`
 	
`no mac-vlan`
 	
В режиме глобальной конфигурации
	назначить VLAN в качестве MAC-based VLAN
	
	удалить MAC-based VLAN

3. Настройка соответствия между MAC-адресом и VLAN

Команда	Описание

`mac-vlan mac <mac-address> <mac-mask> vlan <vlan-id> priority <priority-id>`
 	
`no mac-vlan {mac <mac-address> <mac-mask>|all}`
 	
В режиме глобальной конфигурации
	Создать соответствие между MAC-адресом и VLAN
	
	Удалить соответствие между MAC-адресом и VLAN

4. Включение IP-subnet VLAN на интерфейсе

Команда	Описание

`switchport subnet-vlan enable`
 	
`no switchport subnet-vlan enable`
 	
В режиме конфигурации порта
	Включение IP-subnet VLAN на интерфейсе
	
	Выключение IP-subnet VLAN на интерфейсе

5. Настройка соответствия между IP маской и VLAN

Команда	Описание
`subnet-vlan ip-address <ipv4-address> mask <subnet-mask> vlan <vlan-id> priority <priority-id>`	Добавить соответствие между IP-подсетью и VLAN

`no subnet-vlan {ip-address <ipv4-addrss> mask <subnet-mask>|all}` В режиме глобальной конфигурации	Удалить соответствие между IP-подсетью и VLAN

6. Настройка соответствия между протоколом сетевого уровня и VLAN

Команда	Описание

`protocol-vlan mode {ethernetii etype <etype-id>|llc {dsap <dsap-id> ssap <ssap-id>}|snap etype <etype-id>} vlan <vlan-id> priority <priority-id>`
 	
`no protocol-vlan {mode {ethernetii etype <etype-id>|llc {dsap <dsap-id> ssap <ssap-id>}|snap etype <etype-id>}|all}`
 	
В режиме глобальной конфигурации
	Добавить соответствие между протоколом и VLAN
	
	Удалить соответствие между протоколом и VLAN

7. Настройка приоритета для Динамических VLAN

Команда	Описание

`dynamic-vlan mac-vlan prefer`
 	
`dynamic-vlan subnet-vlan prefer`
 	
В режиме глобальной конфигурации
	Задать приоритет между динамическими VLAN

25.3 Конфигурация динамических VLAN

Сценарий:

В компании существует несколько отделов, каждый из них принадлежит к своему VLAN. Некоторым сотрудникам отдела, принадлежащего к VLAN100, часто приходится перемещаться по всей офисной сети. Предположим, ноутбук сотрудника M имеет MAC-адрес 00-03-0f-11-22-33. Когда сотрудник M перемещается в часть сети с VLAN200 или 300, порт коммутатора, настроенный в режим Hybrid с VLAN 100 в качестве untag направит трафик с MAC-адресом ноутбука M во VLAN 100.

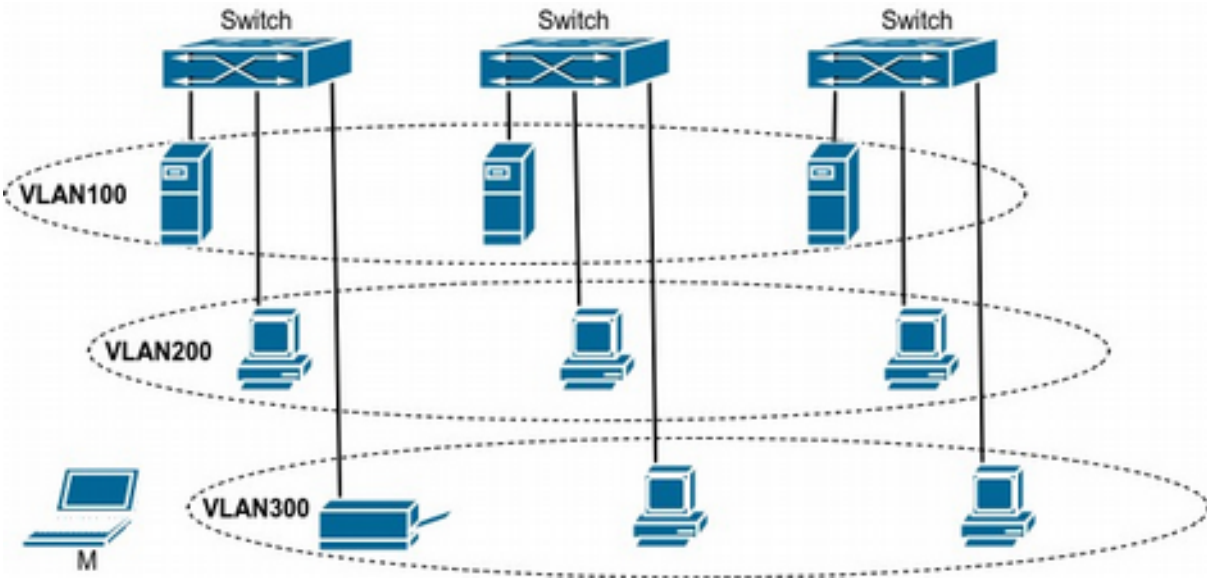


Рисунок 25.1 Пример применения динамических VLAN

Объект	Описание конфигурации
MAC VLAN	Глобальная конфигурация SwitchA, SwitchB, SwitchC

Для примера взята конфигурация коммутатора SwitchA, но она одинакова для SwitchB и SwitchC:

```
SwitchA(Config)#mac-vlan mac 00-03-0f-11-22-33 vlan 100 priority 0
SwitchA(Config)#interface ethernet 1/0/1
SwitchA(Config-Ethernet1/0/1)#switchport mode hybrid
SwitchA(Config-Ethernet1/0/1)#switchport hybrid allowed vlan 100 untagged
```

25.4 Решение проблем с конфигурацией динамических VLAN

- Первый пакет к устройству, подключенному к динамическому VLAN, может не пройти. Сначала необходимо, чтобы коммутатор изучил мак-адрес этого устройства, для этого необходимо с данного устройства отправить пакет на коммутатор (например, ping).

26. GVRP

26.1 Общие сведения о GVRP

GVRP (Genecic VLAN Registration Protocol) является одним из приложений GARP (Generic Attribute Registration Protocol, Протокол регистрации общих аттрибутов). GARP был разработан IEEE для использования в сетевых мостах, сетевых коммутаторах, или других аналогичных устройствах с возможностью регистрации и перерегистрации специальных атрибутов, таких как идентификаторы VLAN и членство в мультикастовых группах в больших локальных сетях. GVRP - приложение GARP, которое отвечает за обмен информацией о VLAN и позволяет коммутаторам регистрировать VLAN динамически. Рассмотрим пример на рисунке:

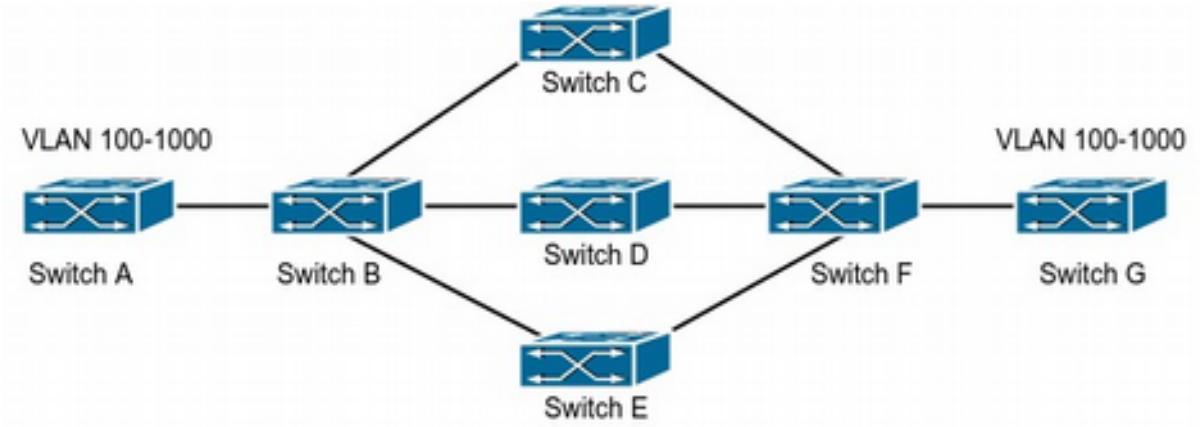


Рисунок 26.1 - типовое применение GVRP

В сети 2 уровня коммутаторы A и G не подключены друг к другу напрямую. Коммутаторы B,C,D,E,F выступают в роли промежуточных коммутаторов, соединяющий A и G. На коммутаторах A и G вручную настроены VLAN100-1000, в то время как на коммутаторах B,C,D,E,F VLAN не настроены. Пока GVRP не включен A и G не имеют связности друг с другом, поскольку промежуточные коммутаторы не имеют соответствующих VLAN. Однако после включения GVRP на всех коммутаторах его механизм передачи атрибутов VLAN позволяет промежуточным коммутаторам динамически регистрировать VLAN и у коммутаторов A и G появится связность в VLAN100-1000. VLAN, динамически зарегистрированные на промежуточных коммутаторах, будут удалены, если VLAN100-1000 будут удалены с коммутаторов A и G вручную.
Таким образом, несмежные коммутаторы, находясь в одной и той же VLAN могут установить связность друг с другом через GVRP, вместо ручной настройки VLAN на каждом из промежуточных коммутаторов.

26.2 Конфигурация GVRP

1. Настройка таймеров GVRP
2. Настройка GVRP на интерфейсе

3. Включение функции GVRP

1. Настройка таймеров GVRP

Команда	Описание

`garp timer join <200-500>`
`garp timer leave <500-1200>`
`garp timer leaveall <5000-60000>`
`no garp timer (join | leave | leaveAll)`
 	
В режиме глобальной конфигурации
	Настройка таймера для отправки GVRP-сообщений leaveall, join, и leave.

2. Настройка GVRP на интерфейсе

Команда	Описание

`gvrp`
`no gvrp`
 	
В режиме конфигурации порта
	Включение\выключение функции GVRP на интерфейсе

3. Включение функции GVRP

Команда	Описание

`gvrp`
`no gvrp`
 	
В режиме глобальной конфигурации
	Включение\выключение функции GVRP глобально

26.3 Пример конфигурации GVRP

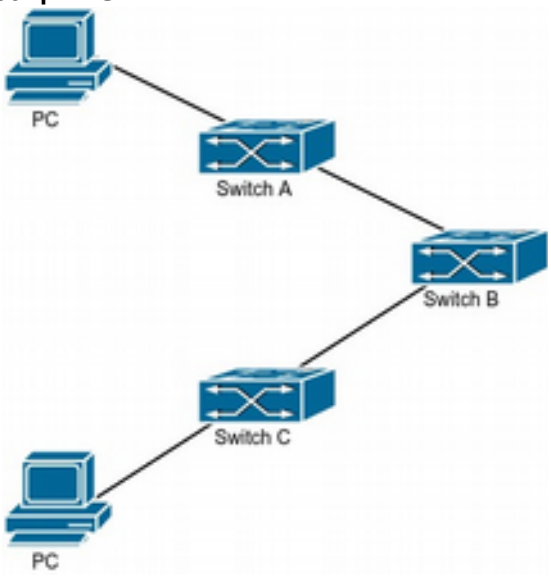


Рисунок 26.2 Пример конфигурации GVRP

Для получения информации динамической регистрации VLAN и её обновления на коммутаторах должен быть сконфигурирован протокол GVRP. Настроенный протокол GVRP на коммутаторах Switch A, Switch B и Switch C позволяет динамически сконфигурировать VLAN 100 на коммутаторе B а двум ПК, подключенным к VLAN 100 на коммутаторах Switch A и Switch C, связаться между собой без статического конфигурирования VLAN 100 на коммутаторе Switch B.

Объект	Описание конфигурации
VLAN100	Порты Ethernet1/0/2-6 на коммутаторах Switch A и Switch C
Режим Trunk	Порт Ethernet1/0/11 на Switch A и Switch C, порт Ethernet1/0/10 и 1/0/11 на коммутаторе Switch B.
Функция GVRP	Коммутаторы Switch A, Switch B и Switch C
Порт GVRP	Порт Ethernet1/0/11 на Switch A и Switch C, порт Ethernet1/0/10 и 1/0/11 на коммутаторе Switch B.

Две рабочих станции (PC) подключены к любым портам коммутаторов Switch A и Switch B, в которые назначен VLAN100. Порт 1/0/11 Switch A подключен к порту 1/0/10 Switch B, а порт 1/0/11 Switch B подключен к порту 1/0/11 Switch A.

Switch A:

```
Switch (config)#gvrp
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/0/2-6
Switch (Config-Vlan100)#exit
Switch (config)#interface ethernet 1/0/11
Switch (Config-If-Ethernet1/0/11)#switchport mode trunk
Switch (Config-If-Ethernet1/0/11)#gvrp
Switch (Config-If-Ethernet1/0/11)#exit
```

Switch B:

```
Switch(config)#gvrp
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode trunk
Switch(Config-If-Ethernet1/0/10)#gvrp
Switch(Config-If-Ethernet1/0/10)#exit
Switch (config)#interface ethernet 1/0/11
Switch (Config-If-Ethernet1/0/11)#switchport mode trunk
```

```
Switch (Config-If-Ethernet1/0/11)#gvrp
Switch (Config-If-Ethernet1/0/11)#exit
```

Switch C:

```
Switch (config)#gvrp
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/0/2-6
Switch (Config-Vlan100)#exit
Switch (config)#interface ethernet 1/0/11
Switch (Config-If-Ethernet1/0/11)#switchport mode trunk
Switch (Config-If-Ethernet1/0/11)#gvrp
Switch (Config-If-Ethernet1/0/11)#exit
```

26.4 Решение проблем с конфигурацией GVRP

- Рекомендуется избегать использования функций GVRP и RSTP одновременно на коммутаторе. Если необходимо включить GVRP, сначала необходимо отключить функцию RSTP для портов.
- Таймеры GARP на обоих концах сети должны быть одинаковы, иначе GVRP не сможет работать нормально.

27. Voice VLAN

27.1 Общие сведения о Voice VLAN

Voice VLAN (Голосовая VLAN) предназначен для трафика голосовых данных пользователя. Настроив Voice VLAN пользователь сможет настроить QoS (качество сервиса) для голосовых данным и повысить приоритет передачи трафика голосовых данным для обеспечения качества вызова.
После настройки соответствия Voice VLAN - MAC-адрес и включения Voice VLAN на интерфейсе, коммутатор будет отслеживать MAC-адрес голосового устройства в трафике данных, входящем в порт и передавать его Voice VLAN. Благодаря этому оборудование может всегда относиться к определенной Voice VLAN даже если голосовое устройство будет перемещено физически без модификации конфигурации коммутатора.

Важно! Использование динамических VLAN требует настройку порта в режим Hybrid.

27.2 Конфигурация Voice VLAN

1. Выбор VLAN как Voice VLAN
2. Добавление голосового оборудования в Voice VLAN
3. Включение Voice VLAN на портах

1. Выбор VLAN как Voice VLAN

Команда	Описание

`voice-vlan vlan <vlan-id>`
 	
`no voice-vlan`
 	
В режиме глобальной конфигурации
	Выбор VLAN в качестве Voice VLAN
	
	Отмена выбора VLAN в качестве Voice VLAN

2. Добавление голосового оборудования в Voice VLAN

Команда	Описание

`voice-vlan mac <mac-address> mask <mac-mask> priority <priority-id> [name <voice-name>]`
 	
`no voice-vlan {mac <mac-address> mask <mac-mask>|name <voice-name> |all}`
 	
В режиме глобальной конфигурации
	Выбор MAC-адреса голосового оборудования для добавления в Voice VLAN
	
	Удаление MAC-адреса голосового оборудования из Voice VLAN

3. Включение Voice VLAN на портах

Команда	Описание

`switchport voice-vlan enable`
`no switchport voice-vlan enable`
 	
В режиме конфигурации порта
	Включение функции Voice VLAN на порту
	
	Выключение функции Voice VLAN на порту

27.3 Пример конфигурации Voice VLAN

Сценарий:

Устройства “IP-phone1” и “IP-phone2” могут быть подключены к любому порту Ethernet-порту коммутатора. “IP-phone1” имеет MAC-адрес 00-03-0f-11-22-33 и подключен к порту коммутатора Ethernet 1/0/1, “IP-phone2” имеет MAC-адрес 00-03-0f-11-22-55 и подключен к порту коммутатора Ethernet 1/0/2.

Объект	Описание конфигурации
Voice VLAN	Конфигурация в режиме глобальной конфигурации на коммутаторе

Конфигурация будет выглядеть следующим образом:

```
Switch 1:
Switch(config)#vlan 100
Switch(Config-Vlan100)#exit
Switch(config)#voice-vlan vlan 100
Switch(config)#voice-vlan mac 00-03-0f-11-22-33 mask 255 priority 5
name company
Switch(config)#voice-vlan mac 00-03-0f-11-22-55 mask 255 priority 5
name company
switch(Config)#interface ethernet1/0/10
switch(Config-If-Ethernet1/0/10)#switchport mode trunk
switch(Config-If-Ethernet1/0/10)#exit
switch(Config)#interface ethernet 1/0/1
switch(Config-If-Ethernet1/0/1)#switchport mode hybrid
switch(Config-If-Ethernet1/0/1)#switchport hybrid allowed vlan 100
untag
switch(Config-If-Ethernet1/0/1)#exit
switch(Config)#interface ethernet 1/0/2
switch(Config-If-Ethernet1/0/2)#switchport mode hybrid
switch(Config-If-Ethernet1/0/2)#switchport hybrid allowed vlan 100
untag
```

```
switch(Config-If-Ethernet1/0/2)#exit
```

27.4 Решение проблем с Voice VLAN

- Voice VLAN не может использоваться одновременно с MAC VLAN.

28. Конфигурирование таблицы MAC-адресов

28.1 Общие сведения о таблице MAC-адресов

Таблица MAC - это таблица соответствий между MAC-адресами устройств назначения и портами коммутатора. MAC-адреса могут быть статические и динамические. Статические MAC-адреса настраиваются пользователем вручную, имеют наивысший приоритет, хранятся постоянно и не могут быть перезаписаны динамическими MAC-адресами. MAC-адреса - это записи, полученные коммутатором в пересылке кадров данных, и хранятся в течение ограниченного периода времени. Когда коммутатор получает кадр данных для дальнейшей передачи, он сохраняет MAC-адрес кадра данных вместе с соответствующим ему портом назначения. Когда MAC-таблица опрашивается для поиска MAC-адреса назначения, при нахождении нужного адреса кадр данных отправляется на соответствующий порт, иначе коммутатор отправляет кадр на широковещательный домен. Если динамический MAC-адрес не встречается в принятых кадрах данных длительное время, запись о нем будет удалена из MAC-таблицы коммутатора.

Возможны 2 операции с таблицей MAC-адресов:
1. Поиск MAC-адреса;
2. Пересылка или фильтрация кадра данных в соответствии с таблицей.

28.1.1 Получение таблицы MAC-адресов

Таблица MAC-адресов может быть создана динамически или статически. Статическая конфигурация заключается в ручной настройке соответствия между MAC-адресами и портами. Динамическое обучение - это процесс, в котором коммутатор изучает соответствие между MAC-адресами и портами и регулярно обновляет таблицу MAC. В этом разделе мы рассмотрим процесс динамического обучения MAC-таблицы.

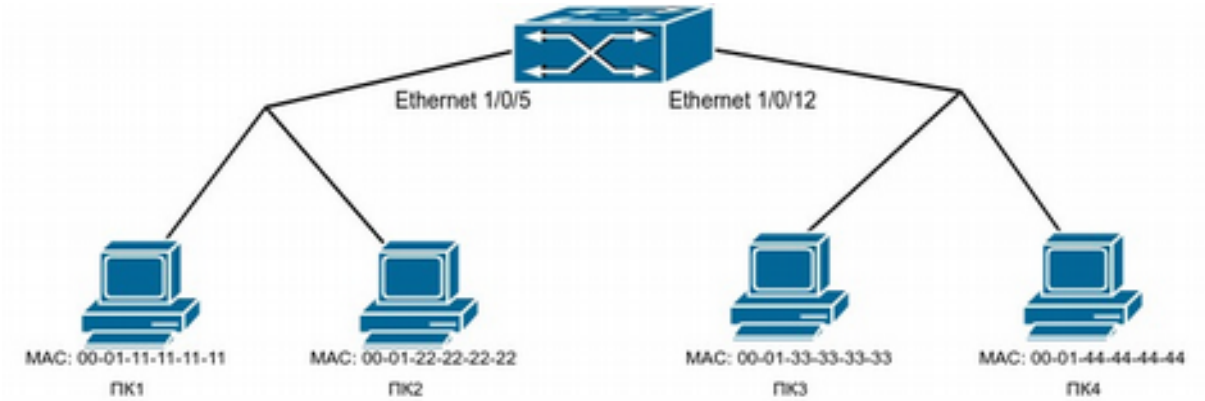


Рисунок 28-1 Динамическое обучение MAC-таблицы.

Топология на Рисунке 28-1: 4 ПК подключены к коммутатору. ПК1 и ПК2 подключены из одного физического сегмента (домена коллизий) подключены к порту

коммутатора Ethernet 1/0/5, а ПК3 и ПК4, также из одного физического сегмента, подключены к порту Ethernet 1/0/12.

Начальная таблица MAC-адресов не содержит записей. Рассмотрим пример обмена кадрами между ПК1 и ПК3 и процесс обучения MAC-адресов:

1. Когда ПК1 отправляет кадр к ПК3, MAC-адрес источника 00-01-11-11-11-11 из этого сообщения, а также порт коммутатора Ethernet 1/0/5 заносятся в MAC-таблицу;
2. В это же время коммутатор определяет, что сообщение предназначено для 00-01-33-33-33-33, а поскольку MAC-таблица содержит только запись соответствия MAC-адреса 00-01-11-11-11-11 и порта Ethernet 1/0/5, коммутатор передает это сообщение всем портам коммутатора (при условии, что все порты принадлежат VLAN 1 по-умолчанию);
3. ПК3 и ПК4, подключенные к порту Ethernet 1/0/12, получают кадр, отправленный ПК1, но так как MAC-адрес назначения 00-01-33-33-33-33, ПК4 не отвечает, только ПК3 отвечает ПК1. Когда порт Ethernet 1/0/12 принимает кадр от ПК3, в таблице MAC-адресов создается запись соответствия адреса 00-01-33-33-33-33 порту Ethernet 1/0/12.
4. Теперь таблица MAC-адресов имеет 2 записи: адрес 00-01-11-11-11-11 - порт Ethernet 1/0/5 и адрес 00-01-33-33-33-33 - порт Ethernet 1/0/12.
5. После обмена кадрами между ПК1 и ПК3, коммутатор больше не получает кадры от ПК1 и ПК3. ПОэтому записи соответствия MAC-адресов в MAC-таблице удаляются через 300 или 600 секунд (простое или двойне время жизни). По-умолчанию выбрано время жизни в 300 секунд, но оно может быть изменено на коммутаторе.

28.1.2 Пересылка или фильтрация

Коммутатор может переслать или отфильтровать принятые кадры данных в соответствии с таблицей MAC-адресов. Рассмотрим пример на рисунке 7-1: допустим, что коммутатор изучил MAC-адреса ПК1 и ПК3, а пользователь вручную добавил соответствия для MAC-адресов ПК2 и ПК4. Таблица MAC-адресов будет выглядеть следующим образом:

MAC-адрес	Номер порта	Способ добавления
00-01-11-11-11-11	1/0/5	Динамическое обучение
00-01-22-22-22-22	1/0/5	Статическое добавление
00-01-33-33-33-33	1/0/12	Динамическое обучение
00-01-44-44-44-44	1/0/12	Статическое добавление

1. Пересылка данных в соответствии с таблицей MAC-адресов:
   Если ПК 1 отправит кадр к ПК 3, коммутатор пересылает принятый кадр данных с порта 1/0/5 в порт 1/0/12.
2. Фильтрация в соответствии с таблицей MAC-адресов:
   Если ПК 1 отправит кадр к ПК 2, коммутатор, проверив таблицу MAC-адресов,

находит ПК 2 в том же физическом сегменте, что и ПК 1 - коммутатор отбрасывает этот кадр.

Коммутатором могут пересылаться 3 типа кадров:

1. **Широковещательные**. Коммутатор может определять коллизии в домене, но не в широковещательном. Если VLAN не определена, все устройства, подключенные к коммутатору, находятся в одном широковещательном домене. Когда коммутатор получает широковещательный кадр, он передает кадр во все порты. Если на коммутаторе настроены VLAN, таблица MAC-адресов соответствующим образом адаптирована для добавления информации о VLAN и широковещательные кадры будут пересылаться только в те порты, в которых настроена данная VLAN.
2. **Многоадресные.** Если многоадресный домен неизвестен, коммутатор пересылает многоадресный кадр как широковещательный. Если на коммутаторе включен IGMP-snooping и сконфигурирована многоадресная группа, коммутатор будет пересылать многоадресный кадр только портам этой группы.
3. **Одноадресные.** Если на коммутаторе не настроена VLAN, коммутатор ищет MAC-адрес назначения в таблице MAC-адресов и отправляет кадр на соответствующий порт. Если соответствие MAC-адреса и порта не найдено в таблице MAC-адресов, коммутатор пересылает одноадресный кадр как широковещательный. Если на коммутаторе настроен VLAN, коммутатор пересылает кадр только в этом VLAN. Если в таблице MAC-адресов найдено соответствие для VLAN, отличного от того, в котором был принят кадр, коммутатор пересылает кадр широковещательно в том VLAN, в котором кадр был принят.

28.2 Конфигурация таблицы MAC-адресов.

1. Настройка времени жизни MAC-адреса
2. Настройка статической пересылки и фильтрации
3. Очистка таблицы MAC-адресов
4. Обучение таблицы MAC-адресов через CPU

1. Настройка времени жизни MAC-адреса

Команда	Описание

`mac-address-table aging-time <0| aging-time>`
`no mac-address-table aging-time`
 	
В режиме глобальной конфигурации
	Настройка времени жизни MAC-адреса
	
	Применение настроек по-умолчанию

2. Настройка статической пересылки и фильтрации

Команда	Описание
`mac-address-table {static |`	Настройка статических записей и

`blackhole} address <mac-addr> vlan <vlan-id > [interface ethernet <interface-name>] | [source|destination|both]`
 	
`no mac-address-table {static | blackhole | dynamic} [address <mac-addr>] [vlan <vlan-id>] [interface ethernet <interface-name>]`
 	
В режиме глобальной конфигурации
	фильтрации
	
	Удаление статических записей и фильтрации

`l2-address-table static-multicast address {<ip-addr> |<mac-addr>} vlan <vlan-id> {interface [ethernet <interface-name>] | port-channel <port-channel-id>}`
 	
`no l2-address-table static-multicast address {<ip-addr> | <mac-addr>} vlan <vlan-id> {interface [ethernet <interface-name>] | port-channel <port-channel-id>}`
 	
В режиме глобальной конфигурации
	Настройка статической записи Многоадресного MAC-адреса
	
	Удаление статической записи Многоадресного MAC-адреса

3. Очистка таблицы MAC-адресов

Команда	Описание
`clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet | portchannel] <interface-name>]` В режиме глобальной конфигурации	Очистка динамических записей в таблице MAC-адресов.

4. Обучение таблицы MAC-адресов через CPU

Команда	Описание

`mac-address-learning cpu-control`
 	
`no mac-address-learning cpu-control`
	Включение функции обучения MAC-адресов через CPU.
	
	Отключение функции обучения MAC-адресов через CPU.

В режиме глобальной конфигурации	
`show collision-mac-address-table` В привилегированном режиме	Отображение коллизий в таблице MAC-адресов
`clear collision-mac-address-table` В режиме глобальной конфигурации	Очистка коллизий в таблице MAC-адресов

28.3 Пример конфигурации таблицы MAC-адресов

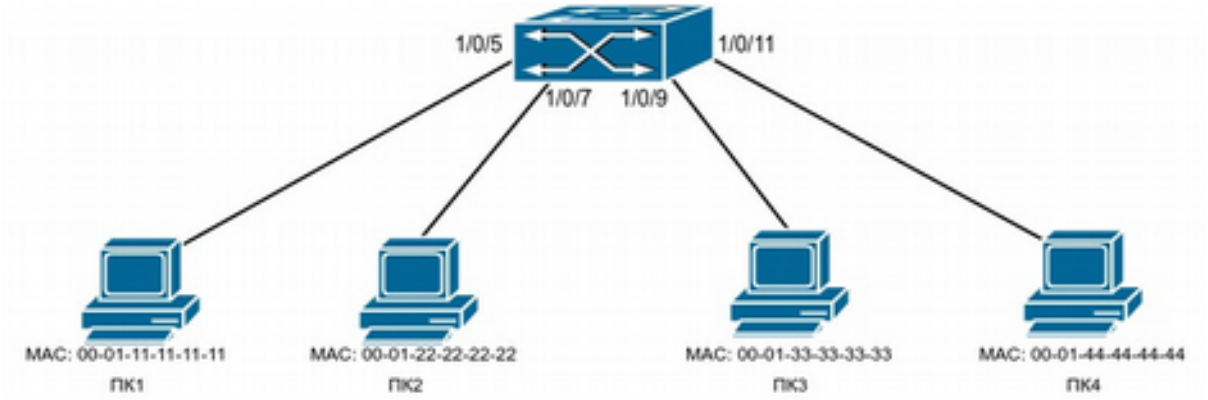


Рисунок 28-2 Пример конфигурации таблицы MAC-адресов

Как показано на рисунке 28-2, ПК1 - 4 подключены к портам коммутатора 1/0/5, 1/0/7, 1/0/9, 1/0/11, все ПК помещены во VLAN 1 по-умолчанию. ПК 1 хранит конфиденциальные данные и недоступен для ПК из других физических сегментов. ПК 1 и ПК 2 статически приписаны к портам 7 и 9 соответственно.

Этапы конфигурации:

1. Настроить MAC-адрес как фильтруемый:

```
Switch(config)#mac-address-table static 00-01-11-11-11-11 discard
vlan 1
```

2. Настроить статические соответствия ПК 2 и ПК 3 портам 1/0/7 и 1/0/9

```
Switch(config)#mac-address-table static address 00-01-22-22-22-22
vlan 1 interface ethernet 1/0/7
Switch(config)#mac-address-table static address 00-01-33-33-33-33
vlan 1 interface ethernet 1/0/9
```

28.4 Решение проблем при конфигурации таблицы MAC-адресов

Если с помощью команды ‘show mac-address-table’ обнаруживается, что коммутатор не смог создать динамическое соответствие между MAC-адресом и портом,

возможные причины:

- Подключенный кабель поврежден;
- На порту включен Spanning Tree и порт находится в состоянии “discarding” или устройство только что подключено к порту, а Spanning Tree находится в состоянии вычисления дерева;
- В остальных случаях проверьте порт коммутатора и обратитесь в техническую поддержку для решения проблемы

28.5 Уведомления об изменениях в MAC-таблице

Данная функция позволяет уведомлять администратора об изменениях в таблице MAC-адресов с помощью SNMP trap.

28.5.1 Настройка уведомлений об изменениях в MAC-таблице

1. Включение SNMP-функции уведомления об изменениях в MAC-таблице глобально
2. Включение уведомления об изменениях в MAC-таблице глобально
3. Настройка интервала отправки уведомления об изменениях в MAC-таблице
4. Настройка размера истории таблицы
5. Настройка типа события для отправки SNMP-trap
6. Просмотр конфигурации и данных
7. Очистка статистики

1. Включение SNMP-функции уведомления об изменениях в MAC-таблице глобально

Команда	Описание
snmp-server enable traps mac-notification **no snmp-server enable traps mac-notification** В режиме глобальной конфигурации	Включение SNMP-функции уведомления об изменениях в MAC-таблице Выключение SNMP-функции уведомления об изменениях в MAC-таблице

2. Включение уведомления об изменениях в MAC-таблице глобально

Команда	Описание
mac-address-table notification **no mac-address-table notification** В режиме глобальной конфигурации	Включение уведомления об изменениях в MAC-таблице Выключение уведомления об изменениях в MAC-таблице

3. Настройка интервала отправки уведомления об изменениях в MAC-таблице

Команда	Описание

`mac-address-table notification interval <0-86400>`
 	
`no mac-address-table notification interval`
 	
В режиме глобальной конфигурации
	Настройка интервала отправки уведомления об изменениях в MAC-таблице
	
	Возврат значений по-умолчанию (30 секунд)

4. Настройка размера истории таблицы

Команда	Описание

`mac-address-table notification history-size <0-500>`
 	
`no mac-address-table notification history-size`
 	
В режиме глобальной конфигурации
	Настройка размера истории таблицы
	
	Возврат значений по-умолчанию (10 записей)

5. Настройка типа события для отправки SNMP-trap

Команда	Описание

`mac-notification {added | both | removed}`
 	
`no mac-notification`
 	
В режиме конфигурации порта
	Выбор типа события для отправки SNMP-trap
	
	Выключение отправки по событию с данного интерфейса

6. Просмотр конфигурации и данных

Команда	Описание
`show mac-notification summary` В привилегированном режиме	Просмотр конфигурации и данных

7. Очистка статистики

Команда	Описание
`clear mac-notification statistics` В привилегированном режиме	Очистка статистики

28.5.2 Пример настройки уведомлений об изменениях в MAC-таблице

Предположим, система управления сетью (NMS - Network Management Station) настроена на прием сообщений SNMP-trap от коммутатора. Для того, чтобы коммутатор отправлял сообщения NMS при изменениях в таблице MAC-адресов, можно настроить функционал следующим образом:

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server enable traps mac-notification
Switch(config)# mac-address-table notification
Switch(config)# mac-address-table notification interval 5
Switch(config)# mac-address-table notification history-size 100
Switch(Config-If-Ethernet1/0/4)# mac-notification both
```

29. MSTP

29.1. Общие сведения о MSTP

Изначально для защиты сетей с кольцевыми топологиями использовались STP и его модификация RSTP, которые строили единое для всех VLAN покрывающее дерево. Это было просто с точки зрения эксплуатации, но не позволяло гибко управлять трафиком, разнося разные VLAN по разным физическим каналам. Проблема гибкости была решена в проприетарном PerVLAN Spanning Tree (PVST), который создавал отдельный процесс построения покрывающего дерева для каждого VLAN. Данный подход был довольно прост с точки зрения эксплуатации и очень гибок, но при большом количестве VLAN вызывал перегрузки CPU коммутатора. Так как трафик большинства VLAN использовал идентичные пути, смысла в разделении процессов STP для них не было, соответственно концепция протокола была доработана. Так появился Multiple Spanning Tree Protocol (MSTP), в котором создаются независимые экземпляры покрывающего дерева (*MSTI - Multiple Spanning Tree Instance*) для отдельных групп VLAN. Соответствия VLAN-MSTI задаются администратором вручную. Формат MSTP BPDU аналогичен RSTP BPDU. Для снижения нагрузки на коммутаторы, все BPDU различных MSTI коммутатора объединяются в один BPDU.

29.1.1 Регионы MSTP

Новая концепция вызывала сложности в эксплуатации, так как было необходимо идентично конфигурировать соответствие VLAN-MSTI на всех коммутаторах. Для упрощения и поддержания обратной совместимости с STP и RSTP была разработана концепция регионов.
Регион MSTP может быть образован из нескольких смежных коммутаторов с одинаковыми MSID (MST Configuration Identification), состоящими из:

- Имя региона MSTP;
- Ревизия конфигурации;
- Дайджест соответствий VLAN-MSTI.

MSID добавляется к MSTP BPDU так, что сохраняется совместимость с STP и RSTP. При этом MSTP BPDU, отправленные разными коммутаторами одного региона, воспринимаются смежными STP/RSTP-коммутаторами как RSTP BPDU одного коммутатора (Рис. 1-1). Таким образом кольцевая топология на разных коммутаторах по-прежнему поддерживается и в регионе MSTP сохраняется гибкость управления трафиком.

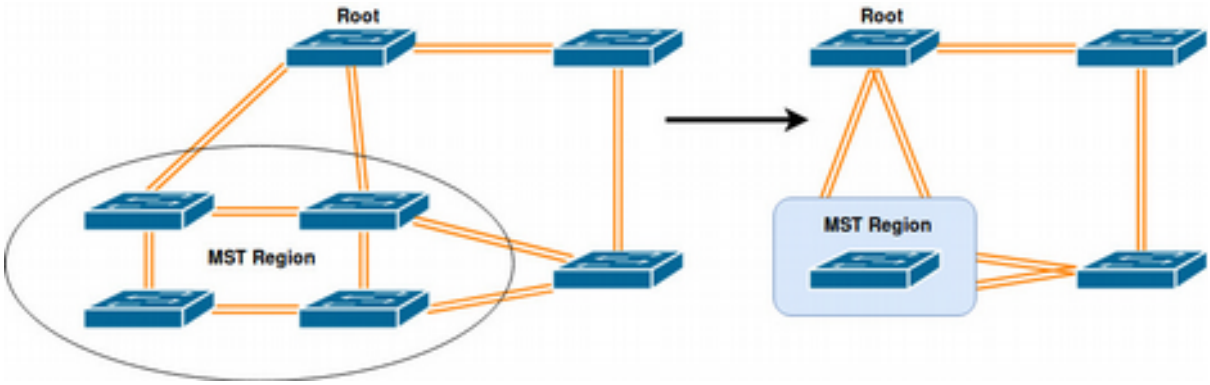


Рисунок 29.1 Регион MST в сети

MSTP внутри региона
Для каждого региона выбирается региональный корневой коммутатор, относительно которого строится внутреннее покрывающее дерево (*IST - Internal Spanning Tree*), объединяющее все коммутаторы региона. Региональный корневой коммутатор выбирается по наименьшему приоритету коммутатора, а при равных по минимальной стоимости пути до корневого коммутатора всей сети (либо региона, в котором находится корневой коммутатор). Если таких коммутаторов несколько, то среди них выбирается один с наименьшим ID.

MSTP между регионами
Для защиты топологий соединения различных регионов и отдельных коммутаторов строится общее покрывающее дерево (*CST - Common Spanning Tree*). В качестве корневой коммутатора в CST выбирается коммутатор с наименьшим приоритетом, а при равных с наименьшим ID. Каждый регион MSTP представляется для CST как отдельный виртуальный коммутатор.

CST совместно с IST всех регионов формируют полное покрывающее дерево сети (*CIST - Common and Internal Spanning Tree*).

29.1.2 Роли портов

В CIST порты имеют все те же роли, что есть в RSTP:

- Root port

Порт с наименьшей стоимостью пути до корневого коммутатора (регионального в MSTI).

- Designated port

Порт , предоставляющий подключенной к нему сети самый дешевый путь до корневого коммутатора (регионального в MSTI).

- Alternate port

Резерв Root port.

- Backup port

Резерв Designated port.

Также в MSTI доступна новая роль - Master port - это порт с наименьшей стоимостью пути из региона до корневого коммутатора CIST.

29.1.3 Балансировка трафика в MSTP

Параметры коммутатора и его портов могут быть изменены для каждого MSTI в отдельности, таким образом трафик разных групп VLAN может быть отправлен по разным путям, распределяя нагрузку по всей сети.

29.2 Конфигурация MSTP

1. Включить spanning-tree и выбрать режим;
2. Сконфигурировать MSTI;
3. Определить параметры региона MSTP;
4. Определить таймеры MSTP;
5. Включить механизмы ускорения сходимости;
6. Выбрать формат MSTP BPDU;
7. Определить параметры порта;
8. Сконфигурировать аутентификацию;
9. Определить метод перестроения spanning-tree.

1. Включение spanning-tree и выбор режима

Команда	Описание

`spanning-tree`
 	
`no spanning-tree`
 	
В режиме глобальной конфигурации
	Включение функции spanning-tree. Команда `no` отключает эту функцию.

`spanning-tree mode {stp|rstp|mstp}` *`no spanning-tree mode`* В режиме глобальной конфигурации	Выбор режима spanning-tree. Команда `no` устанавливает режим по-умолчанию.
`spanning-tree mcheck` В режиме конфигурации порта	Отслеживание режима подключенной сети и переключение на STP при необходимости.

2. Конфигурация MSTI

Команда	Описание

spanning-tree priority <bridge-priority> *no spanning-tree priority* В режиме глобальной конфигурации	Установка приоритета spanning-tree коммутатора. Команда no устанавливает приоритет по-умолчанию.
spanning-tree mst <instance-id> priority <bridge-priority> no spanning-tree mst <instance-id> priority В режиме глобальной конфигурации	Установка приоритета коммутатора для указанного MSTI. Команда no устанавливает приоритет по-умолчанию.

spanning-tree mst <instance-id> cost <cost> *no spanning-tree mst <instance-id> cost* В режиме конфигурации порта	Установка стоимости пути через порт в указанном MSTI. Команда no устанавливает стоимость по-умолчанию.
spanning-tree mst <instance-id> port-priority <port-priority> no spanning-tree mst <instance-id> port-priority В режиме конфигурации порта	Установка приоритета порта spanning-tree в указанном MSTI. Команда no устанавливает приоритет по-умолчанию.
spanning-tree [mst <instance-id>] rootguard no spanning-tree mst <instance-id> rootguard В режиме конфигурации порта	Включение/выключения функционала rootguard для порта spanning-tree в указанном MSTI. Порт с включенным rootguard не может стать root port.
spanning-tree [mst <instance-id>] loopguard no spanning-tree [mst <instance-id>] loopguard	Включение/выключение функционала loopguard для порта spanning-tree в указанном MSTI. Loopguard блокирует петли, возникающие при некорректной разблокировке порта spanning-

В режиме конфигурации порта	tree (например, при отсутствии BPDU от подключенной к порту сети).

3. Определение параметров региона MSTP

Команда	Описание
spanning-tree mst configuration *no spanning-tree mst configuration* В режиме глобальной конфигурации	Переход в режим конфигурации MSTI. Команда с приставкой *no* сбрасывает настройки всех MSTI.
show В режиме конфигурации MSTI	Отображает информацию о текущей конфигурации MSTI.
instance <instance-id> vlan <vlan-list> no instance <instance-id> [vlan <vlan-list>] В режиме конфигурации MSTI	Установка соответствий VLAN-MSTI.
name <name> no name В режиме конфигурации MSTI	Установка имени региона MSTP.
revision-level <level> no revision-level В режиме конфигурации MSTI	Установка уровня ревизии для региона MSTP.
abort В режиме конфигурации MSTI	Выход из режима конфигурации MSTI без сохранения примененной конфигурации.

4. Определение таймеров MSTP

Команда	Описание
spanning-tree forward-time	Установка значения таймера

<time> *no spanning-tree forward-time* В режиме глобальной конфигурации	Bridge_Forward_Delay для коммутатора. Bridge_Forward_Delay - таймер перехода порта из статуса blocking в forwarding.
spanning-tree hello-time <time> *no spanning-tree hello-time* В режиме глобальной конфигурации	Установка значения таймера Bridge_Hello_Time для коммутатора. Bridge_Hello_Time - таймер отправки spanning-tree BPDU.
spanning-tree maxage <time> *no spanning-tree maxage* В режиме глобальной конфигурации	Установка значения таймера Bridge_Max_Age для коммутатора. Bridge_Max_Age - таймер времени жизни лучшего полученного spanning-tree BPDU.
spanning-tree max-hop <hop-count> *no spanning-tree max-hop* В режиме глобальной конфигурации	Установка значения счетчика Max_Hop, который определяет какое количество коммутаторов может пройти BPDU, до того как будет отброшен.

5. Включение механизма ускорения сходимости

Команда	Описание
spanning-tree link-type p2p {auto|force-true|force-false} *no spanning-tree link-type* В режиме конфигурации порта	Выбор механизма определения типа подключенной к порту сети. *auto* - автоматическое определение типа соединения; *force-true* - всегда point-to-point; *force-false* - всегда shared.
spanning-tree portfast [bpdufilter| bpduguard] [recovery <30-3600>] no spanning-tree portfast В режиме конфигурации порта	Включение/выключение механизма portfast определяющего порт spanning-tree как граничный. *bpdufilter* - отбрасывает поступающие на порт BPDU; *bpduguard* - отключает порт при получении BPDU.

6. Выбор формата MSTP BPDU

Команда	Описание
spanning-tree format standard *spanning-tree format privacy* *spanning-tree format auto* *no spanning-tree format* В режиме конфигурации порта	Установка формата BPDU. *standard* - стандарт IEEE; *privacy* - CIsco-совместимый формат; *auto* - автоматическое определение формата по поступающим BPDU.

7. Определение параметров порта

Команда	Описание
spanning-tree cost *no spanning-tree cost* В режиме конфигурации порта	Установка стоимости пути через порт spanning-tree.
spanning-tree port-priority *no spanning-tree port-priority* В режиме конфигурации порта	Установка приоритета порта spanning-tree в указанном MSTI.
spanning-tree rootguard *no spanning-tree rootguard* В режиме конфигурации порта	Включение/выключения функционала rootguard для порта spanning-tree. Порт с включенным rootguard не может стать root port.
spanning-tree transmit-hold-count <tx-hold-count-value> *no spanning-tree transmit-hold-count* В режиме глобальной конфигурации	Установка количества BPDU отправляемых в течение интервала Bridge_Hello_Time.
spanning-tree cost-format {dot1d | dot1t}	Установка формата стоимости пути. *dot1d* - значения в интервале 1-65535;

В режиме глобальной конфигурации	*dot1t* - значения в интервале 1-200000000.

8. Конфигурация аутентификации

Команда	Описание
spanning-tree digest-snooping *no spanning-tree digest-snooping* В режиме конфигурации порта	Включение/выключение аутентификации spanning-tree.

9. Определение метода перестроения spanning-tree

Команда	Описание
spanning-tree tcflush {enable| disable| protect} *no spanning-tree tcflush* В режиме глобальной конфигурации	Установка режима перестроения топологии spanning-tree. *disable* - FDB не сбрасывается при перестроении топологии; *enable* - FDB сбрасывается при перестроении топологии; *protect* - FDB сбрасывается не чаще чем раз в 10 секунд при перестроении топологии.
spanning-tree tcflush {enable| disable| protect} *no spanning-tree tcflush* В режиме конфигурации порта	Установка режима перестроения топологии spanning-tree для порта.

29.3 Пример конфигурации MSTP

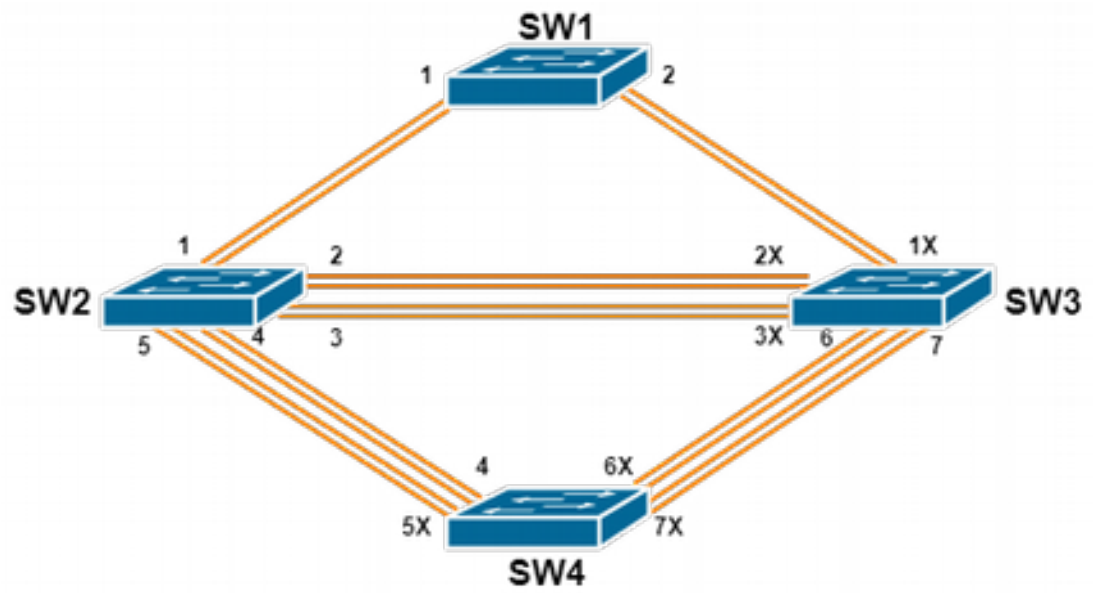


Рисунок 29-2 Пример сети с кольцевой топологией

На всех коммутаторах в сети (Рис. 29-2) включен spanning-tree в режиме MSTP. Все праметры spanning-tree установлены по умолчанию и равны.

По умолчанию MSTP формирует древовидную топологию, растущую из SW1, блокируя избыточные соединения. Порты с пометкой X переведены в состояние blocking, остальные в состоянии forwarding.

Ниже представлена конфигурация коммутаторов по умолчанию.

Имя коммутатора		**SW1**	**SW2**	**SW3**	**SW4**
MAC-адрес коммутатора		…00-00-01	…00-00-02	…00-00-03	…00-00-04
Приоритет коммутатора		32768	32768	32768	32768
Приоритет порта	1	128	128	128	
	2	128	128	128	
	3		128	128	
	4		128		128
	5		128		128
	6			128	128

	7			128	128
Стоимость пути	1	200000	200000	200000	
	2	200000	200000	200000	
	3		200000	200000	
	4		200000		200000
	5		200000		200000
	6			200000	200000
	7			200000	200000

Сконфигурируем сеть:

- Сконфигурируем VLAN:
  - Создадим VLAN 20, 30, 40, 50 на коммутаторах SW2, SW3 и SW4;
  - Переведем порты 1-7 коммутаторов SW2, SW3 и SW4 в режим trunk.
- Сконфигурируем MSTP:
  - Определим коммутаторы SW2, SW3 и SW4 в регион MSTP;
  - Установим соответствие VLAN 20 и 30 - MSTI 3;
  - Установим соответствие VLAN 40 и 50 - MSTI 4.
- Распределим нагрузку, определив корневые коммутаторы для каждого MSTI:
  - Установим приоритет коммутатора SW3 равным 0 в MSTI 3;
  - Установим приоритет коммутатора SW4 равным 0 в MSTI 4;

Конфигурация:

SW2

```
SW2(config)#vlan 20
SW2(Config-Vlan20)#exit
SW2(config)#vlan 30
SW2(Config-Vlan30)#exit
SW2(config)#vlan 40
SW2(Config-Vlan40)#exit
SW2(config)#vlan 50
SW2(Config-Vlan50)#exit
SW2(config)#spanning-tree mst configuration
SW2(Config-Mstp-Region)#name sw2-sw3-sw4
SW2(Config-Mstp-Region)#instance 3 vlan 20;30
SW2(Config-Mstp-Region)#instance 4 vlan 40;50
SW2(Config-Mstp-Region)#exit
SW2(config)#interface e1/0/1-7
SW2(Config-Port-Range)#switchport mode trunk
```

```
SW2(Config-Port-Range)#exit
SW2(config)#spanning-tree
```

SW3

```
SW3(config)#vlan 20
SW3(Config-Vlan20)#exit
SW3(config)#vlan 30
SW3(Config-Vlan30)#exit
SW3(config)#vlan 40
SW3(Config-Vlan40)#exit
SW3(config)#vlan 50
SW3(Config-Vlan50)#exit
SW3(config)#spanning-tree mst configuration
SW3(Config-Mstp-Region)#name sw2-sw3-sw4
SW3(Config-Mstp-Region)#instance 3 vlan 20;30
SW3(Config-Mstp-Region)#instance 4 vlan 40;50
SW3(Config-Mstp-Region)#exit
SW3(config)#interface e1/0/1-7
SW3(Config-Port-Range)#switchport mode trunk
SW3(Config-Port-Range)#exit
SW3(config)#spanning-tree
SW3(config)#spanning-tree mst 3 priority 0
```

SW4

```
SW4(config)#vlan 20
SW4(Config-Vlan20)#exit
SW4(config)#vlan 30
SW4(Config-Vlan30)#exit
SW4(config)#vlan 40
SW4(Config-Vlan40)#exit
SW4(config)#vlan 50
SW4(Config-Vlan50)#exit
SW4(config)#spanning-tree mst configuration
SW4(Config-Mstp-Region)#name sw2-sw3-sw4
SW4(Config-Mstp-Region)#instance 3 vlan 20;30
SW4(Config-Mstp-Region)#instance 4 vlan 40;50
SW4(Config-Mstp-Region)#exit
SW4(config)#interface e1/0/1-7
SW4(Config-Port-Range)#switchport mode trunk
SW4(Config-Port-Range)#exit
SW4(config)#spanning-tree
SW4(config)#spanning-tree mst 4 priority 0
```

После применения описанной конфигурации коммутатор SW1 остается корневым для MST 0 всей сети. В регионе sw2-sw3-sw4 коммутатор SW2 становится региональным корневым для MSTI 0, SW3 - для MSTI 3, SW4 - для MSTI 4.
MSTP генерирует топологии для MSTI 0, MSTI 3, и MSTI 4. Порты с пометкой X переведены в состояние blocking, остальные в состоянии forwarding.

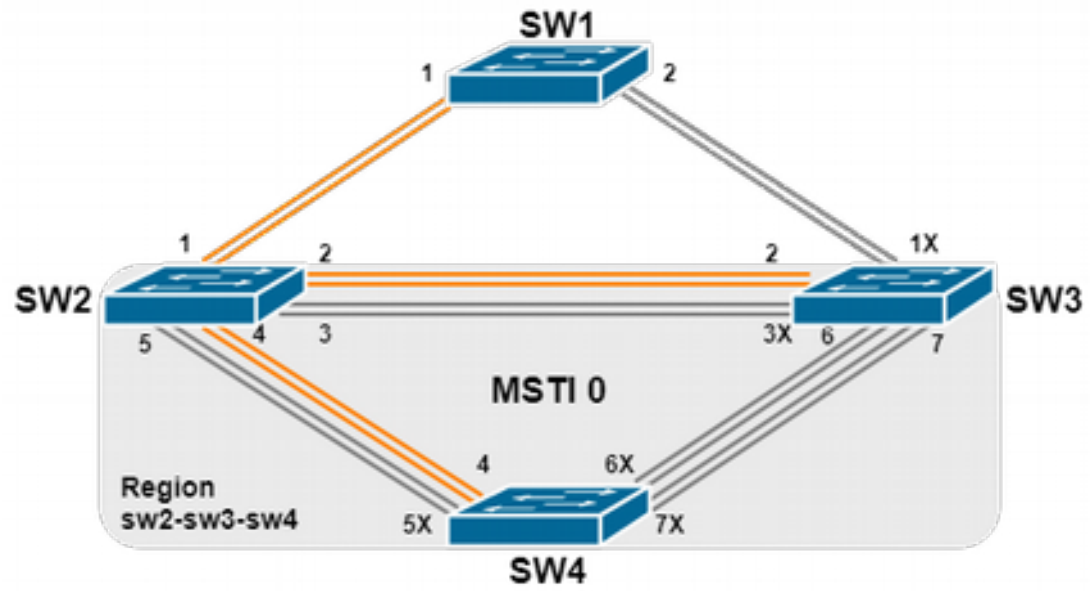


Рисунок 29-3 Топология MSTI 0

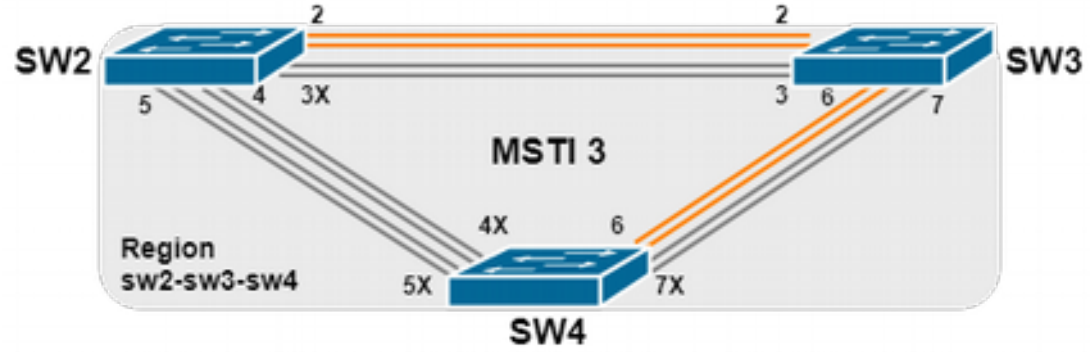


Рис. 29-4 Топология MSTI 3

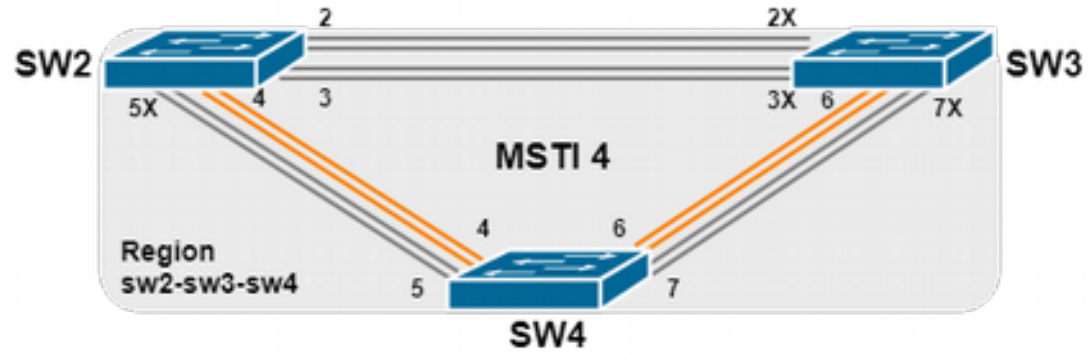


Рисунок 29-5 Топология MSTI 4

29.4. Решение проблем при конфигурации MSTP

- Для включения MSTP на порту, MSTP должен быть включен глобально.
- Параметры MSTP взаимосвязаны и следует соблюдать следующие соответствия, иначе MSTP может работать некорректно:

  2 x (Bridge_Forward_Delay - 1 sec) >= Bridge_Max_Age

  Bridge_Max_Age >= 2 x (Bridge_Hello_Time + 1 sec)
- Нужно всегда помнить, что изменение параметров MSTP может вызвать изменение топологии.

31. Качество сервиса (QoS)

31.1 Общие сведения о QoS

QoS (Quality of Service) - это набор возможностей, которые позволяют логически разделять проходящий по сети трафик на основании критериев и управлять качеством каждого типа трафика, обеспечивая лучший сервис для выбранного трафика. QoS обеспечивает гарантию предсказуемого сервиса передачи данных для выполнения требований программ. QoS не генерирует дополнительную полосу, но обеспечивает более эффективное управление существующей пропускной способностью в соответствии с требованиями приложений и политикой управления сетью.

31.1.1 Термины QoS

QoS: Quality of Service, качество сервиса, обеспечивает гарантию предсказуемого сервиса передачи данных для выполнения требований программ.

Домен QoS: сетевая топология, сформированная устройствами, поддерживающими QoS для обеспечения качества сервиса.

CoS: Class of Service, информация о классификации, передаваемая на 2 уровне модели OSI в подзаголовке 802.1Q заголовка Ethernet-кадра. CoS занимает 3 бита,
поэтому может принимать значения от 0 до 7.

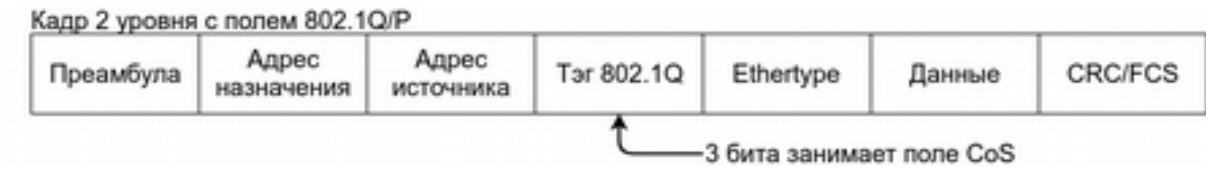


рис. 31-1. поле CoS

ToS: Type of Service, однобайтовое поле в составе заголовка пакета IPv4, используется для обозначения типа сервиса IP-пакетов. Может содержать DSCP и IP-precedence.

рис. 31-2. поле DSCP

IP presedence: информация о классификации, передаваемая в IPv4 заголовке 3 уровня (поле ToS). Занимает 3 бита, поэтому может принимать значения от 0 до 7.

DSCP: Differentiated Services Code Point**,** информация о классификации, передаваемая в IPv4 заголовке 3 уровня (поле ToS). Занимает 6 бит, поэтому может принимать значения от 0 до 63. Поле пересекается с IP Precedence, но совместимо с ним.

Internal Priority: внутренняя настройка приоритета в чипе коммутатора, сокращенно Int-P или IntP.

Classification (классификация): классификация отдельных пакетов в трафике в соответствии с информацией о классификации, передаваемой в заголовке пакета или на основании списков контроля доступа (ACL).

Policing (управление полосой пропускания): действие механизма QoS на входе, которое устанавливает политику для полосы трафика и управляет классифицированными пакетами.

Remark (перемаркировка): действие механизма QoS на входе, выполняющее перемаркировку пакета в соответствии с настроенной политикой.

Scheduling (управление очередями): действие механизма QoS на выходе, которое распределяет трафик по очередям в соответствии с Internal Priority и принимает решение о передаче или сбросе пакетов.

31.1.2 Реализация QoS

Спецификации передачи IP-пакетов охватывают адресацию и сервисы источника и получателя трафика, а также описывают механизм правильной передачи пакетов с использованием протоколов уровня 4 модели OSI (например TCP). В большинстве случаев IP использует максимально возможную пропускную способность вместо механизма защиты полосы пропускания. Это приемлемо для таких сервисов, как электронная почта или FTP, но для постоянно растущих объемов мультимедийных сервисов этот метод не может удовлетворить требования необходимой пропускной способности и низких задержек.
Используя различные методы, QoS определяет приоритет для каждого входящего пакета. Информация о классификации содержится в заголовке IP-пакета 3-го уровня или в заголовке кадра 802.1Q уровня 2. QoS обеспечивает одинаковый сервис для пакетов с одинаковым приоритетом, в то же время для пакетов с разным приоритетом сервис может обеспечиваться разный. Коммутатор или маршрутизатор с поддержкой QoS может обеспечивать различную пропускную способность в соответствии с информацией о классификации, помечать трафик в соответствии с настроенной политикой, а также сбрасывать некоторые пакеты с низким приоритетом в случае нехватки полосы пропускания.

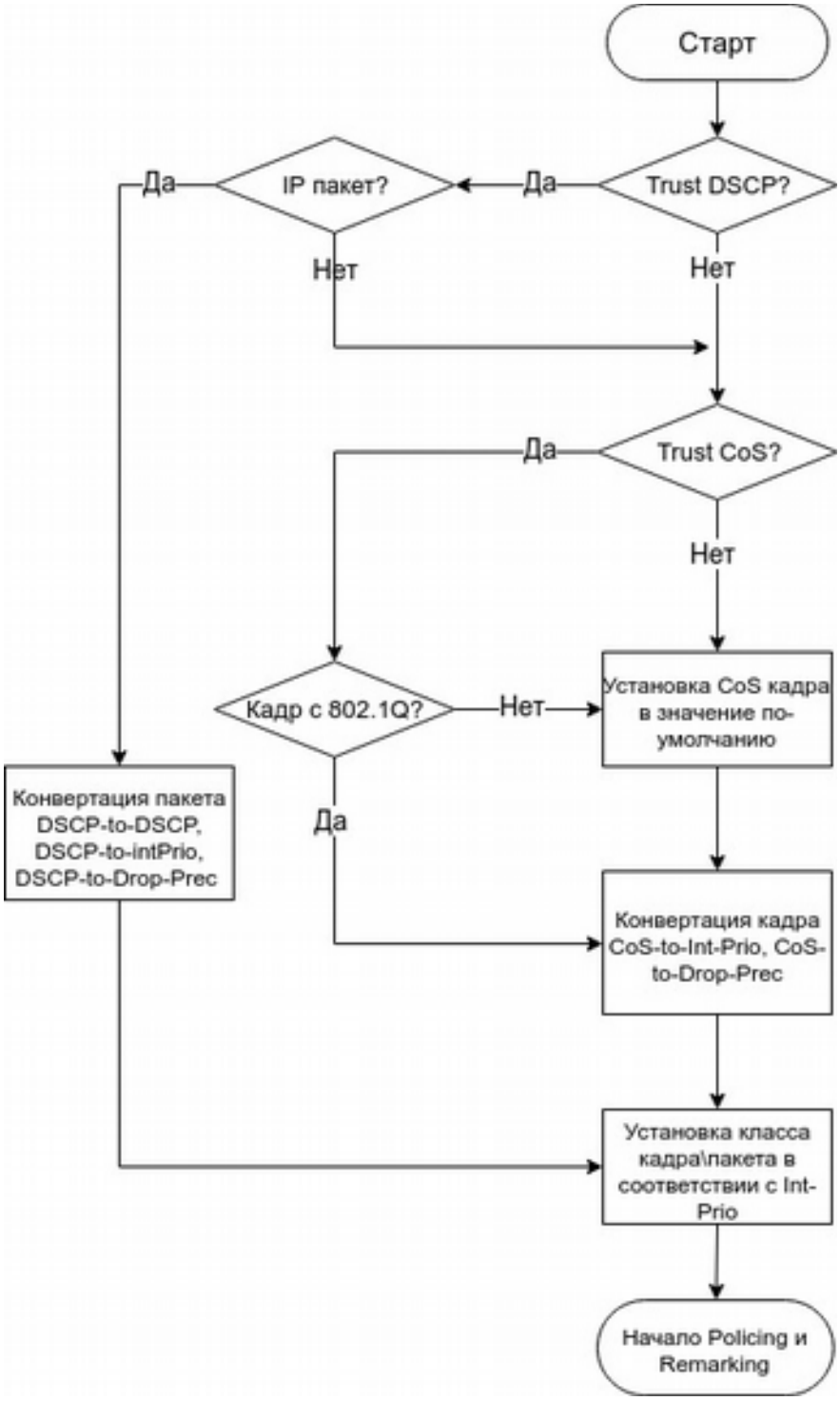
QoS может быть сконфигурирован гибко: степень сложности зависит от топологии сети и глубины анализа трафика.

31.1.3 Базовая модель QoS

Базовая модель QoS состоит из 4 частей: Classification (классификация), Policing (применение политик), Remark (перемаркировка) - действия на входе, Scheduling (планирование) - действие на выходе. **На схеме ниже изображена базовая модель**

QoS.

Classification (классификация): классифицирует трафик в соответствии с классификационной информацией пакетов и генерирует Internal Priority и Приоритет сброса. В зависимости от типов пакетов и настроек коммутатора классификация обеспечивается различным образом. **Схема ниже показывает процесс классификации.**



Policing (управление полосой пропускания) и Remarking (перемаркировка)
Policing может выполняться на потоке данных с целью выделения полосы классифицированному трафику в соответствии с настроенной политикой.
Remarking позволяет заменить оригинальное значение DSCP и CoS кадра.

Работа с очередями и планирование.
Существует значение внутреннего приоритета и приоритета сброса для пакетов

исходящего трафика. Коммутатор назначает пакеты различным очередям в соответствии с внутренними приоритетом, а операция планирования выполняет передачу пакетов в соответствии с весом очереди и приоритетом сброса.

Следующая схема описывает процесс работы с очередями:

31.2 Порядок конфигурации QoS

Настройка карты классов (class map)

Позволяет создать правило на основе ACL, CoS, VLAN ID, IPv4 Precedence, DSCP, IPv6 FL для классификации потока данных. Разные классы потоков данных могут быть применены в разных политиках.

Настройка карты политик (policy map)

Карта политик позволяет связать политики, такие как ограничение полосы, изменение значения DSCP, с картами классов, тем самым применив их к различным потокам данных. Также в карте политик можно применить набор политик для нескольких классов одновременно.

Применение QoS к портам или VLAN

Конфигурирование доверительного режима (trust mode) на порту или привязка политик к

порту. Политики будут задействованы на порту только если они привязаны к нему. Политики могут быть привязаны к VLAN. Не рекомендуется одновременно использовать карту политик на VLAN и на её портах, но если это все-таки будет сделано, приоритет карты политик на порту будет выше.

Конфигурирование алгоритма управления очередями

Настройте алгоритм управления очередью такие как Strict Priority (SP), Weighted round robin (WRR), SP + WRR.

1. Настройка карты классов (class map):

Команда	Описание
`policy burst <burst_group> <normal_burst_kbytes>` в режиме глобальной конфигурации	Настройка разрешенного размера всплесков трафика (burst). Данной моделью коммутатора поддерживается 2 размера burst (`<burst_group>`) Значение по умолчанию `<normal_burst_kbytes>` - 1024 Кбайта. Для возврата к конфигурации по-умолчанию необходимо задать значение `<normal_burst_kbytes>` в 1024 Кбайта.

`class-map <class-map-name>`
 	
`no class-map <class-map-name>`
 	
в режиме глобальной конфигурации
	Создание карты классов с именем `<class-map-name>` и вход в режим конфигурирования этой карты классов.
	
	Удаление карты классов с именем `<class-map-name>`

`match {access-group <acl-index-or-name> | ip dscp <dscp-list>| ip precedence <ip-precedence-list> | ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list>| vlan <vlan-list>| cos <cos-list> }`
`no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan |cos }`
 	
в режиме конфигурирования карты классов
	Настройка критерия соответствия данных карте классов.
	
	Удаление критерия соответствия.

2. Настройка карты политик:

Команда	Описание

`policy-map <policy-map-name>`
 	
`no policy-map <policy-map-name>`
 	
в режиме глобальной конфигурации
	Создание карты политик с именем и вход в режим её конфигурирования `<policy-map-name>`
	
	Удаление карты политик с именем `<policy-map-name>`

`class <class-map-name> [insert-before <class-map-name>]`
 	
`no class <class-map-name>`
 	
в режиме глобальной конфигурации
	Задать для текущей карты политик ассоциацию с картой классов с именем `<class-map-name>`.
	`insert-before <class-map-name>` - позволяет добавить карту классов для ассоциации раньше, чем с именем `<class-map-name>`.
	
	Отменить ассоциацию.

`set {ip dscp <new-dscp> | ip precedence <new-precedence> | internal priority <new-inp> | drop precedence <new-dp> | cos <new-cos> | s-vid <new-vid>}`
 	
`no set {ip dscp | ip precedence | internal priority | drop precedence | cos | s-vid }`
 	
в режиме конфигурирования карты классов в карте политик
	Присвоить классифицированному трафику новое значение dscp (`ip dscp <new-dscp>`), значение ip presedence (`ip precedence <new-precedence>`), значение приоритета сброса (`drop precedence <new-dp>`), значение поля cos (`cos <new-cos>`), внешний тег vlan (`s-vid <new-vid>`)
	
	Отменить присвоение.

`policy <bits_per_second> burst-group <burst-group-id>`
 	
`no policy`
 	
в режиме конфигурирования карты классов в карте политик
	Настроить политику ограничения скорости.
	
	Удалить политику ограничения скорости

`accounting`
 	
`no accounting`
 	
в режиме конфигурирования карты
	Установка функции статистики для трафика, попавшего в class-map.
	
	Отключение функции статистики для трафика, попавшего в class-map.

классов в карте политик	

`drop`
`no drop`
 	
`transmit`
`no transmit`
 	
в режиме конфигурирования карты классов в карте политик
	Выбрать действие сброса, либо передачи для трафика текущего класса.
	Команда `no` отменяет выбранное действие.

3. Применение QoS к портам или VLAN

Команда	Описание

`mls qos trust { cos | dscp}`
 	
`no mls qos trust { cos | dscp}`
 	
в режиме конфигурирования интерфейса
	Доверять меткам CoS и DSCP на порту. По-умолчанию установлено доверие меткам только CoS.
	
	Не доверять меткам CoS и DSCP на порту.

`mls qos cos {<default-cos>}`
 	
`no mls qos cos`
 	
в режиме конфигурирования интерфейса
	Установить значение <default-cos> в качестве CoS для входящего трафика без 802.1q-тэга.
	
	Удалить значение CoS для входящего трафика без 802.1q-тэга.

`service-policy input <policy-map-name>`
 	
`no service-policy input {<policy-map-name>}`
 	
в режиме конфигурирования интерфейса
	Применить карту политик с именем `<policy-map-name>` для входящего трафика на порту
	
	Удалить карту политик с именем `<policy-map-name>` с порта.

`service-policy input <policy-map-name> vlan <vlan-list>`
 	
`no service-policy input {<policy-map-name>} vlan <vlan-list>`
 	
в режиме глобальной конфигурации
	Применить карту политик с именем `<policy-map-name>` для входящего трафика в VLAN `<vlan-list>`
	
	Удалить карту политик с именем `<policy-map-name>` с VLAN `<vlan-list>`.

4. Настройка алгоритмов управления очередями и веса очередей

Команда	Описание

`mls qos queue algorithm {sp | wrr | wdrr }`
`no mls qos queue algorithm`
 	
в режиме глобальной конфигурации
	Устанавливает алгоритм управления очередями.
	По умолчанию используется алгоритм WRR.

`mls qos queue weight <weight0..weight7>`
`no mls qos queue weight`
 	
в режиме глобальной конфигурации
	Устанавливает вес очередей на порту.
	По умолчанию вес очередей 1 2 3 4 5 6 7 8.

`mls qos queue wdrr weight <weight0..weight7>`
`no mls qos queue wdrr weight`
 	
в режиме глобальной конфигурации
	Устанавливает вес очередей на порту для алгоритма WDRR.
	По-умолчанию вес очередей 10 20 40 80 160 320 640 1280

5. Настройка карты преобразования QoS

Команда	Описание

`mls qos map {cos-intp <intp1…intp8> | cos-dp<dp1…dp8> | dscp-intp <in-dscp list> to <intp> | dscp-dp <in-dscp list> to <dp> | dscp-dscp <in-dscp list> to <out-dscp>}`
 	
`no mls qos map {cos-intp | cos-dp | dscp-intp | dscp-dp | dscp-dscp}`
 	
в режиме глобальной конфигурации
	Задать преобразование приоритетов QoS из COS в INTP (cos-) или из DSCP в INTP (dscp-intp)

6. Очистка счетчиков данных в карте политик на определенном порту или VLAN

Команда	Описание
`clear mls qos statistics [interface <interface-name> | vlan <vlan-id>]`	Очистка счетчиков данных в карте политик. `<interface-name>` - имя порта;

в привилегированном режиме	<vlan-id> - имя vlan

7. Просмотр конфигурации QoS

Команда	Описание
show mls qos maps [cos-intp | dscp-intp | dscp-dp | dscp-dsc] в привилегированном режиме	Отображение конфигурации карты преобразований.
show class-map [<class-map-name>] в привилегированном режиме	Отображение информации о конфигурации карты классов
show policy-map [<policy-map-name>] в привилегированном режиме	Отображение информации о карте политик
show mls qos {interface [<interface-id>] [policy | queuing] | vlan <vlan-id>} в привилегированном режиме	отображение информации о конфигурации QoS на порту

31.3 Пример конфигурации QoS

Пример 1:

Включить функцию QoS, изменить вес исходящих очередей на порту на 1:1:2:2:4:4:8:8, включить доверие к меткам CoS и установить значение CoS 5 по-умолчанию для входящего трафика без метки 802.1q.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch#config
Switch(config-If-Ethernet1/0/1)#mls qos queue wrr weight 1 1 2 2 4 4 8
8
Switch(Config-If-Ethernet1/0/1)#mls qos cos 5
```

Результат настройки:

Когда кадр с меткой 802.1q и значением CoS пройдет через порт, знначения CoS от 0 до 7 распределятся следующим образом в исходящие очереди 1,2,3,4,5,6,7,8 по порядку соответственно. Если на порт придет кадр без метки 802.1q, он будет определен по-умолчанию в очередь 6, соответствующую CoS 5.

Пример 2:

Установить на порту ethernet1/0/2 для пакетов из сегмента 192.168.1.0/24 полосу в 10 Мбит/с с величиной всплеска 4Мбайта.

Конфигурация будет выглядеть следующим образом:

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch (config)#policy burst 1 4000
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)#exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#policy 10000 burst-group 1
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#service-policy input p1
```

Пример 3:

Как показано на рис 8.1, внутри блока QoS-домен, Switch1 классифицирует различный трафик, задавая ему различные значения IP precedence. Например, установка значения CoS 5 для пакетов из сегмента 192.168.1.0/24 на порту ethernet 1/0/1. Порт Switch1 в сторону Switch2 настроен как trunk. Порт ethernet1/0/1 коммутатора Switch2 настроен для доверия меткам CoS. Таким образом, внутри домена QoS пакеты разных приоритетов будут поступать в разные очереди и получать разную пропускную способность.

Конфигурация будет выглядеть следующим образом:

QoS configuration in Switch1:

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)#exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 5
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/0/1
```

```
Switch(Config-If-Ethernet1/0/1)#service-policy input p1
```

QoS configuration in Switch2:

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mls qos trust cos
```

31.4 Решение проблем при настройке QoS

- Доверие меткам CoS или DSCP может использоваться одновременно с доверием другим меткам или картами политик как для IPv4, так и для IPv6 трафика;
- При одновременном доверии меткам CoS и DSCP, приоритет DSCP выше;
- Если сконфигурирован динамический VLAN (mac vlan/голосовой vlan/vlan подсети IP/vlan протокола), тогда значение CoS для пакета равно значению CoS для динамического VLAN;
- Карта политик (policy-map) может быть применена только на входящее направление трафика;
- Не рекомендуется применять карту политик (policy-map) к VLAN и к порту, который относится к этой же VLAN одновременно;
- Действия карты политик “set cos”, “set dscp” и “set ip-presedence” являются взаимоисключающими и не могут использоваться в одно и то же время.

32. Перенаправление трафика на основе потока

32.1 Общие сведения о перенаправлении трафика на основе потока

Функция перенаправления трафика на основе потока позволяет коммутатору передавать кадры данных, удовлетворяющие определенным условиям (обозначенным в ACL), на указанный порт. Кадры данных, удовлетворяющие одному и тому же условию, называются **классом потока**, входящий порт для кадров данных называется **портом источника перенаправления**, а указанный выходной порт называется **портом назначения перенаправления**.

Существует 2 типа применения перенаправления на основе потока:

1. Для мониторинга и управления сетью, а также диагностики проблем в сети: подключение порту назначения перенаправления анализатора трафика (снифера) или устройств мониторинга;
2. Специальная политика передачи для специального типа кадров данных.

Коммутатор может выбрать только один порт назначения перенаправления для одного и того же класса потока в порту источника перенаправления. В то же время он может назначать разные порты назначения перенаправления для разных классов потоков в порту источника перенаправления. Один и тот же класс потока может применяться к различным портам источника перенаправления.

32.2 Конфигурация перенаправления трафика на основе потока

1. Конфигурирование перенаправления трафика на основе потока;
2. Проверка текущей конфигурации

1. Конфигурирование перенаправления трафика на основе потока;

Команда	Описание

`access-group <aclname> redirect to interface [ethernet <IFNAME>| <IFNAME>]`
 	
`no access-group <aclname> redirect`
 	
в режиме конфигурирования интерфейса
	Применить ACL `<aclname>` в качестве класса потока для перенаправления трафика на порту источника перенаправления. В качестве порта назначения перенаправления указывается интерфейс после `redirect to interface`.
	
	Удалить настройку перенаправления трафика на основе потока.

2. Проверка текущей конфигурации

Команда	Описание

`show flow-based-redirect {interface [ethernet <IFNAME> | <IFNAME>]}` в привилегированном режиме	Отобразить информацию о текущей конфигурации перенаправления трафика на основе потока.

32.3 Пример конфигурации перенаправления трафика на основе потока

Необходимо реализовать запрос пользователя: перенаправить кадры данных с IP источника 192.168.1.111 из порта 1 в порт 6.

Шаги конфигурации:

1. Создать ACL, под который будут попадать кадры данных с IP источника 192.168.1.111
2. Применить ACL на порту источника для перенаправления трафика.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#access-list 1 permit host 192.168.1.111
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# access-group 1 redirect to interface
ethernet 1/0/6
```

32.4 Решение проблем с перенаправлением трафика на основе потока

- Только следующие типы ACL поддерживаются: именованный standard IP ACL, именованный extended IP ACL, нумерованный standard IP ACL, нумерованный extended IP ACL, именованный standard MAC ACL, именованный extended MAC ACL, нумерованный standard MAC ACL, нумерованный extended MAC ACL, нумерованный IPv6 ACL и нумерованный standard IPv6 ACL;
- Параметры Timerange и Portrange не могут быть установлены в ACL;
- Тип ACL должен быть настроен как Permit;
- Порт источника перенаправления не может быть портом назначения перенаправления одновременно.

33. Интерфейс управления уровня 3

33.1 Общие сведения об интерфейсе управления уровня 3

Коммутатор поддерживает только L2-коммутацию, но имеет возможность настройки функций L3 для связи IP-протоколов управления.

Рекомендуется создавать на коммутаторе для управления только один L3-интерфейс. Интерфейс уровня 3 является не физическим, а логическим интерфейсом на основе VLAN и может содержать один или несколько L2 портов, принадлежащих к это VLAN, или не содержать L2 портов. Чтобы интерфейс уровня 3 был в состоянии UP, необходимо, чтобы как минимум один порт уровня 2, принадлежащий к этому интерфейсу, был в состоянии UP, иначе интерфейс уровня 3 находится в состоянии DOWN. Коммутатор может использовать IP-адреса настроенные на интерфейсе уровня 3 для связи с другими устройствами через IP-протокол.

33.2 Настройка интерфейса уровня 3

1. Создать интерфейс управления 3 уровня;
2. Настроить описание интерфейса VLAN.

1. Создать интерфейс управления 3 уровня;

Команда	Описание

`interface vlan <vlan-id>`
 	
`no interface vlan <vlan-id>`
 	
В режиме глобальной конфигурации
	Создать VLAN-интерфейс управления.
	
	Удалить созданный VLAN-интерфейс управления.

2. Настроить описание интерфейса VLAN.

Команда	Описание

`description <text>`
 	
`no description`
 	
В режиме конфигурирования interface vlan
	Назначить описание VLAN-интерфейсу управления
	
	Удалить описание VLAN-интерфейса управления

34. Конфигурация протокола IP

34.1 Общая информация о IPv4 и IPv6

IPv4 - текущая версия глобального универсального Интернет-протокола. Практика показывает, что является IPv4 простым, гибким, открытым, стабильным, простым в реализации, а также обладает хорошей совместимостью с протоколами других уровней. Не смотря на то, что протокол не подвергался серьезным изменениям с момента его выхода в 1980-х, он имеет широкое распространение по всему миру вместе с Интернет. Однако, инфраструктура сети Интернет и сервисов Интернет-приложений продолжает расти высокими темпами, и IPv4 демонстрирует свои недостатки, столкнувшись с текущим масштабом и сложностью этой сети.

IPv6 - это следующее поколение Интернет-протокола, созданная IETF для замены IPv4. IPv6 разработан в том числе и для решения проблемы нехватки адресов сети Интернет, препятствующую дальнейшему её развитию.

Наиболее важная проблема, решаемая IPv6 - гораздо больший, по сравнению с IPv4 объем адресов. Запас свободных блоков IPv4-адресов исчерпан, в то время как количество пользователей сети Интернет продолжает расти. Растет и число устройств, требующих выход в Интернет. В результате этого требуется все большее количество IPv4-адресов, предоставлять которые становится все более затруднительно. Работа по преодолению нехватки IPv4 адресов велась долгое время, были предложены некоторые технологии, позволяющие продлить жизнь IPv4 инфраструктуры, такие как NAT (Network Address Translation) и CIDR (Classless Inter-Domain Routing) и т.д. Эти технологии в совокупности хоть и позволяют смягчить проблему нехватки IPv4 адресов, но в то же время они порождают ряд других проблем, которые также необходимо решать. Таким образом, на сегодняшний день, единственным возможным решением, учитывающим большинство проблем, существующих в IPv4, становится переход на следующее поколение - IPv6.

Протокол IPv6 не только сохранил, но и улучшил поддержку функционала IPv4. Прежде всего, 128-битная схема адресации протокола IPv6 обеспечивает достаточное число глобально уникальных IP-адресов для текущей потребности узлов глобальной IP-сети с большим запасом для дальнейшего роста (в 296 раз, по сравнению с IPv4), что позволяет отказаться от механизма трансляции адресов. Иерархическая схема адресации облегчает агрегирование маршрутов, эффективно снижает количество записей в таблице маршрутизации, увеличивает эффективность маршрутизации и обработки пакетов данных.

IPv6 сохранил и расширил поддержку существующих протоколов маршрутизации (RIPng, OSPFv3, IS-ISv6, MBGP4+ и т.д.). Расширен функционал Multicast - он полностью заменил функционал broadcast IPv4.

Глобально уникальный IPv6 адрес может быть получен конечным устройством автоматически как через DHCPv6, так и через без него, с помощью NDP. Эти функции автоматической настройки адреса делают процесс смены адресов в существующей сети проще и удобнее. В то же время IPv6 осуществляет поддержку и Mobile IP protocol.

Дизайн заголовка IPv6 более совершенен, чем у IPv4: заголовок содержит меньше полей данных и не включает поле контрольной суммы, что увеличивает скорость

обработки заголовка IPv6. В заголовке IPv6 поле фрагментации может быть передано как дополнительное необязательное поле. Протокол предполагает, что конечные IPv6-узлы выполняют Path MTU Discovery для определения максимально допустимого размера отправляемых пакетов, и протокол более высокого уровня ограничит размер пакета. В заголовок IPv6 могут быть интегрированы расширенные поля IPSec, которые обеспечат сервисы безопасности “end-to-end”, такие как контроль доступа, конфиденциальность и целостность данных, что делает реализацию шифрования, проверки подлинности и VPN проще.

34.2 Конфигурация протокола IPv4

1. Настроить IPv4 адрес на интерфейсе уровня 3;
2. Задать шлюз по-умолчанию.

1. Настроить IPv4 адрес на интерфейсе уровня 3;

Команда	Описание

`ip address <ip-address> <mask> [secondary]`
 	
`no ip address [<ip-address> <mask>]`
 	
В режиме конфигурирования interface vlan
	Назначить IP-адрес VLAN-интерфейсу
	
	Удалить назначенный IP-адрес VLAN-интерфейса

2. Задать шлюз по-умолчанию.

Команда	Описание

`ip default-gateway <A.B.C.D>`
 	
`no ip default-gateway <A.B.C.D>`
 	
В режиме глобальной конфигурации
	Задать шлюз по-умолчанию для коммутатора
	
	Удалить шлюз по-умолчанию из конфигурации

34.3 Конфигурация адреса IPv6

1. Базовая конфигурация IPv6:
    a. Настроить адрес IPv6 для VLAN-интерфейса;
    b. Задать шлюз по-умолчанию:
2. Настройка IPv6 ND (Neighbor Discovery)

a. Настройка количества сообщений DAD neighbor solicitation;
b. Настройка интервала отправки сообщений DAD neighbor solicitation;
c. Настройка статических записей IPv6-neighbor;
d. Удаление всех динамических записей в таблице IPv6 neighbor.

1. Базовая конфигурация IPv6:
   a. Настроить адрес IPv6 для VLAN-интерфейса;

Команда	Описание
`ipv6 address <ipv6-address/prefix-length> [eui-64]`	Настройка IPv6 адреса, включая объединенные глобальные unicast адреса, site-local адреса и link-local адреса
`no ipv6 address <ipv6-address/prefix-length>`	Удалить ipv6 адрес `<ipv6-address/prefix-length>` из конфигурации
В режиме конфигурации интерфейса	

   b. Задать шлюз по-умолчанию:

Команда	Описание
`ipv6 default-gateway <X:X::X:X>`	Задать шлюз по-умолчанию для коммутатора
`no ipv6 default-gateway <X:X::X:X>`	Удалить шлюз по-умолчанию из конфигурации
В режиме глобальной конфигурации	

2. Настройка IPv6 ND (Neighbor Discovery)
   a. Настройка количества сообщений DAD neighbor solicitation;

Команда	Описание
`ipv6 nd dad attempts <value>`	Настройка количества сообщений, отправляемых последовательно при обнаружении интерфейсом дублировать ipv6 адреса.
`no ipv6 nd dad attempts`	Восстановить значение по-умолчанию (значение по-умолчанию - **1**).
В режиме глобальной конфигурации	

b. Настройка интервала отправки сообщений DAD neighbor solicitation;

Команда	Описание

`ipv6 nd ns-interval <seconds>`
 	
`no ipv6 nd ns-interval`
 	
В режиме конфигурации интерфейса
	Задать интервал отправки запросов соседям (в секундах).
	
	Восстановить значение по-умолчанию (1 секунда)

c. Настройка статических записей IPv6-neighbor;

Команда	Описание

`ipv6 neighbor <ipv6-address> <hardware-address> interface <interface-type interface-name>`
 	
`no ipv6 neighbor <ipv6-address>`
 	
В режиме конфигурации интерфейса
	Создать статическую запись для соседа. Запись содержит IPv6 адрес соседа `<ipv6-address>`, его MAC-адрес `<hardware-address>` и порт 2 уровня `<interface-type interface-name>`.
	
	Создать статическую запись для соседа с IPv6 адресом `<ipv6-address>`

d. Удаление всех динамических записей в таблице IPv6 neighbor.

Команда	Описание
`clear ipv6 neighbors` В привилегированном режиме	Удаление всех динамических записей в таблице IPv6-соседей. Команда не удаляет статические записи.

34.5 Решение проблем IPv6

- Если подключенный ПК не получает IPv6 адрес, проверьте RA анонсирование на коммутаторе.

35. ARP

35.1 Общая информация о ARP

ARP (Address Resolution Protocol, Протокол Обнаружения Адресов) - в основном используется для определения IP адреса по Ethernet MAC-адресу. Коммутатор поддерживает статическое добавление записей в ARP-таблицу.

35.2 Конфигурация ARP

Статическое добавление записи в ARP-таблицу

Команда	Описание
`arp <ip_address> <mac_address>`	Добавление статической ARP-записи на интерфейсе.
`no arp <ip_address>`	Удаление статической ARP-записи на интерфейсе.
В режиме конфигурирования интерфейса	

35.3 Решение проблем с ARP

Если icmp пинг от коммутатора до непосредственно подключенного к нему сетевого устройства не успешен, проверьте следующие моменты:

- Проверьте, изучил ли коммутатор ARP
- Если записи в таблице ARP нет, включите отладку ARP (debug arp) и просмотрите условия приема/отправки ARP-пакетов
- Проверьте физическую составляющую соединения

36. Функция предотвращения ARP-сканирования

36.1 Общие сведения о функции предотвращения ARP-сканирования

Сканирование ARP это один из методов сетевой атаки. С целью обнаружения всех активных хостов в сегменте сети, источник атаки будет отправлять большое количество ARP-сообщений. Такая рассылка может занять большую часть пропускной способности сети, что само по себе может привести к проблемам в сети из-за исчерпания пропускной способности. Но обычно сканирование ARP это лишь подготовка к атакам с использованием уязвимостей найденных активных хостов.

Поскольку ARP сканирование угрожает безопасности и стабильности сети, его важно предотвратить. Коммутатор предоставляет полное решение для предотвращения сканирования ARP: если будет обнаружен хост или порт с признаками сканирования ARP, коммутатор отключить источник атаки для обеспечения безопасности сети.

Существует два метода предотвращения сканирования ARP: на основе портов и на основе IP. Метод на основе портов считает количество сообщений ARP, полученных с порта за определенный период, а если число превысит установленный порог - коммутатор выключит порт. Метод на основе IP считает считает количество ARP-сообщений, полученных от IP адреса в за определенный период времени, трафик от этого IP будет заблокирован. Оба метода предотвращения сканирования ARP можно использовать одновременно: после того как порт был заблокирован, он может быть восстановлен если настроена функция автоматического восстановления; после того, как IP был заблокирован, он может быть восстановлен, когда скорость принятых ARP-пакетов будет ниже уровня настроенного порога.

Для оптимизации нагрузки на коммутатор и эффективной настройки функционала, существует возможность задать доверенные порты и IP, сообщения ARP от которых не будут проверены коммутатором.

36.2 Настройка функции предотвращения ARP-сканирования

1. Включение функции предотвращения ARP-сканирования;
2. Настройка порогов на основе портов и на основе IP;
3. Настройка доверенных портов;
4. Настройка доверенных IP;
5. Настройка времени автоматического восстановления;
6. Просмотр информации, логирование и отладка.

1. Включение функции предотвращения ARP-сканирования:

Команда	Описание
`anti-arpscan enable`	Включение функции предотвращения ARP-сканирования
`no anti-arpscan enable`	Выключение функции предотвращения ARP-сканирования

В режиме глобальной конфигурации	

2. Настройка порогов на основе портов и на основе IP:

Команда	Описание

`anti-arpscan port-based threshold <threshold-value>`
 	
`no anti-arpscan port-based threshold`
 	
В режиме глобальной конфигурации
	Установить порог (от 2 до 200 пакетов в секунду) на основе порта
	
	Восстановить значение по-умолчанию (10 пакетов в секунду)

`anti-arpscan ip-based threshold <threshold-value>`
 	
`no anti-arpscan ip-based threshold`
 	
В режиме глобальной конфигурации
	Установить порог (от 1 до 200 пакетов в секунду) на основе IP
	
	Восстановить значение по-умолчанию (3 пакета в секунду)

3. Настройка доверенных портов:

Команда	Описание

`anti-arpscan trust {port | supertrust-port | iptrust-port}`
 	
`no anti-arpscan trust {port | supertrust-port | iptrust-port}`
 	
В режиме конфигурации интерфейса
	Установить режим доверия. `port` - режим доверия для порта, но не для IP; `supertrust-port` - режим доверия для IP и порта одновременно; `iptrust-port` - режим доверия для IP, но не для порта.
	
	Отменить режим доверия.

4. Настройка доверенных IP:

Команда	Описание
`anti-arpscan trust ip <ip-`	Задать доверенный IP `<ip-address>`

address> [<netmask>] no anti-arpscan trust ip <ip-address> [<netmask>] В режиме глобальной конфигурации	Удалить доверенный IP <ip-address>

5. Настройка времени автоматического восстановления:

Команда	Описание
anti-arpscan recovery enable no anti-arpscan recovery enable В режиме глобальной конфигурации	Включить функцию автоматического восстановления после блокировки. Выключить функцию автоматического восстановления после блокировки.
anti-arpscan recovery time <seconds> no anti-arpscan recovery time В режиме глобальной конфигурации	Задать время в секундах, по истечении которого IP или порт будет восстановлен после блокировки автоматически Восстановить значения по-умолчанию (300 секунд)

6. Просмотр информации, логирование и отладка:

Команда	Описание
anti-arpscan log enable no anti-arpscan log enable В режиме глобальной конфигурации	Включение логирования событий функции предотвращения сканирования ARP Выключение логирования событий функции предотвращения сканирования ARP
anti-arpscan trap enable no anti-arpscan trap enable В режиме глобальной конфигурации	Включение отправки SNMP-trap о событиях функции предотвращения сканирования ARP Выключение отправки SNMP-trap о событиях функции предотвращения сканирования ARP

`show anti-arpscan [trust {ip | port | supertrust-port | iptrust-port} | prohibited {ip | port}]` В привилегированном режиме	Просмотр информации доверенных (`trust`) и заблокированных (`prohibited`) портов и IP

`debug anti-arpscan [port | ip]`
 	
`no debug anti-arpscan [port | ip]`
 	
В привилегированном режиме
	Включение вывода отладки на основе порта или IP
	
	Выключение вывода отладки на основе порта или IP

36.3 Пример конфигурации функции предотвращения ARP-сканирования

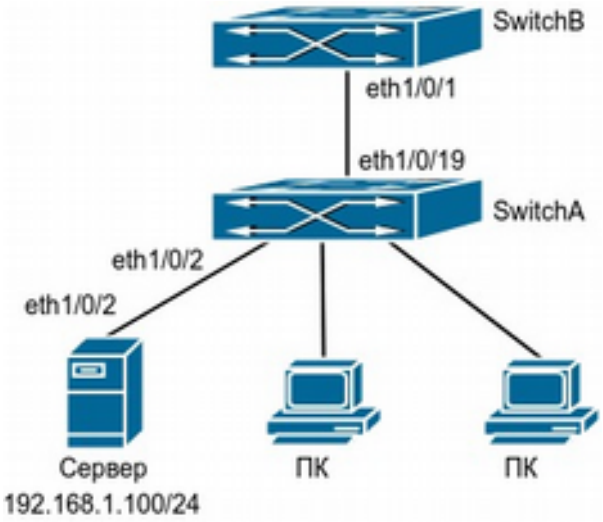


Рис. 36-1 Пример топологии применения функции предотвращения ARP-сканирования

В сетевой топологии на рисунке выше порт eth1/0/1 коммутатора SwitchB подключен к порту eth1/0/19 коммутатора SwitchA. Порт eth1/0/2 коммутатора SwitchA подключен к файловому серверу (IP-адрес 192.168.1.100/24), а все остальные порты коммутатора SwitchA подключены к ПК пользователей.

Следующая конфигурация может эффективно предотвратить сканирование ARP без ущерба нормальной работе сети:

`SwitchA:`

```
SwitchA(config)#anti-arpscan enable
SwitchA(config)#anti-arpscan recovery time 3600
SwitchA(config)#anti-arpscan trust ip 192.168.1.100 255.255.255.0
```

```
SwitchA(config)#interface ethernet1/0/2
SwitchA (Config-If-Ethernet1/0/2)#anti-arpscan trust port
SwitchA (Config-If-Ethernet1/0/2)#exit
SwitchA(config)#interface ethernet1/0/19
SwitchA (Config-If-Ethernet1/0/19)#anti-arpscan trust supertrust-port
Switch A(Config-If-Ethernet1/0/19)#exit
```

SwitchB:

```
Switch B(config)# anti-arpscan enable
SwitchB(config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)#anti-arpscan trust port
SwitchB(Config-If-Ethernet1/0/1)exit
```

36.3 Решение проблем при использовании функции предотвращения ARP-сканирования

- Функция предотвращения ARP-сканирования выключена по-умолчанию. После включения функции воспользуйтесь командой “**debug anti-arpscan**” для отладки.

37. Предотвращение подделки ARP (ARP Spoofing)

37.1 Общие сведения о ARP Spoofing

Протокол ARP отвечает за сопоставление IP-адреса с MAC-адресом. Весь процесс сопоставления заключается в том, что хост отправляет пакет, содержащий информацию о требуемом IP-адресе, широковещательно. Другой хост, которому принадлежит требуемый IP-адрес, отправляет в ответ пакет, содержащий свой IP-адрес и MAC-адрес. Таким образом два хоста могут обмениваться информацией друг с другом на основе MAC-адреса.

Для сокращения количества ARP-пакетов в сети, протокол ARP спроектирован таким образом, что даже если хост не запрашивал ARP другого хоста, при получении такого пакета он внесет запись в свою таблицу. Поэтому существует возможность подделки ARP-пакета (ARP Spoofing). Когда злоумышленник хочет перехватить трафик между двумя хостами, он отправляет ARP-ответы на оба этих хоста по отдельности, заставляя их принимать свой MAC-адрес за MAC-адреса друг-друга. Таким образом трафик от одного хоста к другом фактически будет передаваться через хост злоумышленника, что позволяет ему не только прочитать необходимую информацию, но и модифицировать пакеты данных на свое усмотрение для последующей передачи.

37.1.1 Отключение обновления без запроса (arp-security)

Основным методом предотвращения ARP Spoofing в сетях является отключение на коммутаторе возможность автоматического обновления ARP. После этого злоумышленник не сможет изменить MAC-адрес в ARP-таблице. В то же время это не прерывает функцию автоматического обучения ARP. Таким образом, это в значительной степени предотвращает возможность подмены ARP.

37.1.2 ARP Guard

Существует также вероятность подмены злоумышленником адреса шлюза или коммутатора - в этом случае кроме перехвата трафика данных, существует также опасность отказа всей сети из-за передачи трафика не по назначению. Для предотвращения подмены адреса шлюза, возможно использовать функцию ARP Guard. При получении на порт ARP-ответа с source адресом, указанным в ARP-Guard, это пакет будет расценен как вредоносный и отброшен.

37.1.3 Рассылка ARP коммутатором без запроса (Gratuitous ARP)

Еще одним из способов предотвращения подмены ARP коммутатора (или шлюза) является периодическая рассылка коммутатором ARP-ответов без запроса (функция Gratuitous ARP). С одной стороны это позволяет предотвратить акату, так как хосты периодически будут обновлять свои ARP-таблицы и вероятность подмены будет низка. С другой стороны это позволит уменьшить количество исходящего трафика от хостов, так как не будет необходимости отправлять ARP-запрос шлюзу для обновления ARP-таблицы.

37.2 Настройка функции предотвращения ARP Spoofing

1. Отключить автоматическое обновления ARP;
2. Отключить автоматическое обучение ARP;
3. Конвертировать динамические ARP в статические;
4. Настроить защищенный IP-адрес для arp-guard;
5. Настроить Gratuitous ARP;
6. Просмотреть конфигурацию Gratuitous ARP.

1. Отключить автоматическое обновления ARP:

Команда	Описание

`ip arp-security updateprotect`
 	
`no ip arp-security updateprotect`
 	
В режиме глобальной конфигурации и в режиме конфигурирования интерфейса
	Выключить автоматическое обновление ARP
	
	Включить автоматическое обновление ARP

2. Отключить автоматическое обучение ARP:

Команда	Описание

`ip arp-security learnprotect`
 	
`no ip arp-security learnprotect`
 	
В режиме глобальной конфигурации и в режиме конфигурирования интерфейса
	Выключить автоматическое обучение ARP
	Включить автоматическое обучение ARP

3. Конвертировать динамические ARP в статические:

Команда	Описание
`ip arp-security convert` В режиме глобальной конфигурации и в режиме конфигурирования интерфейса	Конвертировать динамические ARP в статические ARP

4. Настроить защищенный IP-адрес для arp-guard

Команда	Описание
`arp-guard ip <addr>`	Добавить ARP Guard адрес

`no arp-guard ip <addr>` В режиме конфигурирования интерфейса	Удалить ARP Guard адрес

5. Настроить Gratuitous ARP.

Команда	Описание

`ip gratuituous-arp <5-200>`
 	
`no ip gratuituous-arp`
 	
В режиме глобальной конфигурации или в режиме конфигурирования интерфейса
	Включить функцию gratuitious ARP и задать интервал отправки сообщений ARP `<5-200>` в секундах.
	
	Отключить функцию gratuitious ARP

6. Просмотреть конфигурацию Gratuitous ARP.

Команда	Описание
`show ip gratuituous-arp [interface vlan <1-4094>]` в привилегированном режиме	Добавить ARP-Guard адрес Удалить ARP-Guard адрес

37.3 Пример использования функции предотвращения ARP Spoofing

Рис. 37-1 Пример топологии для использования функции предотвращения ARP spoofing.

Оборудование	Конфигурация	Кол-во
Коммутатор	IP:192.168.2.4; mac: 00-00-00-00-00-04	1

Хост A	IP:192.168.2.1; mac: 00-00-00-00-00-01	2
Хост B	IP:192.168.1.2; mac: 00-00-00-00-00-02	3
Хост C	IP:192.168.2.3; mac: 00-00-00-00-00-03	несколько

На рисунке 37-1 связь установлена между хостами B и C. Хост A хочет, чтобы коммутатор направлял ему пакеты, отправленные хостом B. В первую очередь Хост A отправляет пакет ARP-ответа на коммутатор в формате 192.168.2.3, 00-00-00-00-00-01, сопоставляя его MAC-адрес с IP-адресом хоста C. Коммутатор обновляет таблицу ARP и начинает отправлять пакеты для 192.168.2.3 на MAC-адрес 00-00-00-00-00-01 (адрес хоста A).

В дальнейшем хост A пересылает принятые пакеты хосту C, заменив адрес источника и адрес назначения. Так как ARP таблица обновляется, хост A должен непрерывно отправлять ARP-ответы с подмененным адресом на коммутатор.

Поэтому необходимо настроить запрещение изучения ARP в стабильной сети, а затем заменить динамические ARP-записи на статические. В результате выученные ARP не будут обновляться и будут защищены.

```
Switch#config
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#arp 192.168.2.1 00-00-00-00-00-01
interface ethernet 1/0/1
Switch(config-if-vlan1)#arp 192.168.2.2 00-00-00-00-00-02
interface ethernet 1/0/2
Switch(config-if-vlan1)#arp 192.168.2.3 00-00-00-00-00-03
interface ethernet 1/0/3
Switch(Config-If-Vlan3)#exit
Switch(Config)#ip arp-security learnprotect
Switch(Config)#
Switch(config)#ip arp-security convert
```

Если топология и конфигурация сети меняется, необходимо запретить обновления ARP: как только запись в ARP таблицу будет добавлена, она не может быть обновлена новым ARP-ответом.

```
Switch#config
Switch(config)#ip arp-security updateprotect
```

Для защиты от подмены адреса коммутатора необходимо настроить ARP Guard и Gratuitous ARP:

```
Switch#config
Switch(config)#int eth 1/0/1-3
Switch(config-if-port-range)#arp-guard ip 192.168.2.4
```

```
Switch(config-if-port-range)#exit
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip gratuitous-arp 5
```

38. Функция контроля динамических ARP (Dynamic ARP Inspection)

38.1 Общие сведения о Dynamic ARP Inspection

Функция контроля динамических ARP (Dynamic ARP Inspection или DAI) - это функция безопасности, которая позволяет проверять пакеты ARP в сети. Через DAI администратор может перехватывать, записывать и отбрасывать пакеты ARP, которые имеют неверный MAC-адрес или IP-адрес.

DAI позволяет проверить легитимность пакетов ARP в соответствии с легитимными IP и MAC-адресами, содержащимися в доверенной базе данных. Эта база может быть создана динамически, с помощью мониторинга DHCP. Если пакет ARP получен из доверенного для DAI порта, коммутатор пересылает его напрямую, без проверки. Если пакет ARP получен из порта, который не является доверенным, коммутатор передаст только легитимный пакет, нелегитимные пакеты коммутатор будет отбрасывать и записывать это действие.

38.2 Настройка Dynamic ARP Inspection

1. Включить DAI на VLAN;
2. Задать доверенный порт;
3. Настроить допустимую скорость ARP с портов.

1. Включить DAI на VLAN;

Команда	Описание
`ip arp inspection vlan <vlan-id>`	Включить DAI на основе VLAN `<vlan-id>`
`no ip arp inspection vlan <vlan-id>`	Выключить DAI на основе VLAN `<vlan-id>`
В режиме глобальной конфигурации	

2. Задать доверенный порт;

Команда	Описание
`ip arp inspection trust`	Настроить порт как доверенный порт для DAI
`no ip arp inspection trust`	Настроить порт как недоверенный порт для DAI (по-умолчанию)
В режиме конфигурации порта	

3. Настроить допустимую скорость ARP с портов.

Команда	Описание
`ip arp inspection limit-rate <rate>`	Настроить лимит ARP-сообщений в секунду для порта
`no ip arp inspection limit-rate <rate>`	Удалить лимит ARP-сообщений (по-умолчанию)
В режиме конфигурации порта	

38.3 Пример использования Dynamic ARP Inspection

DHCP-сервер и ПК пользователя принадлежат VLAN 10. MAC-адрес DHCP-сервера 00-24-8c-01-05-90, IP адрес 192.168.10.2 настроен статически, DHCP-сервер подключен к интерфейсу eth1/0/1 коммутатора. MAC-адрес другого сервера 00-24-8c-01-05-80, IP адрес 192.168.10.2 настроен статически, сервер подключен к интерфейсу eth1/0/2 коммутатора. MAC-адрес ПК пользователя 00-24-8c-01-05-96, IP адрес назначается динамически через DHCP, ПК подключен к интерфейсу eth1/0/3 коммутатора. Интерфейс 3 уровня VLAN 10 имеет адрес 192.168.10.1, MAC адрес f8-f0-82-10-00-01. Конфигурация коммутатора выглядит следующим образом:

```
ip arp inspection vlan 10
ip dhcp snooping enable
ip dhcp snooping vlan 10
!
Interface Ethernet1/0/1
description connect DHCP Server
switchport access vlan 10
ip dhcp snooping trust
ip arp inspection limit-rate 50
ip arp inspection trust
!
Interface Ethernet1/0/2
description connect to Other Server
switchport access vlan 10
ip arp inspection limit-rate 50
!
Interface Ethernet1/0/3
description connect to PC
switchport access vlan 10
ip arp inspection limit-rate 50
!
```

```
interface Vlan10
ip address 192.168.10.1 255.255.255.0
```

В этом случае коммутатор будет перехватывать сообщения ARP со всех портов, кроме eth1/0/1, который настроен как доверенный. Каждый раз при получении сообщения ARP, функционал DAI сравнит данные в сообщении с записью в базе, сформированной в процессе мониторинга DHCP. После того, как запись была добавлена, хост может настроить статически тот адрес, который был получен динамически. Но в случае с сервером, имеющим статический адрес и подключенном к eth1/0/2, такая запись, создана не будет и ARP-ответы пропускаться не будут.

39. Конфигурация DHCP

39.1 Общие сведения о DHCP

DHCP (RFC2131) - сокращение от Dynamic Host Configuration Protocol (Протокол Динамической Конфигурации Узла). DHCP позволяет динамически назначить IP-адрес, а также передать хосту другие параметры сетевой конфигурации, такие как маршрут по-умолчанию, DNS-сервер, местоположение файла образа прошивки и другие.

DHCP - имеет архитектуру “клиент-сервер”. DHCP-клиент запрашивает сетевой адрес и другие параметры у DHCP-сервера, сервер предоставляет сетевой адрес и параметры конфигурации клиентам. Если DHCP-сервер и DHCP-клиент находятся в разных подсетях, для перенаправления пакетов может быть настроен DHCP-relay.

В общем случае процесс предоставления адреса и других данных по DHCP выглядит следующим образом:

1. DHCP клиент отправляет широковещательный запрос DHCPDISCOVER;
2. При получении DHCPDISCOVER пакета DHCP сервер отправляет DHCP клиенту DHCPOFFER пакет, содержащий назначаемый IP-адрес и другие параметры;
3. DHCP клиент отправляет широковещательный DHCPREQUEST;
4. DHCP сервер отправляет пакет DHCPACK клиенту и клиент получает IP-адрес и другие параметры;

Вышеуказанные четыре этапа завершают процесс динамического назначения параметров. Однако, если DHCP сервер и DHCP клиент не находятся в одной сети, сервер не сможет получить широковещательные пакеты, отправленные DHCP клиентом. Для пересылки таких пакетов используется DHCP-relay, который перенаправит широковещательные пакеты от DHCP-клиента серверу как unicast.

Коммутаторы SNR могут быть настроены в качестве DHCP сервера, DHCP relay, а также получать параметры динамически в качестве DHCP-клиента.

39.2 Конфигурация DHCP-сервера

1. Включить\выключить DHCP service;
2. Настроить пул DHCP-адресов:
    a. Создать\удалить:
    b. Настроить передаваемые параметры;
    c. Настроить привязку IP адреса к MAC;
3. Включить логирование конфликта IP-адресов;

1. Включить\выключить DHCP service;

Команда	Описание
`service dhcp`	Включить сервисы DHCP (server, relay)

`no service dhcp` В режиме глобальной конфигурации	Выключить сервисы DHCP (по умолчанию)

`ip dhcp disable`
 	
`no ip dhcp disable`
 	
В режиме конфигурации интерфейса
	Выключить сервисы DHCP на интерфейсе
	
	Включить сервисы DHCP на интерфейсе (по умолчанию)

2. Настроить пул DHCP-адресов:
   a. Создать\удалить:

Команда	Описание

`ip dhcp pool <name>`
 	
`no ip dhcp pool <name>`
 	
В режиме глобальной конфигурации
	Создать пул адресов для DHCP-сервера и войти в режим его конфигурирования.
	
	Удалить пул адресов для DHCP-сервера

   b. Настроить передаваемые параметры;

Команда	Описание

`network-address <network-number> [mask | prefix-length]`
 	
`no network-address`
 	
В режиме конфигурирования DHCP pool
	Добавить область адресов в текущий DHCP pool
	
	Удалить область адресов из текущего DHCP pool

`default-router [<address1>[<address2>[… <address8>]]]`
 	
`no default-router`
 	
В режиме конфигурирования DHCP pool
	Задать один или несколько (до 8 одновременно) шлюзов по-умолчанию. Чем раньше задан адрес, тем выше приоритет он будет иметь.
	
	Удалить адрес шлюза по-умолчанию.

`dns-server [<address1>[<address2>[…`	Задать один или несколько (до 8 одновременно) DNS-адресов. Чем раньше

`<address8>]]]`
 	
`no dns-server`
 	
В режиме конфигурирования DHCP pool
	задан адрес, тем выше приоритет он будет иметь.
	
	Удалить адрес DNS-сервера

`domain-name <domain>`
 	
`no domain-name`
 	
В режиме конфигурирования DHCP pool
	Задать доменное имя
	
	Удалить доменное имя

`netbios-name-server [<address1>[<address2>[… <address8>]]]`
 	
`no netbios-name-server`
 	
В режиме конфигурирования DHCP pool
	Задать один или несколько (до 8 одновременно) адресов WINS-серверов.
	
	Удалить адрес WINS-сервера

`netbios-node-type {b-node|h-node| m-node|p-node|<type-number>}`
 	
`no netbios-node-type`
 	
В режиме конфигурирования DHCP pool
	Задать WINS node-type.
	
	Удалить параметр WINS node-type.

`bootfile <filename>`
 	
`no bootfile`
 	
В режиме конфигурирования DHCP pool
	Задать загрузочный файл
	
	Удалить загрузочный файл

`next-server [<address1>[<address2>[… <address8>]]]`
 	
`no next-server [<address1>[<address2>[… <address8>]]]`
 	
В режиме конфигурирования DHCP pool
	Задать IP-адрес сервера, на котором хратится `bootfile`
	
	Удалить IP-адрес сервера, на котором хратится `bootfile`

`option <code> {ascii <string> | hex <hex> | ipaddress <ipaddress>}`	Настройка параметра `{ascii <string> | hex <hex> | ipaddress <ipaddress>}`, определенного кодом опции `<code>`.

`no option <code>` В режиме конфигурирования DHCP pool	Удалить параметр, определенный кодом опции `<code>`

`lease { days [hours][minutes] | infinite }`
 	
`no lease`
 	
В режиме конфигурирования DHCP pool
	Задать время аренды адреса, `infinite` - постоянное использование
	
	Вернуть значение по-умолчанию (1 day)

`max-lease-time {[<days>] [<hours>] [<minutes>] | infinite}`
 	
`no max-lease-time`
 	
В режиме конфигурирования DHCP pool
	Задать максимальное время аренды адреса, `infinite` - постоянное использование
	
	Вернуть значение по-умолчанию (1 day)

`ip dhcp excluded-address <low-address> [<high-address>]`
 	
`no ip dhcp excluded-address <low-address> [<high-address>]`
 	
В режиме глобальной конфигурации
	Задать диапазон IP-адресов из dhcp pool, который будет исключен из динамического назначения. `<low-address>` - начало диапазона, `<high-address>` - конец диапазона
	
	Удалить диапазон адресов

c. Настроить привязку IP адреса к MAC;

Команда	Описание

`hardware-address <hardware-address> [{Ethernet | IEEE802| <type-number>}]`
 	
`no hardware-address`
 	
В режиме конфигурирования DHCP pool
	Задать аппаратный адрес для фиксированного назначения адреса
	
	Удалить аппаратный адрес для фиксированного назначения адреса

`host <address> [<mask>|<prefix-length>]`	Задать IP-адрес, который будет назначен на заданный `hardware-address` Удалить IP-адрес, который будет назначен на

`no host` В режиме конфигурирования DHCP pool	заданный `hardware-address`

`client-identifier <unique-identifier>`
 	
`no client-identifier`
 	
В режиме конфигурирования DHCP pool
	Задать уникальный ID пользователя
	
	Удалить уникальный ID пользователя

3. Включить логирование конфликта IP-адресов;

Команда	Описание

`ip dhcp conflict logging`
 	
`no ip dhcp conflict logging`
 	
В режиме глобальной конфигурации
	Включить/выключить логирование при обнаружении конфликта адресов, выданных по DHCP

`clear ip dhcp conflict <address | all>` В привилегированном режиме	Удалить одну `<address>` или все `<all>` записи обнаруженных конфликтов адресов

39.3 DHCP-relay

Когда DHCP-клиент и DHCP-сервер находятся в разных сегментах сети, транслировать пакеты может DHCP relay. В результате внедрения DHCP-relay, один DHCP-сервер может использоваться для разных сегментов сети, что не только экономически эффективно, но и удобно в администрировании.

DHCP-клиент, как обычно, выполняет диалог с DHCP-сервером, но в процесс добавляется DHCP-relay. Он перехватывает пакеты от DHCP-клиента и перенаправляет их на заданный адрес DHCP-сервера как unicast, принимает пакеты от DHCP-сервера и перенаправляет их DHCP-клиенту, которому они предназначались.

Настройка DHCP-relay

1. Включить\выключить DHCP service;
2. Настройка DHCP-relay для перенаправления пакетов;
3. Настройка VLAN источника и назначения перенаправления.

1. Включить\выключить DHCP service;

Команда	Описание

`service dhcp`
 	
`no service dhcp`
 	
В режиме глобальной конфигурации
	Включить сервисы DHCP (server, relay)
	
	Выключить сервисы DHCP (по умолчанию)

2. Настройка DHCP-relay для перенаправления пакетов;

Команда	Описание

`ip forward-protocol udp bootps`
 	
`no ip forward-protocol udp bootps`
 	
В режиме глобальной конфигурации
	Включить пересылку `bootps` пакетов
	
	Выключить пересылку `bootps` пакетов

`ip helper-address <ipaddress>`
 	
`no ip helper-address <ipaddress>`
 	
В режиме конфигурации Interface Vlan
	Задать адрес DHCP сервера.
	
	Удалить адрес DHCP сервера.

3. Настройка VLAN источника и назначения перенаправления.

Для использования DHCP-relay на коммутаторе необходимо создать интерфейс уровня 3 для VLAN, которая будет использоваться в качестве share-vlan. Одновременно с этим необходимо включить

Команда	Описание

`ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>`
 	
`no dhcp relay share-vlan`
	Задать соответствие VLAN источника (`sub-vlan <vlanlist>`) и назначения `share-vlan <vlanid>` перенаправления
	
	Удалить соответствие VLAN источника и назначения перенаправления

В режиме глобальной конфигурации	

39.4 Пример конфигурации DHCP

Сценарий 1:

Чтобы упростить настройку и администрирование, компания использует коммутатор в качестве DHCP-сервера. IP-адрес VLAN управления - 10.16.1.2/16. Сеть компании разделена между сетями A и B по местоположению офис. Конфигурация сети A и B показана в таблице ниже:

	Pool A (сеть 10.16.1.0)	Pool B (сеть 10.16.2.0)
Шлюз по-умолчанию	10.16.1.200 10.16.1.201	
DNS сервер	10.16.1.202	
WWW сервер	нет	10.16.1.209
WINS сервер	10.16.1.209	нет
WINS тип ноды	H-node	нет
Время аренды	3 дня	1 день

В сети A IP адрес 10.16.1.210 фиксированно задан для назначения устройству, имеющему MAC-адрес 00-03-22-23-dc-ab.

```
Switch(config)#service dhcp
Switch(config)#interface vlan 1
Switch(Config-Vlan-1)#ip address 10.16.1.2 255.255.0.0
Switch(Config-Vlan-1)#exit
Switch(config)#ip dhcp pool A
Switch(dhcp-A-config)#network 10.16.1.0 24
Switch(dhcp-A-config)#lease 3
Switch(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201
Switch(dhcp-A-config)#dns-server 10.16.1.202
Switch(dhcp-A-config)#netbios-name-server 10.16.1.209
Switch(dhcp-A-config)#netbios-node-type H-node
Switch(dhcp-A-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.1.200 10.16.1.201
Switch(config)#ip dhcp pool B
Switch(dhcp-B-config)#network 10.16.2.0 24
Switch(dhcp-B-config)#lease 1
Switch(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201
Switch(dhcp-B-config)#dns-server 10.16.2.202
```

```
Switch(dhcp-B-config)#option 72 ip 10.16.2.209
Switch(dhcp-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.2.200 10.16.2.201
Switch(config)#ip dhcp pool A1
Switch(dhcp-A1-config)#host 10.16.1.210
Switch(dhcp-A1-config)#hardware-address 00-03-22-23-dc-ab
Switch(dhcp-A1-config)#exit
```

Использование: Когда DHCP/BOOTP клиент подключается к порту коммутатора с VLAN 1, он может получить адрес только из сети 10.16.1.0/24 вместо 10.16.2.0/24. Причина в том, что клиент может широковещательно запрашивать IP-адрес только в сегменте VLAN-интерфейса. Если клиент хочет получить адрес в сети 10.16.2.0/24, шлюз, пересылающий широковещательные пакеты клиента, должен принадлежать сети 10.16.2.0/24, должна быть обеспечена связность между шлюзом и коммутатором.

Сценарий 2:

Коммутатор Switch настроен как DHCP-relay, DHCP-клиент подключен к интерфейсу 1/0/2, DHCP-сервер подключен к интерфейсу 1/0/3. Конфигурация выглядит следующим образом:

```
Switch(config)#service dhcp
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#vlan 2
Switch(Config-Vlan-2)#exit
Switch(config)#interface Ethernet 1/0/2
Switch(Config-Ethernet1/0/2)#switchport access vlan 2
Switch(Config-Ethernet1/0/2)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#ip forward-protocol udp bootps
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip help-address 10.1.1.10
Switch(Config-if-Vlan1)#exit
```

Рекомендуется использовать комбинацию команд “`ip forward-protocol udp bootps`” и “`ip help-address <ip-address>`”. Команда “`ip help-address <ip-address>`” может быть настроена только на интерфейсах уровня 3.

Сценарий 3:

ПК1 и DHCP-сервер подключены к разным портам одного коммутатора Switch1. На ПК1 работает DHCP-клиент, получающий адрес от DHCP-сервера. Switch1 - коммутатор уровня 2, на нем настроены функции DHCP-relay и option 82, Ethernet 1/0/2 - настроен в режим access с vlan 3, Ethernet 1/0/3 настроен в trunk. DHCP сервер имеет адрес

192.168.10.199. На коммутаторе Switch1 создан interface vlan 1 и настроен IP-адрес 192.168.40.50, настроен адрес для перенаправления DHCP - 192.168.10.199. VLan 3 настроен как sub-vlan для vlan 1.

Конфигурация Switch1 выглядит следующим образом:

```
Switch1(config)#vlan 1
Switch1(config)#vlan 3
Switch1(config)#interface ethernet 1/0/2
Switch1(Config-If-Ethernet1/0/2)#switchport access vlan 3
Switch1(config)#interface ethernet 1/0/3
Switch1(Config-If-Ethernet1/0/2)#switchport mode trunk
Switch1(config)#service dhcp
Switch1(config)#ip forward-protocol udp bootps
Switch1(config)#ip dhcp relay information option
Switch1(config)#ip dhcp relay share-vlan 1 sub-vlan 3
Switch1(config)#interface vlan 1
Switch1(config-if-vlan1)#ip address 192.168.40.50 255.255.255.0
Switch1(config-if-vlan1)#ip helper-address 192.168.40.199
```

39.5 Решение проблем при настройке DHCP

Если DHCP-клиент не может получить IP адрес и другие сетевые параметры, после проверки кабеля и клиентского оборудования следует выполнить следующее:

- Проверьте, запущен ли DHCP-сервер;
- Если DHCP клиент и DHCP сервер находятся не в одной сети и не имеют прямой l2-связности, проверьте, настроена ли на коммутаторе, отвечающем за пересылку пакетов, функция DHCP-relay;
- Проверьте, имеет ли DHCP-сервер адресный пул в том же сегменте, что и адрес interface vlan коммутатора, перенаправляющего DHCP-пакеты;
- На данном коммутаторе адресный пул может быть настроен либо как динамический, командой “network-address” , либо как статический, командой “host”. Привязка только одного адреса может быть настроена в каждом пуле. Если необходимо настроить несколько адресов для ручной привязки, необходимо создать отдельный DHCP-pool для каждой привязки.

40. DHCP snooping

40.1 Общие сведения о DHCP snooping

С помощью DHCP snooping коммутатор контролирует процесс получения DHCP-клиентом IP-адреса для предотвращения атак DHCP и появления нелегитимных DHCP-серверов в сети, устанавливая доверенные и недоверенные порты. Сообщения из доверенных портов передаются коммутатором без проверки. Обычно, доверенные порты используются для подключения DHCP-сервера или DHCP relay, а недоверенные - для подключения DHCP-клиентов. Коммутатор передает сообщения DHCP-запросов из недоверенных портов, но не передает DHCP-ответы. КРоме того, при получении DHCP-ответа из недоверенного порта, коммутатор может выполнить предварительно настроенное действие: shutdown или blackhole. Если включена функция DHCP Snooping Binding, то после каждого успешного получения IP адреса через DHCP коммутатор создаст запись в таблице, которая свяжет полученный IP-адрес с MAC-адресом DHCP-клиента, номером его VLAN и порта. С помощью этой информации можно реализовать контроль доступа пользователей.

40.2 Настройка DHCP snooping

1. Включить DHCP Snooping;
2. Включить DHCP Snooping Binding;
3. Задать адрес DHCP сервера;
4. Настроить доверенные порты;
5. Включить функцию привязки DHCP Snooping binding к пользователю;
6. Добавить запись DHCP Snooping binding вручную;
7. Задать действие при получении DHCP-ответа из недоверенного порта;
8. Задать лимит скорости передачи сообщений DHCP;
9. Отладочная информация;

1. Включить DHCP Snooping

Команда	Описание

`ip dhcp snooping enable`
 	
`no ip dhcp snooping enable`
 	
В режиме глобальной конфигурации
	Включить функцию DHCP snooping
	
	Выключить функцию DHCP snooping

`ip dhcp snooping vlan <vlan_id>`
 	
`no ip dhcp snooping vlan <vlan_id>`
	Включить функцию функцию DHCP snooping для VLAN `<vlan_id>`
	
	Выключить функцию функцию DHCP

В режиме глобальной конфигурации	snooping для VLAN `<vlan_id>`

2. Включить DHCP Snooping Binding

Команда	Описание
`ip dhcp snooping binding enable`	Включить функцию DHCP snooping binding
`no ip dhcp snooping binding enable`	Выключить функцию DHCP snooping binding
В режиме глобальной конфигурации	

3. Задать адрес DHCP сервера

Команда	Описание
`ip user helper-address A.B.C.D [port <udpport>] source <ipAddr> (secondary|)`	Задать адрес DHCP сервера для пользователя
`no ip user helper-address (secondary|)`	Удалить адрес DHCP сервера для пользователя
В режиме глобальной конфигурации	

4. Настроить доверенные порты

Команда	Описание
`ip dhcp snooping trust`	Назначить порт в качестве доверенного
`no ip dhcp snooping trust`	Назначить порт в качестве недоверенного (по-умолчанию)
В режиме глобальной конфигурации	

5. Включить функцию привязки DHCP Snooping binding к пользователю

Команда	Описание
`ip dhcp snooping binding user-control [vlan] [max-`	Включить функцию привязки пользователя к IP-адресу, VLAN текущему порту и VLAN,

user]	vlan - включить функцию во VLAN, max-user - задать максимальное количество пользователей. Для работы функционала обязательно указание параметров vlan и max-user.
no ip dhcp snooping binding user-control [vlan] [max-user] В режиме конфигурирования интерфейса	Выключить функцию привязки пользователя к IP-адресу, VLAN текущему порту и VLAN

6. Добавить запись DHCP Snooping binding вручную

Команда	Описание
ip dhcp snooping binding user <mac> address <ipAddr> interface (ethernet|) <ifname>	Добавить статическую запись в таблицу DHCP Snooping binding
no ip dhcp snooping binding user <mac> interface (ethernet|) <ifname> В режиме глобальной конфигурации	Удалить статическую запись в таблицу DHCP Snooping binding

7. Задать действие при получении DHCP-ответа из недоверенного порта

Команда	Описание
ip dhcp snooping action {shutdown|blackhole} [recovery <second>]	Задать действие при получении DHCP-ответа из недоверенного порта: shutdown - выключить порт, blackhole - отбросить кадры с MAC источника, с которым были получены DHCP-ответы. recovery - время восстановления в секундах <second>.
no ip dhcp snooping action В режиме конфигурирования	Удалить действие при получении DHCP-ответа из недоверенного порта (по умолчанию)

интерфейса	

8. Задать лимит скорости передачи сообщений DHCP

Команда	Описание

`ip dhcp snooping limit-rate <pps>`
 	
`no ip dhcp snooping limit-rate`
 	
В режиме глобальной конфигурации
	Задать лимит скорости передачи сообщений DHCP от 0 до 100 pps.
	
	Удалить лимит скорости передачи сообщений DHCP (по-умолчанию)

9. Просмотр записей в таблице DHCP snooping binding

Команда	Описание
`show ip dhcp snooping binding all` В привилегированном режиме	Отобразить все записи в таблице DHCP snooping binding

10. Отладочная информация

Команда	Описание

`debug ip dhcp snooping packet`
`debug ip dhcp snooping event`
`debug ip dhcp snooping update`
`debug ip dhcp snooping binding`
 	
В привилегированном режиме
	Отобразить отладочную информацию

40.3 Пример настройки DHCP snooping

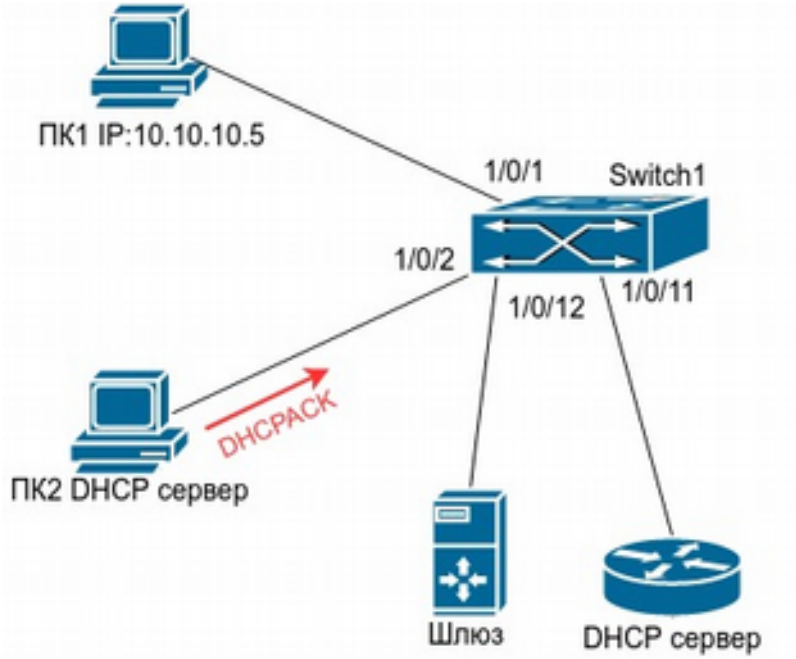


Рисунок 40.1 Настройка DHCP snooping

Как показано на рисунке 40.1, ПК1 подключен к недоверенному порту 1/0/1 коммутатора Switch1 и получает конфигурацию через DHCP, IP-адрес клиента 10.10.10.5. DHCP-сервер и шлюз подключены к портам коммутатора 1/0/11 и 1/0/12 соответственно, настроенным как доверенные. Злоумышленник ПК2, подключенный к недоверенному порту 1/0/2 пытается подделать DHCP-сервер, посылая ложные DHCPACK. Функция DHCP snooping эффективно обнаружит и заблокирует такой тип атаки.

Конфигурация коммутатора Switch1:

```
Switch1(config)#ip dhcp snooping enable
Switch1(config)#interface ethernet 1/0/11
Switch1(Config-Ethernet1/0/11)#ip dhcp snooping trust
Switch1(Config-Ethernet1/0/11)#exit
Switch1(config)#interface ethernet 1/0/12
Switch1(Config-Ethernet1/0/12)#ip dhcp snooping trust
Switch1(Config-Ethernet1/0/12)#exit
Switch1(config)#interface ethernet 1/0/1-2
Switch1(Config-Port-Range)#ip dhcp snooping action shutdown
```

40.4 Решение проблем с конфигурацией DHCP snooping

- Проверьте, включен ли DHCP-snooping;
- Если порт не реагирует на ложные DHCP сообщения, проверьте, настроен ли этот порт как недоверенный.

41. DHCPv6

41.1 Общие сведения о DHCPv6

DHCPv6 [RFC3315] - версия протокола DHCP для работы с IPv6. Этот протокол назначает как IPv6 адреса, так и другие параметры настройки сети, такие, как адрес DNS или доменное имя. DHCPv6 может назначать IPv6 адреса через relay (ретранслятор). DHCPv6 сервер также может обеспечить сервис DHCPv6 без состояния отслеживания (SLAAC), при котором клиенту могут быть назначены параметры конфигурации, такие как адрес DNS-сервера и доменное имя без назначения IPv6-адреса.

В протоколе DHCPv6 предусмотрены три объекта: клиент, relay (ретранслятор) и сервер. Протокол DHCPv6 основан на протоколе UDP. Клиент DHCPv6 отправляет сообщения запроса конфигурации DHCP-серверу или DHCP-relay на порт UDP 547, в ответ сервер или relay DHCPv6 отправляют сообщения на порт UDP 546. Клиент DHCPv6 отправляет сообщения solicit и request DHCP-серверу или relay на multicast-адрес - ff02::1:2.

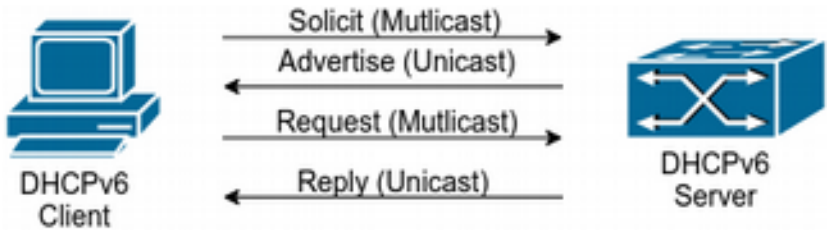


рис. 41-1 процесс согласования DHCPv6

Когда DHCPv6 клиент пытается запросить ipv6 адрес и другую конфигурацию, сначала клиент должен найти DHCPv6-сервер, а только после этого запросить конфигурацию.

1. В момент обнаружения сервера, DHCP клиент пытается найти DHCPv6 сервер, рассылая SOLICIT сообщения, содержащее собственный идентификатор DUID, на мультикаст-адрес FF02::1:2;
2. Каждый DHCPv6-сервер, получивший SOLICIT, ответит клиенту сообщением ADVERTISE (предложение), которое содержит идентификатор DUID сервера и его приоритет;
3. Возможно, что клиент получить несколько сообщений ADVERTISE. В этом случае клиент должен выбрать один сервер и ответить ему сообщение REQUEST, чтобы запросить предложенный им адрес;
4. Выбранный DHCPv6-сервер подтверждает клиенту IPv6 адрес и другие параметры в сообщении REPLY.

Вышеуказанные четыре этапа завершают процесс динамического назначения параметров. Однако, если DHCPv6 сервер и DHCPv6 клиент не находятся в одной сети, сервер не сможет получить multicast-пакеты от клиента и ответить ему. Для пересылки таких пакетов используется DHCPv6-relay, функции которого реализованы на коммутаторе. Когда DHCPv6-relay получает сообщение от DHCPv6 клиента, он инкапсулирует его в пакет Relay-forward и доставляет следующему DHCPv6-relay или

серверу.

Для делегирования IPv6 префиксов DHCPv6 сервер настраивается на маршрутизаторе провайдера (PE), а DHCPv6-клиент настраивается на маршрутизаторе клиента (CPE). Маршрутизатор клиента шлет маршрутизатору провайдера запрос на выделение префикса адресов и получает предварительно настроенный префикс. Затем CPE маршрутизатор делит выделенный префикс на /64 подсети. Эти префиксы будут анонсированы сообщениями объявления маршрутизатора (RA) хостам.

41.2 Настройка DHCPv6-сервера

1. Включить\выключить сервис DHCPv6;
2. Настроить адресный пул DHCPv6:
    a. Создать\удалить адресный пул;
    b. Настроить параметры адресного пула;
3. Включить функцию DHCPv6 сервера на порту;

1. Включить\выключить сервис DHCPv6;

Команда	Описание

`service dhcpv6`
 	
`no service dhcpv6`
 	
В режиме глобальной конфигурации
	Включить сервисы DHCPv6 (server, relay)
	
	Выключить сервисы DHCPv6 (по умолчанию)

2. Настроить адресный пул DHCPv6:
    a. Создать\удалить адресный пул;

Команда	Описание

`ipv6 dhcp pool <poolname>`
 	
`no ipv6 dhcp pool <poolname>`
 	
В режиме глобальной конфигурации
	Создать адресный пул DHCPv6
	
	Удалить адресный пул DHCPv6

    b. Настроить параметры адресного пула;

Команда	Описание
`network-address <ipv6-pool-start-address> {<ipv6-pool-end-address> | <prefix-length>} [eui-64]`	Задать диапазон адресов, назначаемых пулом от `<ipv6-pool-start-address>` до `<ipv6-pool-`

	`end-address>` с длиной префикса `<prefix-length>`. Если длина префикса 64 бита, адрес может быть выделен по стандарту EUI-64 `[eui-64]`
`no network-address` В режиме конфигурации адресного пула DHCPv6	Удалить диапазон адресов, назначаемых пулом

`dns-server <ipv6-address>`
 	
`no dns-server <ipv6-address>`
 	
В режиме конфигурации адресного пула DHCPv6
	Задать адрес DNS-сервера
	
	Удалить адрес DNS-сервера

`domain-name <domain-name>`
 	
`no domain-name <domain-name>`
 	
В режиме конфигурации адресного пула DHCPv6
	Задать доменное имя
	
	Удалить доменное имя

`excluded-address <ipv6-address>`
 	
`no excluded-address <ipv6-address>`
 	
В режиме конфигурации адресного пула DHCPv6
	Исключить адрес из пула.
	
	Удалить исключение.

`lifetime {<valid-time> | infinity} {<preferred-time> | infinity}`
 	
`no lifetime`
 	
В режиме конфигурации адресного пула DHCPv6
	Задать время аренды адреса `<valid-time>` и `<preferred-time>` в секундах, `infinity` - устанавливает неограниченное время.
	
	Восстановить значения по умолчанию: preffered-time 2592000 секунд (30 дней), valid-time 604800 секунд (7 дней)

3. Включить функцию DHCPv6 сервера на порту;

Команда	Описание

`ipv6 dhcp server <poolname> [preference <value>] [rapid-commit] [allow-hint]`	Включить функцию DHCPv6 сервера на интерфейсе и привязать используемый адресный пул `<poolname>`. `[preference <value>]` - задать приоритет `<value>` для данного DHCP-сервера, `[rapid-commit]` - быстрый ответ на solicit, `[allow-hint]` - разрешить делегировать префикс, предлагаемый клиентом.
`no ipv6 dhcp server <poolname>`	Выключить функцию DHCPv6 сервера на интерфейсе
В режиме конфигурации интерфейса	

41.3 Настройка DHCPv6-relay

1. Включение/выключение сервиса DHCPv6;
2. Настроить DHCPv6-relay на интерфейсе.

1. Включение/выключение сервиса DHCPv6;

Команда	Описание
`service dhcpv6`	Включить сервисы DHCPv6 (server, relay)
`no service dhcpv6`	Выключить сервисы DHCPv6 (по умолчанию)
В режиме глобальной конфигурации	

2. Настроить DHCPv6-relay на интерфейсе.

Команда	Описание
`ipv6 dhcp relay destination {[<ipv6-address>] [interface { <interface-name> | vlan <1-4096>}]}`	Настроить адрес назначения для DHCPv6-relay
`no ipv6 dhcp relay destination {[<ipv6-address>] [interface { <interface-name> | vlan <1-4096>}]}`	Удалить адрес назначения для DHCPv6-relay

В режиме конфигурации интерфейса	

41.4 Настройка сервера делегирования префиксов DHCPv6

1. Включить/выключить DHCPv6 сервис;
2. Настроить пул делегирования префиксов;
3. Настроить адресный пул DHCPv6:
    a. Создать/удалить адресный пул DHCPv6;
    b. Настроить пул делегирования префиксов, используемый адресным пулом;
    c. Настроить статическую привязку префиксов;
    d. Настроить другие параметры адресного пула DHCPv6;
4. Включить функцию сервера делегирования префиксов DHCPv6 на интерфейсе.

1. Включить/выключить DHCPv6 сервис;

Команда	Описание

`service dhcpv6`
 	
`no service dhcpv6`
 	
В режиме глобальной конфигурации
	Включить сервисы DHCPv6 (server, relay)
	
	Выключить сервисы DHCPv6 (по умолчанию)

2. Настроить пул делегирования префиксов;

Команда	Описание

`ipv6 local pool <poolname> <prefix|prefix-length> <assigned-length>`
 	
`no ipv6 local pool <poolname>`
 	
В режиме глобальной конфигурации
	Создать адресный пул `<poolname>` для делегирования префиксов `<prefix|prefix-length>`
	
	Удалить адресный пул `<poolname>`

3. Настроить адресный пул DHCPv6:
    a. Создать/удалить адресный пул DHCPv6;

Команда	Описание

`ipv6 dhcp pool <poolname>`
 	
`no ipv6 dhcp pool <poolname>`
 	
В режиме глобальной конфигурации
	Создать адресный пул DHCPv6
	
	Удалить адресный пул DHCPv6

b. Настроить пул делегирования префиксов, используемый адресным пулом;

Команда	Описание

`prefix-delegation pool <poolname> [lifetime <valid-time> <preferred-time>]`
 	
`no prefix-delegation pool <poolname>`
 	
В режиме конфигурации адресного пула DHCPv6
	Задать делегируемый пул префиксов `<poolname>` для адресного пула DHCPv6 и назначить используемый префикс клиенту, в полях `<preferred-time> <valid-time>` задать предпочтительное и действительное время аренды префикса.
	
	Удалить делегируемый пул префиксов `<poolname>`

c. Настроить статическую привязку префиксов;

Команда	Описание

`prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>] [lifetime <valid-time> <preferred-time>]`
 	
`no prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]`
 	
В режиме конфигурации адресного пула DHCPv6
	Настроить префикс `<ipv6-prefix/prefix-length>` для статической привязки к клиенту `<client-DUID>`
	
	удалить `<ipv6-prefix/prefix-length>` из статической привязки к клиенту `<client-DUID>`

d. Настроить другие параметры адресного пула DHCPv6;

Команда	Описание

`dns-server <ipv6-address>`
 	
`no dns-server <ipv6-address>`
 	
В режиме конфигурации адресного пула DHCPv6
	Задать адрес DNS-сервера
	
	Удалить адрес DNS-сервера

`domain-name <domain-name>`
 	
`no domain-name <domain-name>`
 	
В режиме конфигурации адресного пула DHCPv6
	Задать доменное имя
	
	Удалить доменное имя

4. Включить функцию сервера делегирования префиксов DHCPv6 на порту

Команда	Описание

`ipv6 dhcp server <poolname> [preference <value>] [rapid-commit] [allow-hint]`
 	
`no ipv6 dhcp server <poolname>`
 	
В режиме конфигурации интерфейса
	Включить функцию DHCPv6 сервера на интерфейсе и привязать используемый адресный пул `<poolname>`. `[preference <value>]` - задать приоритет `<value>` для данного DHCP-сервера, `[rapid-commit]` - быстрый ответ на solicit, `[allow-hint]` - разрешить делегировать префикс, предлагаемый клиентом.
	
	Выключить функцию DHCPv6 сервера на интерфейсе

41.5 Настройка клиента для делегирования префиксов DHCPv6

1. Включить/выключить DHCPv6 сервис;
2. Включить функцию сервера делегирования префиксов DHCPv6 на интерфейсе.

1. Включить/выключить DHCPv6 сервис;

Команда	Описание
`service dhcpv6`	Включить сервисы DHCPv6 (server, relay)

`no service dhcpv6` В режиме глобальной конфигурации	Выключить сервисы DHCPv6 (по умолчанию)

2. Включить функцию сервера делегирования префиксов DHCPv6 на интерфейсе.

Команда	Описание

`ipv6 dhcp client pd <prefix-name> [rapid-commit]`
 	
`no ipv6 dhcp client pd`
 	
В режиме глобальной конфигурации
	Включить функцию DHCPv6 делегирования префиксов на интерфейсе клиента
	
	Выключить функцию DHCPv6 делегирования префиксов на интерфейсе клиента

41.6 Пример конфигурации DHCPv6

При развертывании сетей IPv6 коммутатор SNR может быть настроен как сервер DHCPv6 для управления распределением адресов IPv6. Поддерживается режим с отслеживанием состояния, так и без отслеживания.

Топология:

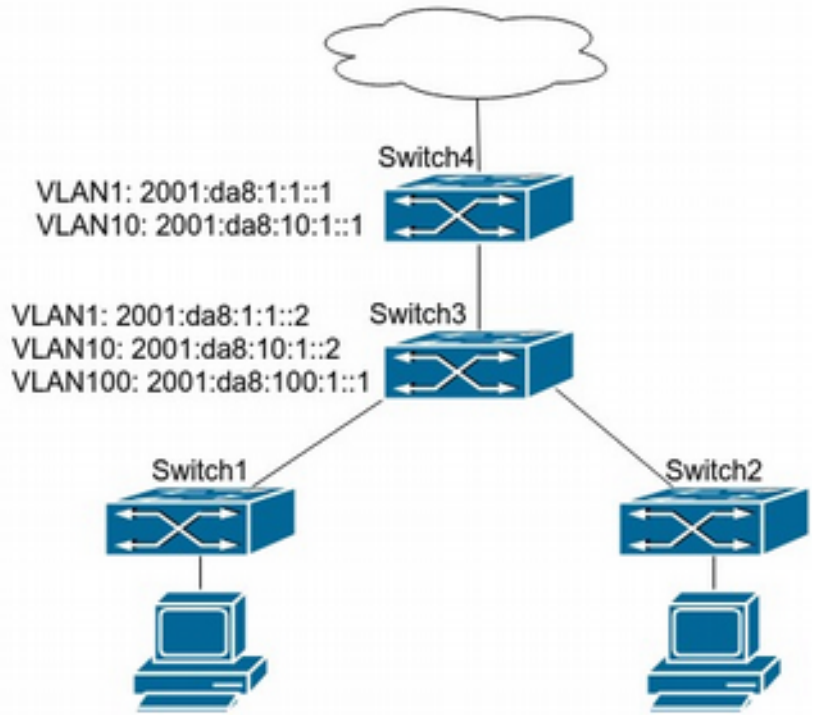


рисунок 41.2: пример настройки DHCPv6

Как показано на рисунке 41.2, на уровне доступа используются коммутаторы Switch1 и Switch2 для подключения пользователей в кампусе. На первом уровне агрегации коммутатор Switch3 настроен как DHCPv6-relay. На втором уровне агрегации коммутатор Switch4 настроен как DHCPv6 сервер и соединен с сетью вышестоящего оператора. На компьютерах пользователей установлена ОС, поддерживающая IPv6.

Конфигурация Switch4:

```
Switch4>enable
Switch4#config
Switch4(config)#service dhcpv6
Switch4(config)#ipv6 dhcp pool EastDormPool
Switch4(dhcpv6-EastDormPool-config)#network-address 2001:da8:100:1::1
2001:da8:100:1::100
Switch4(dhcpv6-EastDormPool-config)#excluded-address 2001:da8:100:1::1
Switch4(dhcpv6-EastDormPool-config)#dns-server 2001:da8::20
Switch4(dhcpv6-EastDormPool-config)#dns-server 2001:da8::21
Switch4(dhcpv6-EastDormPool-config)#domain-name dhcpv6.com
Switch4(dhcpv6-EastDormPool-config)#lifetime 1000 600
Switch4(dhcpv6-EastDormPool-config)#exit
Switch4(config)#interface vlan 1
Switch4(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::1/64
Switch4(Config-if-Vlan1)#exit
Switch4(config)#interface vlan 10
Switch4(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::1/64
Switch4(Config-if-Vlan10)#ipv6 dhcp server EastDormPool preference 80
Switch4(Config-if-Vlan10)#exit
Switch4(config)#
```

Конфигурация Switch3:

```
Switch3>enable
Switch3#config
Switch3(config)#service dhcpv6
Switch3(config)#interface vlan 1
Switch3(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::2/64
Switch3(Config-if-Vlan1)#exit
Switch3(config)#interface vlan 10
Switch3(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::2/64
Switch3(Config-if-Vlan10)#exit
Switch3(config)#interface vlan 100
Switch3(Config-if-Vlan100)#ipv6 address 2001:da8:100:1::1/64
Switch3(Config-if-Vlan100)#no ipv6 nd suppress-ra
Switch3(Config-if-Vlan100)#ipv6 nd managed-config-flag
Switch3(Config-if-Vlan100)#ipv6 nd other-config-flag
Switch3(Config-if-Vlan100)#exit
Switch3(config)#
```

Настройка Switch1 и Switch2 одинакова:

```
Switch1(config)#service dhcpv6
Switch1(config)#interface vlan 1
Switch1(Config-if-Vlan1)#ipv6 address 2001:da8:100:1::2/64
Switch1(Config-if-Vlan1)#ipv6 dhcp relay destination 2001:da8:10:1::1
```

41.7 Решение проблем при конфигурации DHCPv6

Если DHCPv6-клиент не может получить IP адрес и другие сетевые параметры, после проверки кабеля и клиентского оборудования следует выполнить следующее:

- Проверьте, запущен ли DHCPv6-сервер;
- Если DHCPv6 клиент и DHCPv6 сервер находятся не в одной сети и не имеют прямой l2-связности, проверьте, настроена ли на коммутаторе, отвечающем за пересылку пакетов, функция DHCPv6-relay;
- Проверьте, имеет ли DHCP-сервер адресный пул в том же сегменте, что и адрес interface vlan коммутатора, перенаправляющего DHCP-пакеты;

42. DHCP опция 82

42.1 Общие сведения об опции 82

Опция 82 протокола DHCP используется для того, чтобы проинформировать DHCP-сервер о том, от какого DHCP ретранслятора и через какой его порт был получен запрос. Коммутатор с функцией DHCP relay или DHCP snooping добавляет опцию в DHCP-запросы от клиента и передает их серверу. DHCP сервер, в свою очередь, предоставляет IP-адрес и другую конфигурационную информацию в соответствии с преднастроенными политиками на основании информации, полученной в заголовке опции 82. Коммутатор снимет заголовок опции с принятого от DHCP сервера сообщения и передаст сообщение клиенту в соответствии с информацией о физическом интерфейсе, указанной в опции. Применение опции 82 прозрачно для клиента.

Сообщение DHCP может включать множество полей различных опций, опция 82 - одна из них. Она должна располагаться после других опций, но до опции 255.

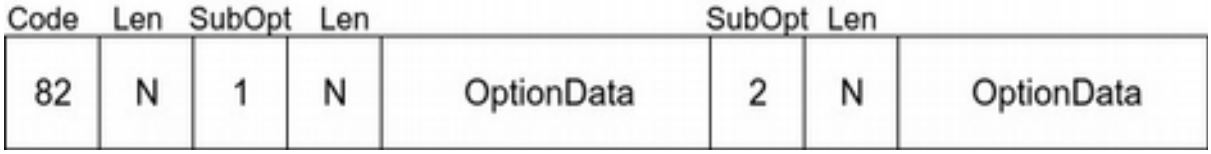


рис. 42.1 формат опции 82

Заголовок опции 82 может содержать несколько суб-опций. RFC3046 описывает 2 суб-опции Circuit-ID и Remote-ID.

42.2 Настройка добавления опции 82

1. Включить добавление опции 82 DHCP relay;
2. Включить добавление опции 82 DHCP snooping;
3. Настроить атрибуты опции 82 DHCP relay на интерфейсе;
4. Включить опцию 82 для DHCP сервера;
5. Настроить формат опции 82 для DHCP Relay;
6. Настроить разделитель;
7. Настроить метод создания опции 82;
8. Команды для диагностики опции 82;

1. Включить добавление опции 82 DHCP relay:

Команда	Описание
`ip dhcp relay information option`	Включить опцию 82 для добавления DHCP relay
`no ip dhcp relay information`	Выключить добавление опции 82 DHCP relay;

`option` В режиме глобальной конфигурации	

2. Включить добавление опции 82 DHCP snooping;

Команда	Описание
`ip dhcp snooping information enable`	Включить опцию 82 для добавления DHCP snooping
`no ip dhcp snooping information enable` В режиме глобальной конфигурации	Выключить добавление опции 82 DHCP snooping;

3. Настроить атрибуты опции 82;

Команда	Описание
i`p dhcp relay information policy {drop | keep | replace}`	Настроить режим политики при получении DHCP запроса, который уже содержит опцию 82: `drop` - запрос будет отброшен; `keep` - запрос будет передан без обработки; `replace` - поле опции 82 будет добавлено заново, после чего запросу будет передан серверу.
`no ip dhcp relay information policy` В режиме конфигурирования интерфейса VLAN	Восстановить значение по-умолчанию `(replace)`
`ip dhcp snooping information option allow-untrusted [replace]`	Разрешить передачу DHCP-запросов с добавленной опцией 82, полученные с недоверенных портов, `replace` - поле опции 82 будет добавлено заново, после чего запросу будет передан серверу.
`no ip dhcp snooping information option allow-`	Отбрасывать DHCP-запросы с добавленной

`untrusted` В режиме глобальной конфигурации	опцией 82, полученные с недоверенных портов (по-умолчанию)

`ip dhcp {snooping | relay} information option subscriber-id { standard | <circuit-id>}`
 	
`no ip dhcp {snooping | relay} information option subscriber-id`
 	
В режиме конфигурирования интерфейса
	Задать контекст `<circuit-id>` не длиннее 64 символов, передаваемый в качестве суб-опции Circuit-ID, добавляемой в DHCP-запросы, полученные с интерфейса. Возможно указать следующие ключи: `%h`: hostname; `%v`: vlan-id; `%M`: local MAC в верхнем регистре; `%m`: local MAC, в нижнем регистре; `%R`: client MAC,в верхнем регистре; `%r`: client MAC , в нижнем регистре; `%s`: slotID; `%p`: portID; `%i`: client ip address
	
	`standard` - стандартное имя VLAN и интерфейса (порта), например ”Vlan2+Ethernet1/0/12”.
	
	Вернуть значение по-умолчанию `(standard)`

`ip dhcp {snooping | relay} information option subscriber-id format {hex | acsii}` В режиме конфигурирования интерфейса	Задать формат опции 82, суб-опции Circuit-ID, добавляемой агентом DHCP-relay

4. Включить опцию 82 для DHCP сервера;

Команда	Описание

`ip dhcp server relay information enable`
 	
`no ip dhcp server relay information enable`
	Идентифицировать сервером коммутатора опцию 82.
	
	Игнорировать сервером коммутатора опцию 82.

В режиме глобальной конфигурации	

5. Настроить формат опции 82 для DHCP Relay;

Команда	Описание
`ip dhcp {snooping | relay} information option subscriber-id format {hex | acsii | vs-hp}` В режиме глобальной конфигурации	Задать формат опции 82, суб-опции Circuit-ID
`ip dhcp {snooping | relay} information option remote-id format {default | vs-hp}`	Задать формат опции 82, суб-опции Remote-ID

6. Настроить разделитель;

Команда	Описание

`ip dhcp {snooping | relay} information option delimiter [colon | dot | slash | space]`
 	
`no ip dhcp {snooping | relay} information option delimiter`
 	
В режиме глобальной конфигурации
	Задать разделитель каждого параметра суб-опций опции 82.
	
	Восстановить значение по-умолчанию `(slash)`

7. Настроить метод создания опции 82;

Команда	Описание

`ip dhcp {snooping|relay} information option self-defined remote-id {hostname | mac | string WORD}`
 	
`no ip dhcp {snooping | relay} information option self-defined`
	Задать метод создания суб-опции Remote-ID опции 82
	
	Восстановить значение по-умолчанию `(mac)`

`remote-id` В режиме глобальной конфигурации	
`ip dhcp {snooping | relay} information option self-defined remote-id format [ascii | hex]` В режиме глобальной конфигурации	Задать формат заданной пользователем суб-опции Remote-ID опции 82

`ip dhcp {snooping | relay} information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD }`
 	
`no ip dhcp {snooping | relay} information option self-defined subscriber-id`
 	
В режиме глобальной конфигурации
	Задать метод создания суб-опции Circuit-ID опции 82
	
	Восстановить значение по-умолчанию `(vlan port)`

`ip dhcp {snooping | relay} information option self-defined subscriber-id format [ascii | hex]` В режиме глобальной конфигурации	Задать формат заданной пользователем суб-опции Circuit-ID опции 82

8. Команды для диагностики опции 82;

Команда	Описание
`show ip dhcp relay information option` В привилегированном режиме	Отобразить информацию состоянии опции 82
`debug ip dhcp {snooping | relay} packet` В привилегированном режиме	Отобразить информацию о пакетах, обработанных агентом DHCP relay или DHCP snooping.

42.3 Пример конфигурации опции 82
42.3.1 Пример конфигурации опции 82 для DHCP relay

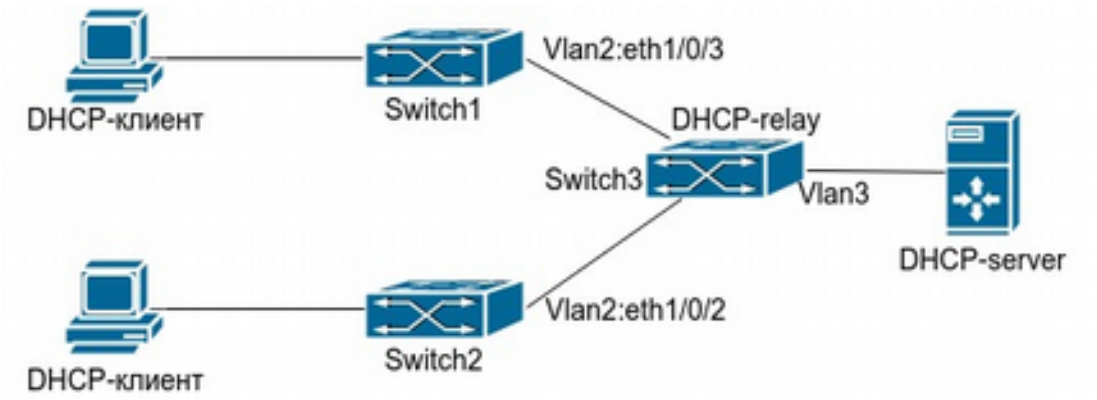


Рис.42.2 конфигурации опции 82 для DHCP relay

В приведенном на рисунке 42.2 примере коммутаторы уровня 2 Switch1 и Switch2 подключены к коммутатору 3-го уровня Switch3, который будет передавать сообщения от DHCP-клиента DHCP-серверу и обратно как агент DHCP relay. Если DHCP опция 82 отключена, DHCP-сервер не может распознать, к сети какого коммутатора, Switch1 или Switch2, подключен DHCP-клиент. В этом случае ПК, подключенные Switch1 и Switch2, получат адреса из общего пула DHCP-сервера. Если же DHCP опция 82 включена, Switch3 будет добавлять информацию о портах и vlan в запрос от DHCP-клиента. Таким образом, DHCP-сервер сможет выделить адрес из двух разных подсетей, чтобы упростить управление.

Конфигурация коммутатора Switch3(MAC address is f8:f0:82:75:33:01):

```
Switch3(Config)#service dhcp
Switch3(Config)#ip dhcp relay information option
Switch3(Config)#ip forward-protocol udp bootps
Switch3(Config)#interface vlan 3
Switch3(Config-if-vlan3)#ip address 192.168.10.222 255.255.255.0
Switch3(Config-if-vlan2)#ip address 192.168.102.2 255.255.255.0
Switch3(Config-if-vlan2)#ip helper 192.168.10.88
```

Пример конфигурации ISC DHCP Server для Linux:

```
ddns-update-style interim;
ignore client-updates;

class "Switch3Vlan2Class1" {
match if option agent.circuit-id = "Vlan2+Ethernet1/0/2" and
option agent.remote-id=f8:f0:82:75:33:01;
}

class "Switch3Vlan2Class2" {
```

```
    match if option agent.circuit-id = "Vlan2+Ethernet1/0/3" and
option agent.remote-id=f8:f0:82:75:33:01;
    }

    subnet 192.168.102.0 netmask 255.255.255.0 {
    option routers 192.168.102.2;
    option subnet-mask 255.255.255.0;
    option domain-name "example.com.cn";
    option domain-name-servers 192.168.10.3;
    authoritative;

    pool {
    range 192.168.102.21 192.168.102.50;
    default-lease-time 86400; #24 Hours
    max-lease-time 172800; #48 Hours
    allow members of "Switch3Vlan2Class1";
    }
    pool {
    range 192.168.102.51 192.168.102.80;
    default-lease-time 43200; #12 Hours
    max-lease-time 86400; #24 Hours
    allow members of "Switch3Vlan2Class2";
    }
    }
```

После описанных выше настроек DHCP-сервер будет выделять адреса из диапазона 192.168.102.21 ~ 192.168.102.50 для устройств, подключенных к коммутатоу Switch2, и из диапазона 192.168.102.51～192.168.102.80 для устройств, подключенных к коммутатоу Switch1.

42.3.2 Пример конфигурации опции 82 для DHCP snooping

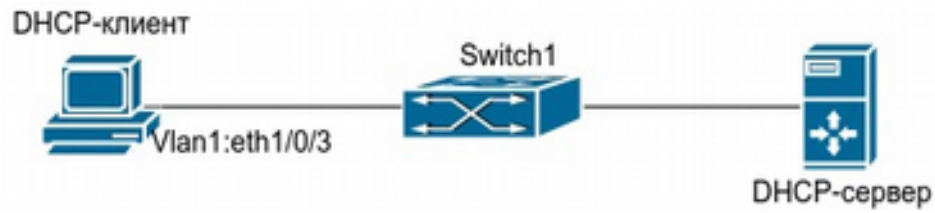


Рис.42.3 настройка опции 82 для DHCP snooping

Как показано на рисунке 42.3, коммутатор уровня 2 Switch1 с включенным DHCP-snooping передает DHCP-запросы серверу и ответы от DHCP-сервера клиенту. После того, как на коммутаторе будет включена функция добавления опции 82 для DHCP snooping, Switch1 будет добавлять информацию о коммутаторе, интерфейсе и VLAN клиента в сообщения запроса.

Конфигурация коммутатора Switch1(MAC address is f8:f0:82:75:33:01):

```
Switch1(config)#ip dhcp snooping enable
Switch1(config)#ip dhcp snooping binding enable
Switch1(config)#ip dhcp snooping information enable
Switch1(Config-If-Ethernet1/0/12)#ip dhcp snooping trust
```

Пример конфигурации ISC DHCP Server для Linux:

```
ddns-update-style interim;
ignore client-updates;

class "Switch1Vlan1Class1" {
match if option agent.circuit-id = "Vlan1+Ethernet1/0/3" and option
agent.remote-id=f8:f0:82:75:33:01;
}

subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name "example.com.cn";
option domain-name-servers 192.168.10.3;
authoritative;
pool {
range 192.168.102.51 192.168.102.80;
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch1Vlan1Class1";
}
}
```

После описанных выше настроек DHCP-сервер будет выделять адреса из диапазона 192.168.102.51 ～ 192.168.102.80 для устройств, подключенных к коммутатоу Switch1.

42.4 Решение проблем с конфигурацией опции 82

- Убедитесь, что DHCP relay и/или DHCP snooping настроен правильно;
- Опция 82 требует взаимодействия DHCP relay и DHCP сервера для выделения IP-адресов. DHCP сервер должен установить политику выделения адресов основываясь на сетевой топологии DHCP relay. Если в сети больше одного ретранслятора, уделите внимание политике передачи DHCP запросов;
- При поиске неисправностей подробная информация о процессе работы функции опции 82 DHCP relay и DHCP-сервера может быть получена с помощью команд

«debug ip dhcp relay packet» и «debug ip dhcp server packet».

43. DHCP опции 60 и 43

43.1 Общие сведения об опциях 60 и 43

DHCP-сервер анализирует сообщения от DHCP-клиента. Если сообщение содержит опцию 60 (Vendor-class-Idetifier, идентификатор производителя), в ответном сообщении DHCP сервер может передать DHCP-клиенту опцию 43 (Vendor Specific Information):

Возможны следующие варианты настройки опций 60 и 43 в адресном пуле DHCP-сервера:

1. Опции 60 и 43 настроены одновременно. Если DHCP сообщение от DHCP клиента с опцией 60 совпадает с опцией 60, сконфигурированной в адресном пуле DHCP-сервера, DHCP-клиент получит в ответ опцию 43 настроенную в этом адресном пуле. Иначе опция 43 клиенту не возвращается.
2. Настроена опция 43, соответствующая любой опции 60. Если будет получено сообщение, содержащее опцию 60 по DHCP клиента, он получит сконфигурированную опцию 60 в ответ.
3. Настроена только опция 60. В этом случае DHCP-сервер не добавит опцию 43 в ответ DHCP-клиенту.

43.2 Настройка опций 60 и 43

Команда	Описание
`option 60 ascii LINE`	Задать опцию 60 в формате ASCII
`option 43 ascii LINE`	Задать опцию 43 в формате ASCII
`option 60 hex WORD`	Задать опцию 60 в формате HEX
`option 43 hex WORD`	Задать опцию 43 в формате HEX
`option 60 ip A.B.C.D`	Задать опцию 60 в формате IP-адреса
`option 43 ip A.B.C.D`	Задать опцию 43 в формате IP-адреса
`no option 60`	Удалить опцию 60 из адресного пула
`no option 43`	Удалить опцию 43 из адресного пула
В режиме конфигурации адресного пула	

43.3 Пример настройки опций 60 и 43

Точка доступа AP7622 отправляет в DHCP-запросе опцию 60, получает IP адрес и атрибут опции 43 от DHCP-сервера для отправки запроса на контроллер беспроводной сети. На DHCP-сервере настроена опция 43, соответствующая опции 60 для данной точки доступа: адреса контроллера беспроводной сети 192.168.100.2 и 192.168.100.3.

Настройка DHCP-сервера:

```
switch (config)#ip dhcp pool a
switch (dhcp-a-config)#option 60 ascii AP7622
switch (dhcp-a-config)#option 43 hex 0104C0A864020104C0A86403
```

43.4 Решение проблем при настройке опций 60 и 43

- Проверьте, включена ли функция DHCP сервера (service dhcp);
- Убедитесь, что настроенная опция 60 в адресном пуле сочетается с опцией 60 в пакетах.

44. DHCPv6 опции 37 и 38

44.1 Общая информация о опциях 37 и 38 DHCPv6

DHCPv6 (протокол динамический конфигурации хоста для IPv6) предназначен для адресной схемы IPv6 и используется для назначения префиксов IPv6, IPv6 адресов и других конфигурационных параметров.

Если DHCPv6 клиент хочет запросить параметры конфигурации у DHCPv6 сервера, который находится в другом сегменте сети, ему необходимо использовать DHCPv6 relay. Сообщение DHCPv6, полученное агентом DHCPv6 Relay, инкапсулируется в “relay-forward” пакет, который затем направляется серверу. DHCPv6 сервер отвечает агенту DHCPv6 relay сообщением “relay-reply”, из которого DHCPv6 relay восстанавливает DHCPv6 сообщение и пересылает клиенту.

При использовании DHCPv6 relay возникает ряд проблем, например: как избежать нелегального присвоения адресов или как назначить конкретный IPv6 адрес конкретному пользователю. Эти задачи решаются добавлением к сообщениям DHCPv6 опций 37 и 38, описанных в RFC4649 и RFC4580.

Функционал опций 37 и 38 DHCPv6 подобен функционалу опции 82 DHCP для IPv4. DHCPv6 relay добавляет к заголовку опции 37 и 38 к запросам клиента и убирает их из ответных от сервера пакетов. Таким образом, применение опций 37 и 38 прозрачно для DHCPv6 клиента.

По содержанию опций 37 и 38 DHCPv6 сервер может аутентифицировать клиента и relay, назначать и управлять адресами. Так как RFC4649 и RFC4580 и не определяют, как должны быть использованы опции, пользователь может использовать их по своему усмотрению.

44.2 Конфигурирование опций 37 и 38 DHCPv6

1. Настройка базовых функций опций DHCPv6 snooping;
2. Настройка базовых функций опций DHCPv6 relay;
3. Настройка базовых функций опций DHCPv6 server.

1. Настройка базовых функций опций DHCPv6 snooping:

Команда	Описание

`ipv6 dhcp snooping remote-id option`
 	
`no ipv6 dhcp snooping remote-id option`
 	
В режиме глобальной конфигурации
	Включить поддержку опции 37 в DHCPv6-snooping
	
	Выключить поддержку опции 37 в DHCPv6-snooping

`ipv6 dhcp snooping subscriber-id`	Включить поддержку опции 38 в DHCPv6-

`option`
 	
`no ipv6 dhcp snooping subscriber-id option`
 	
В режиме глобальной конфигурации
	snooping
	
	Выключить поддержку опции 38 в DHCPv6-snooping

`ipv6 dhcp snooping remote-id policy {drop | keep | replace}`
 	
`no ipv6 dhcp snooping remote-id policy`
 	
В режиме глобальной конфигурации
	Настроить режим политики при получении DHCPv6 запроса, который уже содержит опцию 37: `drop` - запрос будет отброшен; `keep` - запрос будет передан без обработки; `replace` - поле опции 37 будет добавлено агентом
	
	Восстановить значение по-умолчанию `(replace)`

`ipv6 dhcp snooping subscriber-id policy {drop | keep | replace}`
 	
`no ipv6 dhcp snooping subscriber-id policy`
 	
В режиме глобальной конфигурации
	Настроить режим политики при получении DHCPv6 запроса, который уже содержит опцию 38: `drop` - запрос будет отброшен; `keep` - запрос будет передан без обработки; `replace` - поле опции 38 будет добавлено агентом
	
	Восстановить значение по-умолчанию `(replace)`

2. Настройка базовых функций опций DHCPv6 relay:

Команда	Описание

`ipv6 dhcp relay remote-id option`
 	
`no ipv6 dhcp relay remote-id option`
 	
В режиме глобальной конфигурации
	Включить поддержку опции 37 в DHCPv6-relay
	
	Выключить поддержку опции 37 в DHCPv6-relay

`ipv6 dhcp relay subscriber-id option`	Включить поддержку опции 38 в DHCPv6-relay

`no ipv6 dhcp relay subscriber-id option` В режиме глобальной конфигурации	Выключить поддержку опции 38 в DHCPv6-relay

`ipv6 dhcp relay subscriber-id select pv delimiter WORD (delimiter WORD |)`
 	
`no ipv6 dhcp relay subscriber-id select delimiter`
 	
В режиме глобальной конфигурации
	Выбрать разделитель между наименованием порта и vlan для опции 38. Доступны символы #|.|,|;|:|/|+|пробел.
	
	Восстановить значения по-умолчанию - без разделителя.

`ipv6 dhcp relay remote-id <remote-id>`
 	
`no ipv6 dhcp relay remote-id`
 	
В режиме конфигурации Interface Vlan
	Задать содержание опции 37 строкой `<remote-id>`, не более 128 символов
	
	Восстановить значение по-умолчанию (VLAN MAC)

`ipv6 dhcp relay subscriber-id <subscriber-id>`
 	
`no ipv6 dhcp relay subscriber-id`
 	
В режиме конфигурации Interface Vlan
	Задать содержание опции 38 строкой `<subscrider-id>`, не более 128 символов
	
	Восстановить значение по-умолчанию (VLAN+port)

3. Настройка базовых функций опций DHCPv6 server:

Команда	Описание

`ipv6 dhcp server remote-id option`
 	
`no ipv6 dhcp server remote-id option`
 	
В режиме глобальной конфигурации
	Включить поддержку опции 37 для DHCPv6-сервера
	
	Выключить поддержку опции 37 для DHCPv6-сервера

`ipv6 dhcp server subscriber-id option`	Включить поддержку опции 38 для DHCPv6-сервера

`no ipv6 dhcp server subscriber-id option` В режиме глобальной конфигурации	Выключить поддержку опции 38 для DHCPv6-сервера

`ipv6 dhcp use class`
 	
`no ipv6 dhcp use class`
 	
В режиме глобальной конфигурации
	Включить поддержку классов для DHCPv6 адресов
	
	Выключить поддержку классов для DHCPv6 адресов (команда не удаляет настройки классов)

`ipv6 dhcp class <class-name>`
 	
`no ipv6 dhcp class <class-name>`
 	
В режиме глобальной конфигурации
	Создать dhcpv6 класс `<class-name>` и войти в режим его конфигурирования
	
	Удалить dhcpv6 класс `<class-name>`

`ipv6 dhcp server select relay-forward`
 	
`no ipv6 dhcp server select relay-forward`
 	
В режиме конфигурации Interface Vlan
	Выбрать для чтения опции 37 и 38 из верхнего уровня, при наличии нескольких опций
	
	Вернуть значения по-умолчанию - читать опцию из оригинального пакета клиента

`{remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*]}`
 	
`no {remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*]}`
 	
В режиме конфигурирования IPv6 DHCP класса
	Настроить опции 37 и 38, соответствующие данному классу

`class <class-name>`
 	
`no class <class-name>`
	Задать соответствие класса `<class-name>` текущему адресному пулу DHCPv6
	
	Удалить соответствие класса `<class-name>` текущему адресному пулу

В режиме конфигурирования адресного пула DHCPv6	DHCPv6
`address range <start-ip> <end-ip>`	Задать диапазон адресов для текущего адресного пула
`no address range <start-ip> <end-ip>` В режиме конфигурирования адресного пула DHCPv6	Удалить диапазон адресов для текущего адресного пула

44.3 Примеры настройки опций 37 и 38 DHCPv6

44.3.1 Пример настройки опций 37 и 38 для DHCPv6 snooping и сервера

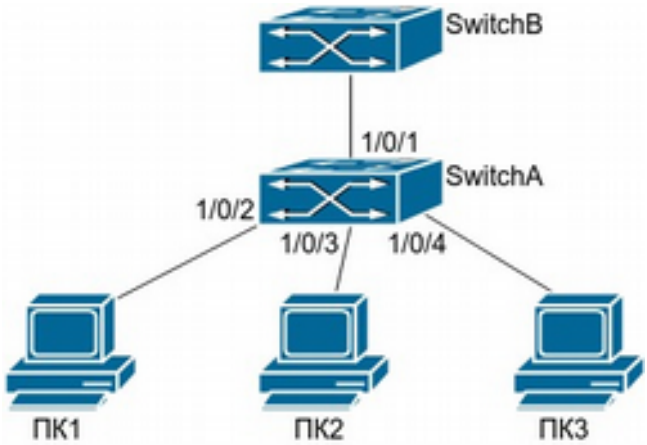


Рисунок 44.1 Пример настройки опций 37 и 38 для DHCPv6 snooping и сервера

Как показано на рисунке 19.1, ПК1, ПК2 и ПК3 подключены к недоверенным портам 1/0/2, 1/0/3 и 1/0/4, и с помощью DHCPv6 получают IP адреса 2010:2, 2010:3 и 2010:4 соответственно. DHCPv6 сервер подключен к доверенному порту 1/0/1. Настроены следующие политики выделения адресов (классы): CLASS1 соответствует опции 38, CLASS2 соответствует опции 37, а CLASS3 - опциям 37 и 38. В пуле адресов TestPool1 классам CLASS1, CLASS2 и CLASS3 будут назначены адреса 2001:da8:100:1::2 - 2001:da8:100:1::30, 2001:da8:100:1::31 - 2001:da8:100:1::60 и 2001:da8:100:1::61 - 2001:da8:100:1::100 соответственно. На коммутаторе SwitchA включена функция DHCPv6-snooping и настроены опции 37 и 38.

Конфигурация коммутатора SwitchA:

```
SwitchA(config)#ipv6 dhcp snooping remote-id option
SwitchA(config)#ipv6 dhcp snooping subscriber-id option
SwitchA(config)#int e 1/0/1
SwitchA(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust
```

```
SwitchA(config-if-ethernet1/0/1)#exit
SwitchA(config)#interface vlan 1
SwitchA(config-if-vlan1)#ipv6 address 2001:da8:100:1::1
SwitchA(config-if-vlan1)#exit
SwitchA(config)#interface ethernet 1/0/1-4
SwitchA(config-if-port-range)#switchport access vlan 1
SwitchA(config-if-port-range)#exit
SwitchA(config)#
```

Конфигурация коммутатора SwitchB:

```
SwitchB(config)#service dhcpv6
SwitchB(config)#ipv6 dhcp server remote-id option
SwitchB(config)#ipv6 dhcp server subscriber-id option
SwitchB(config)#ipv6 dhcp pool TestPool1
SwitchB(dhcpv6-eastdormpool-config)#network-address
2001:da8:100:1::2 2001:da8:100:1::1000
SwitchB(dhcpv6-eastdormpool-config)#dns-server 2001::1
SwitchB(dhcpv6-eastdormpool-config)#domain-name dhcpv6.com
SwitchB(dhcpv6-eastdormpool-config)# excluded-address
2001:da8:100:1::2
SwitchB(dhcpv6-eastdormpool-config)#exit
SwitchB(config)#
SwitchB(config)#ipv6 dhcp class CLASS1
SwitchB(dhcpv6-class-class1-config)#remote-id 00-03-0f-00-00-01
subscriber-id vlan1+Ethernet1/0/1
SwitchB(dhcpv6-class-class1-config)#exit
SwitchB(config)#ipv6 dhcp class CLASS2
SwitchB(dhcpv6-class-class2-config)#remote-id 00-03-0f-00-00-01
subscriber-id vlan1+Ethernet1/0/2
SwitchB(dhcpv6-class-class2-config)#exit
SwitchB(config)#ipv6 dhcp class CLASS3
SwitchB(dhcpv6-class-class3-config)#remote-id 00-03-0f-00-00-01
subscriber-id vlan1+Ethernet1/0/3
SwitchB(dhcpv6-class-class3-config)#exit
SwitchB(config)#ipv6 dhcp pool TestPool1
SwitchB(dhcpv6-eastdormpool-config)#class CLASS1
SwitchB(dhcpv6-pool-eastdormpool-class-class1-config)#address
range 2001:da8:100:1::3 2001:da8:100:1::30
SwitchB(dhcpv6-pool-eastdormpool-class-class1-config)#exit
SwitchB(dhcpv6-eastdormpool-config)#class CLASS2
SwitchB(dhcpv6-pool-eastdormpool-class-class2-config)#address
range 2001:da8:100:1::31 2001:da8:100:1::60
SwitchB(dhcpv6-eastdormpool-config)#class CLASS3
SwitchB(dhcpv6-pool-eastdormpool-class-class3-config)#address
range 2001:da8:100:1::61 2001:da8:100:1::100
```

```
SwitchB(dhcpv6-pool-eastdormpool-class-class3-config)#exit
SwitchB(dhcpv6-eastdormpool-config)#exit
SwitchB(config)#interface vlan 1
SwitchB(config-if-vlan1)#ipv6 address 2001:da8:100:1::2/64
SwitchB(config-if-vlan1)#ipv6 dhcp server TestPool1
SwitchB(config-if-vlan1)#exit
SwitchB(config)#
```

44.3.1 Пример настройки опций 37 и 38 для DHCPv6 relay

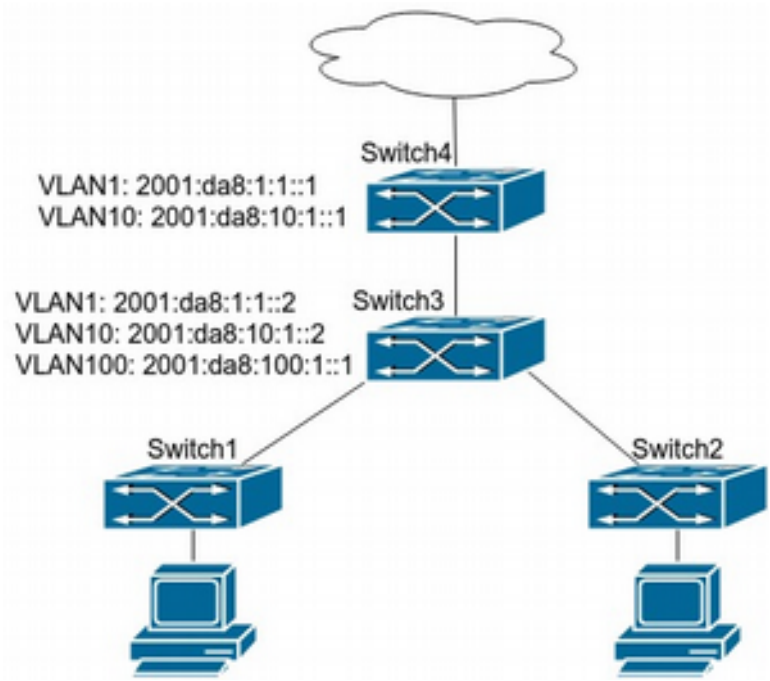


Рисунок 44.2 Пример настройки опций 37 и 38 для DHCPv6 relay

Для подключения пользователей сети кампуса на уровне доступа используются коммутаторы уровня 2 Switch1 и Switch2. На первом уровне агрегации коммутатор Switch3 используется как агент DHCPv6 relay. На втором уровне агрегации коммутатор Switch4 используется как DHCPv6 сервер и соединен с остальной сетью.

Конфигурация Switch2:

```
Switch2(config)#service dhcpv6
Switch2(config)#ipv6 dhcp relay remote-id option
Switch2(config)#ipv6 dhcp relay subscriber-id option
Switch2(config)#vlan 10
Switch2(config-vlan10)#int vlan 10
Switch2(config-if-vlan10)#ipv6 address 2001:da8:1:::2/64
Switch2(config-if-vlan10)#ipv6 dhcp relay destination
```

```
2001:da8:10:1::1
      Switch2(config-if-vlan10)#exit
```

44.4 Решение проблем при настройке опций 37 и 38 DHCPv6

- Сообщения запроса DHCPv6 от клиента рассылаются как мультикаст-пакеты и могут быть получены устройством в пределах VLAN клиента. Если DHCPv6 сервер и DHCPv6 клиент находятся в разных VLAN, необходимо использовать DHCPv6 relay.
- Если пакет с опциями 37,38 не был получен, проверьте выбранную политику DHCPv6 при получении пакета с опцией: политика может выполнять как пропуск, так и перезапись опции или сброс пакета.
- По-умолчанию DHCPv6 сервер считывает опции 37 и 38 из пакета клиента. Также может быть настроено считывание опций из пакета от DHCPv6 relay.

45 DCSCM

45.1 Общие сведения о DCSCM

Технология DCSCM (Destination control and source control multicast) включает 3 аспекта: контроль источника мультикаст-трафика (multicast source control), контроль получателя мультикаст-трафика (destination control) и политика приоритета мультикаст трафика (Multicast policy). Контроль источника мультикаст-трафика (Multicast source control) позволяет контролировать входящий поток мультикаста от источника. Может применяться на пограничном коммутаторе, в точке присоединения к сети вещателя мультикаста, а также на коммутаторе, используемом в качестве Rendezvous Point (RP). Контроль получателя мультикаст трафика (Multicast destination control) основан на ограничении сообщений IGMP, отправленных пользователем. Политика приоритета мультикаст трафика (Multicast policy), предоставляет возможность задать приоритет CoS multicast-пакетам, приходящим на коммутатор.

45.2 Настройка DCSCM

1. Настроить Multicast source control
    a. Включить функцию Multicast source control
    b. Настроить ACL
    c. Применить правило на интерфейсе
2. Настроить Multicast destination control
    a. Включить функцию Multicast destination control
    b. Настроить ACL
    c. Применить правило на интерфейсе
3. Настроить Multicast policy

1. Настроить Multicast source control
    a. Включить функцию Multicast source control

Команда	Описание
`[no] ip multicast source-control` В режиме глобальной конфигурации	Включить функцию Multicast source control, `[no]` отменяет это действие. Эту функцию нельзя выключить до тех пор, пока применено хотя бы одно правило multicast source-control.

    b. Настроить ACL

Команда	Описание
`[no] access-list <5000-5099> {deny|permit} ip {{<source>`	Конфигурация правил для Multicast source control. Каждый лист `<5000-`

<source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination} В режиме глобальной конфигурации	5099> может содержать от 1 до 10 правил. Лист по-умолчанию выполняет запрещающее действие если явно не задано разрешающего правила. [no] удаляет правило.

c. Применить правило на интерфейсе

Команда	Описание
[no] ip multicast source-control access-group <5000-5099> В режиме конфигурирования интерфейса	Применить правило Multicast source control на интерфейсе, [no] отменяет это действие

2. Настроить Multicast destination control
   a. Включить функцию Multicast destination control

Команда	Описание
[no] multicast destination-control В режиме глобальной конфигурации	Включить функцию Multicast destination control, [no] отменяет это действие.

b. Настроить ACL

Команда	Описание
[no] profile-id <1-50> {deny| permit} {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination} no profile-id <1-50>	Добавить правило profile-id <1-50> для Multicast destination control. Команда [no] удаляет это правило. profile-id служит для более удобного конфигурирования ACL Multicast destination control и в последствии должен быть добавлен в этот ACL.

В режиме глобальной конфигурации	
`[no] access-list <6000-7999> {{{add | delete} profile-id WORD} | {{deny|permit} (ip) {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}}` В режиме глобальной конфигурации	Добавить правило ACL `<6000-7999>` для Multicast destination control. Команда `[no]` удаляет это правило.

c. Применить правило на интерфейсе

Команда	Описание
`[no] ip multicast destination-control access-group <6000-7999>` В режиме конфигурирования интерфейса	Применить правило Multicast destination control на интерфейсе, `[no]` отменяет это действие
`[no] ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999>` В режиме глобальной конфигурации	Применить правило Multicast destination control на VLAN `<1-4094>` и `<macaddr>`, `[no]` отменяет это действие
`[no] ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>` В режиме глобальной конфигурации	Применить правило Multicast destination control на IP-адрес или подсеть назначения `<IPADDRESS/M>`, `[no]` отменяет это действие

3. Настроить Multicast policy

Команда	Описание
`[no] ip multicast policy <source_IPADDRESS/M>`	Добавлять значение `<priority>` в метку CoS заголовка VLAN 802.1q пакета

<destination_IPADDRESS/M> cos <priority> В режиме глобальной конфигурации	с адресом источника <source_IPADDRESS/M> и адресом назначения <destination_IPADDRESS/M>, [no] отменяет это действие.

45.3 Пример настройки DCSCM

45.3.1 Пример настройки Multicast Source Control

Чтобы предотвратить прием нежелательных multicast-групп от одного из контент-провайдеров, подключенного к порту Ethernet1/0/5, на коммутаторе настраивается правило Multicast Source Control, разрешающее прием только группы с адресом 239.255.1.2. К порту Ethernet 1/0/10 коммутатора подключен собственный источник мультикаста, поэтому необходимо настроить Multicast Source Control на прием всех групп с этого порта.

Конфигурация коммутатора:

```
Switch(config)#access-list 5000 permit ip any host 239.255.1.2
Switch(config)#access-list 5001 permit ip any any
Switch(config)#ip multicast source-control
Switch(config)#interface ethernet1/0/5
Switch(Config-If-Ethernet1/0/5)#ip multicast source-control access-
group 5000
Switch(config)#interface ethernet1/0/10
Switch(Config-If-Ethernet1/0/10)#ip multicast source-control access-
group 5001
```

45.3.2 Пример настройки Multicast Destination Control

Для реализации политики доступа пользователей необходимо запретить пользователям из подсети 10.0.0.0/8 подписку на группы из диапазона 239.0.0.0/8 Для работы Multicast Destination Control необходим IGMP snooping.

Конфигурация коммутатора:

```
Switch(config)#ip igmp snooping
Switch(config)#ip igmp snooping vlan 2
Switch(config)#access-list 6000 deny ip any 239.0.0.0 0.0.0.255
Switch(config)#access-list 6000 permit ip any any
Switch(config)#multicast destination-control
Switch(config)#ip multicast destination-control 10.0.0.0/8 access-
group 6000
```

Возможен также вариант с использованием profile-id:

```
Switch (config)#profile-id 1 deny ip any 239.0.0.0 0.0.0.255
Switch (config)#access-list 6000 add profile-id 1
Switch (config)#multicast destination-control
Switch (config)#ip multicast destination-control 10.0.0.0/8 access-
group 6000
```

45.3.3 Пример настройки Multicast Policy

Сервер 10.1.1.1 вещает важные мультикаст данные в группе 239.1.2.3, чтобы задать приоритет таким пакетам, необходимо настроить коммутатор следующие образом:

```
Switch(config)#ip multicast policy 10.1.1.1/32 239.1.2.3/32 cos 4
```

После применения этой конфигурации, мультикаст поток на группу 239.1.2.3 будет иметь приоритет CoS 4.

45.4 Решение проблем с настройкой DCSCM

- После применения команды **ip multicast source-control** весь мультикаст трафик будет приостановлен до применения разрешающих правил;
- Применение большого числа правил ACL может полностью израсходовать ресурс TCAM на коммутаторе, поэтому некоторые правила могут не работать; Убедитесь, что ресурса TCAM достаточно для применения требуемых правил.
- Функционал DCSCM аналогичен функционалу ACL, ознакомьтесь с разделом “Решение проблем с настройкой ACL”.

46 IGMP Snooping

46.1 Общие сведения о IGMP Snooping

IGMP (Internet Group Management Protocol) - протокол управления групповой (multicast) передачей данных в IP-сетях. IGMP используется маршрутизаторами и хостами для организации присоединения сетевых устройств к группам многоадресной рассылки (multicast). Маршрутизатор использует multicast-адрес 224.0.0.1 для отправки IGMP-сообщения запроса подтверждения членства в группах. Если хост присоединяется к какой либо группе, он должен отправить IGMP-запрос на соответствующий адрес группы.

IGMP Snooping используется для прослушивания IGMP-сообщений и контроля multicast трафика/ На основе IGMP-сообщений коммутатор ведет таблицу переадресации multicast, трафик отправляется только на порты, с которых поступил запрос на многоадресную группу.

46.2 Настройка IGMP Snooping

1. Включить IGMP Snooping
2. Настроить IGMP Snooping

1. Включить IGMP Snooping

Команда	Описание

`ip igmp snooping`
`no ip igmp snooping`
 	
В режиме глобальной конфигурации
	Включить IGMP Snooping
	Отключить IGMP Snooping

2. Настроить IGMP Snooping

Команда	Описание

`ip igmp snooping vlan <vlan-id>`
`no ip igmp snooping vlan <vlan-id>`
 	
В режиме глобальной конфигурации
	Включить IGMP Snooping для VLAN `<vlan-id>`, команда `no` отменяет это действие.

`ip igmp snooping proxy`
`no ip igmp snooping proxy`
 	
В режиме глобальной конфигурации
	Включить функцию IGMP Snooping proxy, команда `no` отменяет это действие.

`ip igmp snooping vlan <vlan-id>` `limit {group <1-65535> | source`	Задать максимальное количество групп `group <1-65535>` или источников для

<1-65535>} no ip igmp snooping vlan < vlan-id > limit В режиме глобальной конфигурации	групп source <1-65535> для VLAN <vlan-id> Восстановить значения по-умолчанию: group <1-65535> - 50, source <1-65535> - 40
ip igmp snooping vlan<vlan-id> interface (ethernet | port-channel|) IFNAME limit {group <1-65535>| source <1-65535>} strategy (replace | drop) no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit group source strategy В режиме глобальной конфигурации	Задать максимальное количество групп group <1-65535> или источников для групп source <1-65535> во VLAN <vlan-id> для интерфейса IFNAME, а также назначить стратегию (replace | drop) при превышении этого лимита. Восстановить значение по-умолчанию: максимальное значение не ограничено.
ip igmp snooping vlan <vlan-id> l2-general-querier no ip igmp snooping vlan <vlan-id> l2-general-querier В режиме глобальной конфигурации	Включить функцию L2 General-Querier для VLAN <vlan-id> Выключить функцию L2 General-Querier для VLAN <vlan-id>
ip igmp snooping vlan <vlan-id> l2-general-querier-version <version> В режиме глобальной конфигурации	Задать версию IGMP для L2 General-Querier
ip igmp snooping vlan <vlan-id> l2-general-querier-source <source> В режиме глобальной конфигурации	Задать IP-адрес источника сообщений IGMP для L2 General-Querier
ip igmp snooping vlan <vlan-id> mrouter-port interface <interface –name> no ip igmp snooping vlan <vlan-id> mrouter-port interface	Задать Mrouter порт <interface –name> для <vlan-id> Удалить Mrouter порт <interface –name> для <vlan-id>

<interface -name> В режиме глобальной конфигурации	
ip igmp snooping vlan <vlan-id> mrouter-port learnpim no ip igmp snooping vlan <vlan-id> mrouter-port learnpim В режиме глобальной конфигурации	Включить динамическое добавление Mrouter порта для VLAN <vlan-id>, из которого получены PIM-пакеты. Команда **no** отменяет это действие.
ip igmp snooping vlan <vlan-id> mrpt <value> no ip igmp snooping vlan <vlan-id> mrpt В режиме глобальной конфигурации	Задать максимальное время жизни в секундах <value> Mrouter-порта, определенного динамически для <vlan-id>. Восстановить значение <value> по-умолчанию - 255 секунд.
ip igmp snooping vlan <vlan-id> query-interval <value> no ip igmp snooping vlan <vlan-id> query-interval В режиме глобальной конфигурации	Задать интервал отправки <value> в секундах IGMP query general для <vlan-id>. Восстановить значение <value> по-умолчанию - 125 секунд.
ip igmp snooping vlan <vlan-id> immediately-leave no ip igmp snooping vlan <vlan-id> immediately-leave В режиме глобальной конфигурации	Включить функцию быстрого удаления подписки на группу для <vlan-id> Выключить функцию быстрого удаления подписки на группу для VLAN <vlan-id>
ip igmp snooping vlan <vlan-id> query-mrsp <value> no ip igmp snooping vlan <vlan-id> query-mrsp В режиме глобальной конфигурации	Задать максимальное время ответа на General Query <value> в секундах для VLAN <vlan-id> Восстановить значение по-умолчанию - 10 секунд
ip igmp snooping vlan <vlan-id> query-robustness <value>	Задать количество <value> IGMP Query без ответа, после отправки которых коммутатор удалит запись IGMP snooping

`no ip igmp snooping vlan <vlan-id> query-robustness` В режиме глобальной конфигурации	для VLAN `<vlan-id>`. Восстановить значение по-умолчанию - 2.

`ip igmp snooping vlan <vlan-id> suppression-query-time <value>`
 	
`no ip igmp snooping vlan <vlan-id> suppression-query-time`
 	
В режиме глобальной конфигурации
	Задать время подавления Querier `<value>` в секундах при получении query в том же сегменте VLAN `<vlan-id>`.
	
	Вернуть значение по-умолчанию - 255 секунд.

`ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>`
 	
`no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>`
 	
В режиме глобальной конфигурации
	Задать статическую подписку на группу `<A.B.C.D>` от источника `[source <A.B.C.D>]` на интерфейс `<IFNAME>` для VLAN `<vlan-id>`.
	
	Удалить указанную статическую подписку на группу.

`ip igmp snooping vlan <vlan-id> report source-address <A.B.C.D>`
 	
`no ip igmp snooping vlan <vlan-id> report source-address`
 	
В режиме глобальной конфигурации
	Задать IP-адрес источника `<A.B.C.D>` для пересылаемых сообщений IGMP-join для VLAN `<vlan-id>`
	Удалить IP-адрес источника для пересылаемых сообщений IGMP-join

`ip igmp snooping vlan <vlan-id> specific-query-mrsp <value>`
 	
`no ip igmp snooping vlan <vlan-id> specific-query-mrsp`
 	
В режиме глобальной конфигурации
	Задать максимальное время ответа на Membership Query `<value>` в секундах для VLAN `<vlan-id>`
	
	Восстановить значение по-умолчанию - 1 секунда.

46.3 Пример настройки IGMP Snooping

Сценарий №1: IGMP Snooping

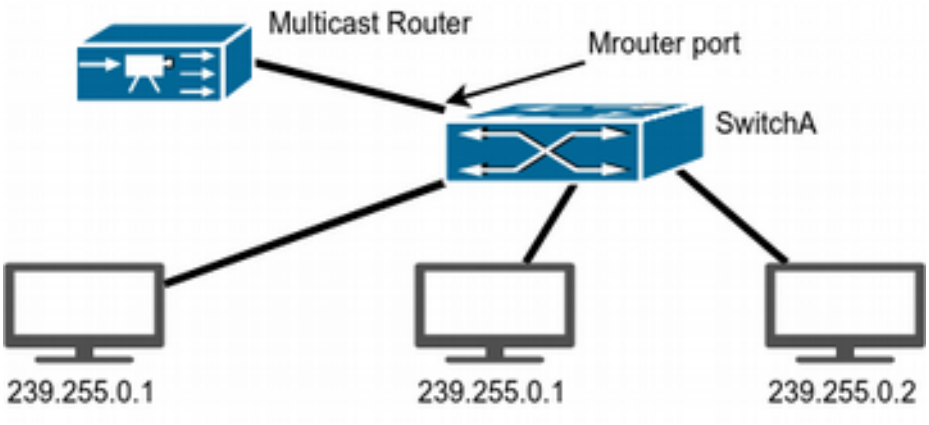


Рисунок 21-1 IGMP Snooping

Как показано на рисунке 22-1, порты коммутатора 1, 2, 6, 10 и 12 добавлены во VLAN 100 на коммутаторе. Multicast маршрутизатор подключен к порту 1, а 4 хоста к остальным портам 2, 6, 10 и 12 соответственно. Поскольку IGMP Snooping по-умолчанию отключен, он должен быть включен сначала глобально, а затем и для VLAN 100. Кроме того, порт 1 должен быть выбран в качестве Mrouter порта для VLAN 100. Эти настройки можно осуществить следующим образом:

```
SwitchA(config)#ip igmp snooping
SwitchA(config)#ip igmp snooping vlan 100
SwitchA(config)#ip igmp snooping vlan 100 mrouter interface ethernet
1/0/1
```

Предположим, что сервер вещает 2 потока с использованием групповых адресов 239.255.0.1 и 239.255.0.2. Хосты из портов 2 и 3 подписались на группу 239.255.0.1, а хост из порта 6 - на группу 239.255.0.2.

Во время подписки IGMP Snooping создаст таблицу, которая будет содержать соответствие портов 2 и 3 группе 239.255.0.1, а порта 6 - группе 239.255.0.2, в результате каждый порт получит трафик только тех групп, которую он запросил и не получит трафик других групп, но каждый порт сможет получить трафик любой их групп, запросив её.

Сценарий №2: IGMP Querier

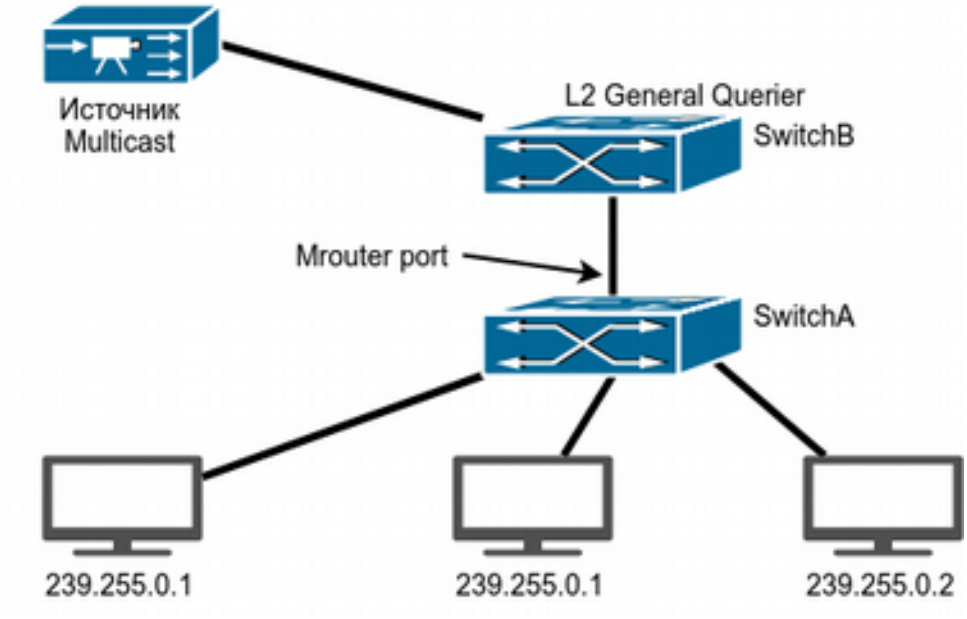


Рисунок 46-2 IGMP Querier

Схема, изображенная на Рисунке 46-1, претерпела изменения: вместо Multicast маршрутизатора подключен источник мультикаст трафика, а между ним и SwitchA подключен коммутатор SwitchB, выполняющий роль IGMP Querier. Но подписчики, источник и порты между ними также принадлежат к VLAN 100.

Конфигурация SwitchA такая же, как и в предыдущем примере. Конфигурация SwitchB будет выглядеть следующим образом:

```
SwitchA#config
SwitchA(config)#ip igmp snooping
SwitchA(config)#ip igmp snooping vlan 100
SwitchA(config)#ip igmp snooping vlan 100 L2-general-querier
```

46.4 Решение проблем с настройкой IGMP Snooping

При настройке и использовании IGMP Snooping могут возникнуть проблемы из-за физического соединения, а также некорректной настройки. Поэтому проверьте следующее:

- Убедитесь, что физическое соединение присутствует;
- Убедитесь, что IGMP Snooping включен как глобально, так и в нужном VLAN;
- Убедитесь, что mrouter порт присутствует;
- Используйте команду `show ip igmp snooping vlan <vlan_id>` для проверки сконфигурированных параметров, а также записей в таблице IGMP Snooping.

47 Аутентификация IGMP Snooping

47.1 Общие сведения о аутентификации IGMP Snooping

Функционал аутентификации для IGMP Snooping используется для контроля доступа пользователей к multicast-группам. При попытке пользователя запросить доступ к multicast-группе, коммутатор запрашивает аутентификацию у RADIUS-сервера. Если коммутатор получит Request-Accept от сервера, он добавит подписку пользователя на группу.

47.2 Настройка аутентификации IGMP Snooping

1. Включить IGMP Snooping
2. Включить аутентификацию для IGMP Snooping
3. Настроить аутентификацию для IGMP Snooping
4. Настроить RADIUS

1. Включить IGMP Snooping:

Команда	Описание

`ip igmp snooping`
`no ip igmp snooping`
 	
В режиме глобальной конфигурации
	Включить IGMP Snooping
	Отключить IGMP Snooping

2. Включить аутентификацию для IGMP Snooping:

Команда	Описание
`igmp snooping authentication enable`	Включить функцию аутентификации IGMP Snooping. После включения этой функции коммутатор запросит аутентификацию для всех существующих записей клиент-группа. Записи, не прошедшие аутентификацию, будут удалены.
`no igmp snooping authentication enable` В режиме глобальной конфигурации	Отключить функцию аутентификации IGMP Snooping

3. Настроить аутентификацию для IGMP Snooping:

Команда	Описание

`igmp snooping authentication free-rule access-list <6000-7999>`
 	
`no igmp snooping authentication free-rule access-list <6000-7999>`
 	
В режиме конфигурирования интерфейса
	Задать группы в виде ACL, аутентификация пользователей для которых не потребуется. Команда **no** отменяет это действие.

`ip igmp snooping authentication radius none`
`no ip igmp snooping authentication radius none`
 	
В режиме глобальной конфигурации
	Разрешить добавление подписки на группу, если RADIUS-сервер не отвечает. Команда `no` отменяет это действие.

`ip igmp snooping authentication forwarding-first`
`no ip igmp snooping authentication forwarding-first`
 	
В режиме глобальной конфигурации
	Настроить порядок процессов процедуры аутентификации. После применения команды запись в таблицу IGMP-snooping будет добавлена перед аутентификацией, если аутентификация будет неуспешна, запись будет удалена. Команда `no` возвращает конфигурацию по-умолчанию - аутентификация выполняется перед добавлением записи.

`ip igmp snooping authentication timeout <30-30000>`
 	
`no ip igmp snooping authentication timeout`
 	
В режиме глобальной конфигурации
	Задать время жизни записи аутентификации `<30-30000>` в секундах.
	Восстановить значение по-умолчанию (600 секунд).

4. Настроить RADIUS:

Команда	Описание

`aaa enable`
`no aaa enable`
 	
В режиме глобальной конфигурации
	Включить функцию AAA
	Отключить функцию AAA

`radius-server key <word>`
 	
`no radius-server key`
 	
В режиме глобальной конфигурации
	Указать ключ `key <word>` для RADIUS-сервера
	Удалить настроенный ключ `key` для RADIUS-сервера

`radius-server authentication host <A.B.C.D>`
`no radius-server authentication host <A.B.C.D>`
 	
В режиме глобальной конфигурации
	Задать адрес RADIUS-сервера
	
	Удалить адрес RADIUS-сервера

47.3 Пример настройки аутентификации IGMP Snooping

На коммутаторе настроен VLAN1 для порта 1/0/1 и VLAN10 для порта 1/0/2. Пользователь подключен к порту 1/0/1, а RADIUS-сервер к порту 1/0/2. Для контроля многоадресных групп разрешенных пользователю в соответствии с политикой, требуется настроить аутентификацию для IGMP Snooping. RADIUS-сервер имеет адрес 10.1.1.3/24, для связи с ним коммутатору будет назначен адрес из этой подсети.
Конфигурация будет происходить следующим образом:

```
Switch#config
Switch(config)#ip igmp snooping
Switch(config)#ip igmp snooping vlan 1
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#igmp snooping authentication enable
Switch(config-if-ethernet1/0/1)# exit
Switch(config)#ip igmp snooping authentication radius none
Switch(config)#interface vlan 10
Switch(config-if-vlan10)#ip address 10.1.1.2 255.255.255.0
Switch(config-if-vlan10)# exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
```

48 MLD Snooping

48.1 Общие сведения о MLD Snooping

MLD - Multicast Listener Discovery Protocol - протокол определения получателей многоадресных потоков, использующийся в IPv6. Аналогичную роль в IPv4 выполняет протокол IGMP. Данный коммутатор поддерживает протокол MLD версии 2.

48.2 Настройка MLD Snooping

1. Включить функцию MLD Snooping;
2. Настроить функцию MLD Snooping.

1. Включить функцию MLD Snooping:

Команда	Описание

`ipv6 mld snooping`
`no ipv6 mld snooping`
 	
В режиме глобальной конфигурации
	Включить MLD Snooping
	Отключить MLD Snooping

2. Настроить функцию MLD Snooping:

Команда	Описание

`ipv6 mld snooping vlan <vlan-id>`
 	
`no ipv6 mld snooping vlan <vlan-id>`
 	
В режиме глобальной конфигурации
	Включить IGMP Snooping для VLAN `<vlan-id>`
	
	Отключить IGMP Snooping для VLAN `<vlan-id>`

`ipv6 mld snooping vlan <vlan-id> limit {group <g_limit> | source <s_limit>}`
 	
`no ipv6 mld snooping vlan <vlan-id> limit`
 	
В режиме глобальной конфигурации
	Задать максимальное количество групп `group <1-65535>` или источников для групп `source <1-65535>` для VLAN `<vlan-id>`
	
	Восстановить значения по-умолчанию: `group <1-65535>` - 50, `source <1-65535>` - 40

`ipv6 mld snooping vlan <vlan-id> l2-general-querier` `no ipv6 mld snooping vlan <vlan-`	Включить функцию L2 General-Querier для VLAN `<vlan-id>` Выключить функцию L2 General-Querier

id> l2-general-querier В режиме глобальной конфигурации	для VLAN <vlan-id>
ipv6 mld snooping vlan <vlan-id> mrouter-port interface <interface -name> no ipv6 mld snooping vlan <vlan-id> mrouter-port interface <interface -name> В режиме глобальной конфигурации	Задать Mrouter порт <interface -name> для <vlan-id> Удалить Mrouter порт <interface -name> для <vlan-id>
ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6 no ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6 В режиме глобальной конфигурации	Включить динамическое добавление Mrouter порта для VLAN <vlan-id>, из которого получены PIM-пакеты. Команда no отменяет это действие.
ipv6 mld snooping vlan <vlan-id> mrpt <value> no ipv6 mld snooping vlan <vlan-id> mrpt В режиме глобальной конфигурации	Задать максимальное время жизни в секундах <value> Mrouter-порта, определенного динамически для <vlan-id>. Восстановить значение <value> по-умолчанию - 255 секунд.
ipv6 mld snooping vlan <vlan-id> query-interval <value> no ipv6 mld snooping vlan <vlan-id> query-interval В режиме глобальной конфигурации	Задать интервал отправки <value> в секундах MLD query для <vlan-id>. Восстановить значение <value> по-умолчанию - 125 секунд.
ipv6 mld snooping vlan <vlan-id> immediate-leave no ipv6 mld snooping vlan <vlan-id> immediate-leave В режиме глобальной конфигурации	Включить функцию быстрого удаления подписки на группу для <vlan-id> Выключить функцию быстрого удаления подписки на группу для VLAN <vlan-id>
ipv6 mld snooping vlan <vlan-id> query-mrsp <value>	Задать максимальное время ответа на General Query <value> в секундах для VLAN <vlan-id>

`no ipv6 mld snooping vlan <vlan-id> query-mrsp` В режиме глобальной конфигурации	Восстановить значение по-умолчанию - 10 секунд

`ipv6 mld snooping vlan <vlan-id> query-robustness <value>`
 	
`no ipv6 mld snooping vlan <vlan-id> query-robustness`
 	
В режиме глобальной конфигурации
	Задать количество `<value>` MLD Query без ответа, после отправки которых коммутатор удалит запись MLD snooping для VLAN `<vlan-id>`.
	Восстановить значение по-умолчанию - 2.

`ipv6 mld snooping vlan <vlan-id> suppression-query-time <value>`
 	
`no ipv6 mld snooping vlan <vlan-id> suppression-query-time`
 	
В режиме глобальной конфигурации
	Задать время подавления Querier `<value>` в секундах при получении query в том же сегменте VLAN `<vlan-id>`.
	Вернуть значение по-умолчанию - 255 секунд.

`Ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source <X:X::X:X>] interface [ethernet | port-channel] <IFNAME>`
 	
`no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source <X:X::X:X>] interface [ethernet | port-channel] <IFNAME>`
 	
В режиме глобальной конфигурации
	Задать статическую подписку на группу `<X:X::X:X>` от источника `[source <X:X::X:X>]` на интерфейс `<IFNAME>` для VLAN `<vlan-id>`.
	
	Удалить указанную статическую подписку на группу.

48.3 Пример конфигурации MLD Snooping

Сценарий №1: IGMP Snooping

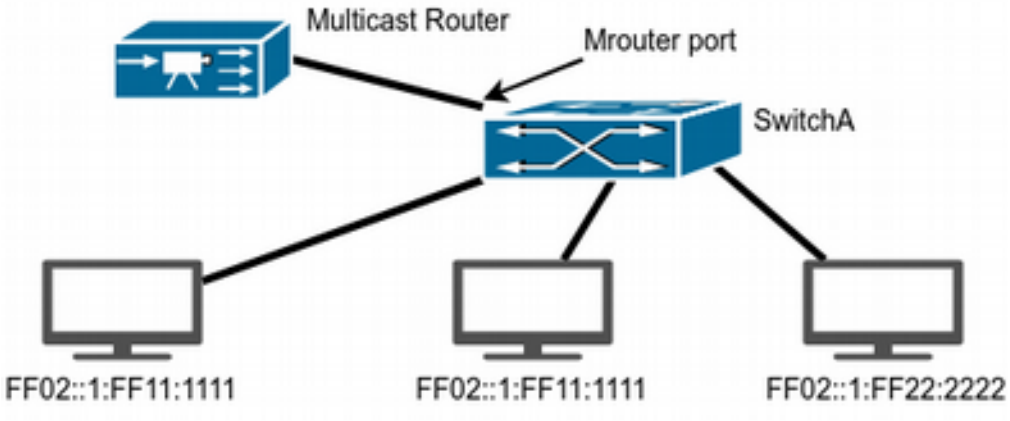


Рисунок 48-1 MLD Snooping

Как показано на рисунке 48-1, порты коммутатора 1, 2, 6, 10 и 12 добавлены во VLAN 100 на коммутаторе. Multicast маршрутизатор подключен к порту 1, а 4 хоста к остальным портам 2, 6, 10 и 12 соответственно. Поскольку IGMP Snooping по-умолчанию отключен, он должен быть включен сначала глобально, а затем и для VLAN 100. Кроме того, порт 1 должен быть выбран в качестве Mrouter порта для VLAN 100. Эти настройки можно осуществить следующим образом:

```
SwitchA(config)#ipv6 mld snooping
SwitchA(config)#ipv6 mld snooping vlan 100
SwitchA(config)#ipv6 mld snooping vlan 100 mrouter interface ethernet
1/0/1
```

Предположим, что сервер вещает 2 потока с использованием групповых адресов FF02::1:FF11:1111 и FF02::1:FF22:2222. Хосты из портов 2 и 3 подписались на группу FF02::1:FF11:1111, а хост из порта 6 - на группу 239.255.0.2.

Во время подписки IGMP Snooping создаст таблицу, которая будет содержать соответствие портов 2 и 3 группе FF02::1:FF11:1111, а порта 6 - группе FF02::1:FF22:2222, в результате каждый порт получит трафик только тех групп, которую он запросил и не получит трафик других групп, но каждый порт сможет получить трафик любой их групп, запросив её.

Сценарий №2: IGMP Querier

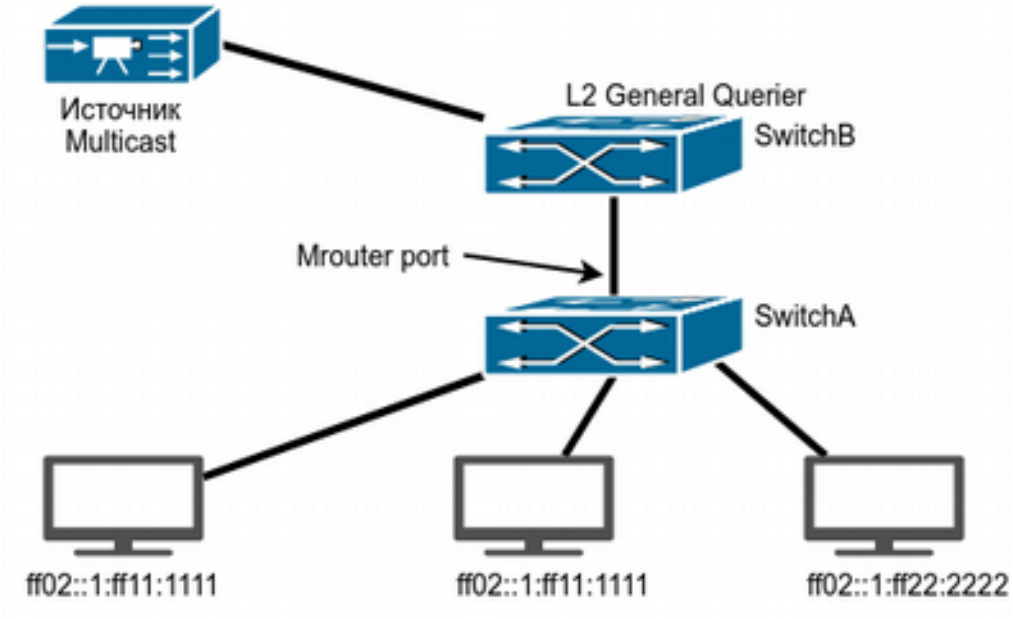


Рисунок 48-2 MLD Querier

Схема, изображенная на Рисунке 48-1, претерпела изменения: вместо Multicast маршрутизатора подключен источник мультикаст трафика, а между ним и SwitchA подключен коммутатор SwitchB, выполняющий роль IGMP Querier. Но подписчики, источник и порты между ними также принадлежат к VLAN 100.

Конфигурация SwitchA такая же, как и в предыдущем примере. Конфигурация SwitchB будет выглядеть следующим образом:

```
SwitchA#config
SwitchA(config)#ipv6 mld snooping
SwitchA(config)#ipv6 mld snooping vlan 100
SwitchA(config)#ipv6 mld snooping vlan 100 L2-general-querier
```

48.4 Решение проблем с конфигураци MLD Snooping

При настройке и использовании MLD Snooping могут возникнуть проблемы из-за физического соединения, а также некорректной настройки. Поэтому проверьте следующее:

- Убедитесь, что физическое соединение присутствует;
- Убедитесь, что IGMP Snooping включен как глобально, так и в нужном VLAN;
- Убедитесь, что на данном коммутаторе сконфигурирован L2 general querier или mrouter порт присутствует;
- Используйте команду `show ipv6 mld snooping vlan <vlan_id>` для проверки сконфигурированных параметров.

49 Multicast VLAN

49.1 Общие сведения о Multicast VLAN

В случае, если получатели Multicast трафика находятся в разных VLAN, в каждом VLAN создается своя копия одного и того же трафика, что может сказаться на свободной полосе пропускания каналов. Проблему решает Multicast VLAN - технология которая позволяет серверу передавать мультикастовый поток в одном VLAN'е, в то время как конечные пользователи смогут получать его, находясь в различных VLAN'ах, подключаясь к одному Multicast VLAN. Пользователи подключаются к мультикастовой рассылке и отсоединяются от нее, используя функционал IGMP\MLD snooping. Это позволяет не передавать multicast поток во все пользовательские VLAN и экономить ресурсы оборудования.

49.2 Настройка Multicast VLAN

Команда	Описание
multicast-vlan no multicast-vlan В режиме конфигурирования VLAN	Назначить текущий VLAN в качестве Multicast VLAN. Команда no отменяет это действие.
multicast-vlan association <vlan-id> no multicast-vlan association <vlan-id> В режиме конфигурирования VLAN	Ассоциировать VLAN <vlan-list> с данным Multicast VLAN Отменить ассоциацию VLAN <vlan-list> с данным Multicast VLAN
multicast-vlan association interface (ethernet | port-channel|) IFNAME no multicast-vlan association interface (ethernet | port-channel|) IFNAME В режиме конфигурирования VLAN	Ассоциировать данный Multicast VLAN с интерфейсом IFNAME Отменить ассоциацию данного Multicast VLAN с интерфейсом IFNAME
multicast-vlan mode {dynamic| compatible} no multicast-vlan mode {dynamic| compatible} В режиме конфигурирования VLAN	Выбрать режим работы Multicast VLAN: compatible - коммутатор не передает join в mrouter port, трафик в него принимается всегда; dynamic - коммутатор не добавит mrouter порт при создании подписки. Команда no

	восстанавливает конфигурацию по-умолчанию умолчанию коммутатор добавить mrouter порт и передаст в него join.

`switchport association multicast-vlan <vlan-id> [out-tag]`
`no switchport association multicast-vlan <vlan-id>`
 	
В режиме конфигурирования интерфейса
	Настроить ассоциацию интерфейса с Multicast VLAN `<vlan-id>`. Команда `[out-tag]` позволяет добавить тэг 802.1q к исходящему Multicast трафику из Multicast VLAN `<vlan-id>` в данный порт.
	Команда `no` отменяет ассоциацию данного интерфейса с Multicast VLAN.
	
	Данная команда заменяет команды в режиме конфигурирования VLAN `multicast-vlan association <vlan-id>` и `multicast-vlan association interface (ethernet | port-channel|) IFNAME`

49.3 Пример настройки Multicast VLAN

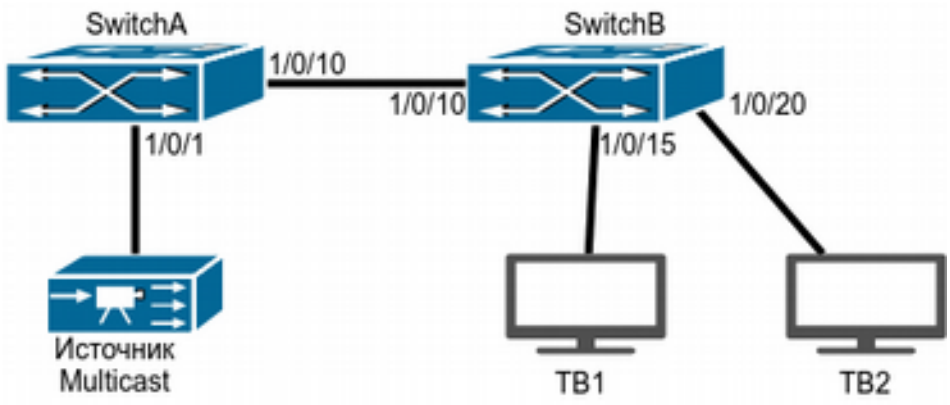


Рисунок 49.1 Настройка Multicast VLAN

Как показано на рисунке 49.1, источники Mutlicast-трафика подключен к коммутатору уровня 3 - SwitchA через порт 1/0/1 которому назначен VLAN10. SwitchA подключен к коммутатору уровня 2 SwitchB через порт 1/0/10, который настроен в режим trunk. К коммутатору SwitchB подключены хосты пользователей TB1 и TB2: TB1 подключен к порту 1/0/15, который принадлежит VLAN 100, а TB2 подключен к порту 1/0/20, который принадлежит VLAN 101. SwitchB подключен к SwitchA через порт 1/0/10. VLAN 20 настроен как Multicast VLAN.

Следующий пример конфигурации предполагает, что IP-адреса интерфейсов уже

сконфигурированы и другое оборудование настроено корректно:

```
SwitchA#config
SwitchA(config)#vlan 10
SwitchA(config-vlan10)#switchport access ethernet 1/0/1
SwitchA(config-vlan10)exit
SwitchA(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip pim dense-mode
Switch(Config-if-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan20)#exit
SwitchA(config)#interface vlan 20
SwitchA(Config-if-Vlan20)#ip pim dense-mode
SwitchA(Config-if-Vlan20)#exit
SwitchA(config)#ip pim multicast
SwitchA(config)# interface ethernet1/0/10
SwitchA(Config-If-Ethernet1/0/10)switchport mode trunk

SwitchB#config
SwitchB(config)#vlan 100
SwitchB(config-vlan100)#Switchport access ethernet 1/0/15
SwitchB(config-vlan100)exit
SwitchB(config)#vlan 101
SwitchB(config-vlan101)#Switchport access ethernet 1/0/20
SwitchB(config-vlan101)exit
SwitchB(config)# interface ethernet 1/0/10
SwitchB(Config-If-Ethernet1/0/10)#switchport mode trunk
SwitchB(Config-If-Ethernet1/0/10)#exit
SwitchB(config)#vlan 20
SwitchB(config-vlan20)#multicast-vlan
SwitchB(config-vlan20)#multicast-vlan association 100,101
SwitchB(config-vlan20)#exit
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 20
```

50 ACL

50.1 Общие сведения об ACL

ACL (Access Control List, список контроля доступа) - это механизм фильтрации IP-пакетов, позволяющий контролировать сетевой трафик, разрешая или запрещая прохождение пакетов на основе заданных признаков. Пользователь может самостоятельно задать критерии фильтрации ACL и применить фильтр на входящее по отношению к коммутатору направление трафика.

Access-list - последовательный набор правил. Каждое правило состоит из информации о фильтре и действии при обнаружении соответствия правилу. Информация, включенная в правило, представляет собой эффективную комбинацию таких условий, как исходный IP-адрес, IP-адрес получателя, номер протокола IP и порт TCP, порт UDP.

Списки доступа можно классифицировать по следующим критериям:

- Критерий на основе информации о фильтре: IP ACL (фильтр на основе информации уровня 3 или выше), MAC ACL (уровня 2) и MAC-IP ACL (уровень 2 или уровень 3 или выше).
- Критерий сложности конфигурации: стандартный (standard) и расширенный (extended), расширенный режим позволяет создавать более точные фильтры.
- Критерий на основе номенклатуры: нумерованный или именованный.

Описание ACL должен охватывать три вышеупомянутые аспекта.

Access-group - это описание привязки ACL к входящему направлению трафика на конкретном интерфейсе. Если группа доступа создана, все пакеты из входящего направления через интерфейс будут сравниваться с правилом ACL.

ACL может содержать два действия правила и действия по умолчанию: «разрешение» (permit) или «отказ»(deny). Access-list может состоять из нескольких правил. Фильтр сравнивает условия пакета с правилами, начиная с первого, до первого совпадения, остальные правила не будут обработаны. Глобальное действие по умолчанию применяется только в том случае, если ACL применен на интерфейсе, но в нем нет правил, либо для полученного пакета нет совпадений.

50.2 Настройка ACL

1. Настроить Access-list:
    1. Настроить нумерованный standard IP access-list;
    2. Настроить нумерованный extended IP access-list;
    3. Настроить именованный standard IP access-list:
        i. Создать именованный standard IP access-list;
        ii. Создать permit и\или deny правила;
    4. Настроить именованный extended IP access-list;
        i. Создать именованный extended IP access-list;
        ii. Создать permit и\или deny правила;
    5. Настроить нумерованный standard MAC access-list;
    6. Настроить нумерованный extended MAC access-list;
    7. Настроить именованный extended MAC access-list:
        i. Создать именованный extended MAC access-list;
        ii. Создать permit и\или deny правила;
    8. Настроить нумерованный extended MAC-IP access-list;

9. Настроить именованный extended MAC-IP access-list;
    i. Создать именованный extended MAC-IP access-list;
    ii. Создать permit и\или deny правила;
10. Настроить нумерованный standard IPv6 access-list;
11. Настроить именованный standard IPv6 access-list;
    i. Создать именованный standard IPv6 access-list;
    ii. Создать permit и\или deny правила;

2. Включить функцию фильтрации пакетов
3. Настроить временной период действия
4. Настроить access-group
5. Просмотр статистики ACL

1. Настроить Access-list:
    1. Настроить нумерованный standard IP access-list;

Команда	Описание

`access-list <num> {deny | permit} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}}`
 	
`no access-list <num>`
В режиме глобальной конфигурации
	Создать нумерованный standard IP access-list `<num>`, если данный access-list уже создан, правило будет добавлено в данный ACL.
	Удалить ACL `<num>`

    2. Настроить нумерованный extended IP access-list;

Команда	Описание
`access-list <num> {deny | permit} icmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>][time-range<time-range-name>]` В режиме глобальной конфигурации	Создать правило протокола ICMP для нумерованного extended IP access-list. Если ACL не был создан ранее, он будет создан после применения данной команды.
`access-list <num> {deny | permit} igmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>]`	Создать правило протокола IGMP для нумерованного extended IP access-list. Если ACL не был создан ранее, он будет создан после применения данной команды.

В режиме глобальной конфигурации	
access-list <num> {deny | permit} tcp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range<time-range-name>] В режиме глобальной конфигурации	Создать правило протокола TCP для нумерованного extended IP access-list. Если ACL не был создан ранее, он будет создан после применения данной команды.
access-list <num> {deny | permit} udp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [precedence <prec>] [tos <tos>][time-range<time-range-name>] В режиме глобальной конфигурации	Создать правило протокола UDP для нумерованного extended IP access-list. Если ACL не был создан ранее, он будет создан после применения данной команды.
access-list <num> {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num>} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>] В режиме глобальной конфигурации	Создать правило других протоколов, либо для всех IP протоколов для нумерованного extended IP access-list. Если ACL не был создан ранее, он будет создан после применения данной команды.
no access-list <num> В режиме глобальной конфигурации	Удалить нумерованный ACL

3. Настроить именованный standard IP access-list:
   i. Создать именованный standard IP access-list;

Команда	Описание

`ip access-list standard <name>`
 	
`no ip access-list standard <name>`
 	
В режиме глобальной конфигурации
	Создать именованный standard IP access-list `<name>`, если данный access-list уже создан, правило будет добавлено в данный ACL. Войти в режим конфигурирования созданного ACL `<name>`.
	Удалить ACL `<name>`

ii. Создать permit и\или deny правила;

Команда	Описание
`[no] {deny | permit} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}}` В режиме конфигурации ACL	Создать правило для текущего ACL. Команда `[no]` удаляет это правило.

4. Настроить именованный extended IP access-list;
   i. Создать именованный extended IP access-list;

Команда	Описание
ip access-list extended <name> no ip access-list extended <name> В режиме глобальной конфигурации	Создать именованный extended IP access-list `<name>`, войти в режим конфигурирования созданного ACL `<name>`. Удалить ACL `<name>`

ii. Создать permit и\или deny правила;

Команда	Описание
`[no] {deny | permit} icmp {{<sIpAddr>`	Создать правило

<sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>] [time-range<time-range-name>] В режиме конфигурации ACL	протокола ICMP для текущего ACL. Команда **[no]** удаляет это правило.
[no] {deny | permit} igmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>] [time-range<time-range-name>] В режиме конфигурации ACL	Создать правило протокола IGMP для текущего ACL. Команда [no] удаляет это правило.
[no] {deny | permit} tcp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range<time-range-name>] В режиме конфигурации ACL	Создать правило протокола TCP для текущего ACL. Команда [no] удаляет это правило.
[no] {deny | permit} udp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [precedence <prec>] [tos <tos>][time-range<time-range-name>] В режиме конфигурации ACL	Создать правило протокола UDP для текущего ACL. Команда [no] удаляет это правило.

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num>} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>] [time-range<time-range-name>] В режиме конфигурации ACL	Создать правило других протоколов, либо для всех IP протоколов для текущего ACL. Команда [no] удаляет это правило.

5. Настроить нумерованный standard MAC access-list;

Команда	Описание
access-list<num>{deny|permit} {any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} no access-list <num> В режиме глобальной конфигурации	Создать нумерованный standard MAC access-list <num>, если данный access-list уже создан, правило будет добавлено в данный ACL. Удалить ACL <num>

6. Настроить нумерованный extended MAC access-list;

Команда	Описание
access-list<num> {deny|permit} {any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac| {host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}}[untagged-eth2 | tagged-eth2 | untagged-802-3 | tagged-802-3] no access-list <num> В режиме глобальной конфигурации	Создать нумерованный extended MAC access-list <num>, если данный access-list уже создан, правило будет добавлено в данный ACL. Удалить ACL <num>

7. Настроить именованный extended MAC access-list:
   i. Создать именованный extended MAC access-list;

Команда	Описание
mac-access-list extended <name> no mac-access-list extended <name> В режиме глобальной конфигурации	Создать именованный extended MAC access-list <name>, войти в режим конфигурирования созданного ACL <name>. Удалить ACL <name>

ii. Создать permit и\или deny правила;

Команда	Описание
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>} |{<dmac><dmac-mask>}} [cos <cos-val> [<cos-bitmask>] [vlanId <vid-value> [<vid-mask>] [ethertype<protocol>[<protocol-mask>]]]] В режиме конфигурации ACL	Создать правило именованного extended MAC ACL для поиска соответствия поля Cos 802.1p и Vlanid. Команда [no] отменяет это правило.
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}}[untagged-eth2 [ethertype <protocol> [protocol-mask]]] В режиме конфигурации ACL	Создать правило именованного extended MAC ACL для поиска соответствия кадру ethernet 2 без тэга vlan. Команда [no] отменяет это правило.
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}} [untagged-802-3] В режиме конфигурации ACL	Создать правило именованного extended MAC ACL для поиска соответствия кадру 802.3 без тэга vlan. Команда [no] отменяет это правило.
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-	Создать правило именованного extended MAC ACL для поиска

destination-mac<host_dmac>}|{<dmac><dmac-mask>}}[tagged-eth2 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype<protocol> [<protocol-mask>]]] В режиме конфигурации ACL	соответствия кадру ethernet 2 с тэгом vlan. Команда [no] отменяет это правило.
[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}} [tagged-802-3 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]]] В режиме конфигурации ACL	Создать правило именованного extended MAC ACL для поиска соответствия кадру 802.3 с тэгом vlan. Команда [no] отменяет это правило.

8. Настроить нумерованный extended MAC-IP access-list;

Команда	Описание
access-list<num>{deny|permit} {any-source-mac| {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac><dmac-mask>}} icmp {{<source> <source-wildcard>} |any-source| {host-source <source-host-ip>}} {{<destination> <destination-wildcard>} | any-destination | {host-destination <destination-host-ip>}} [<icmp-type> [<icmp-code>]] [precedence <precedence>] [tos <tos>] [time-range <time-range-name>] В режиме глобальной конфигурации	Создать MAC-ICMP правило для нумерованного extended MAC-IP ACL. Если ACL не был создан ранее, он будет создан после применения данной команды.
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}| {<dmac><dmac-mask>}}igmp {{<source><source-wildcard>}|any-	Создать MAC-IGMP правило для нумерованного extended MAC-IP ACL. Если ACL не был создан ранее, он будет создан после применения данной команды.

source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>] В режиме глобальной конфигурации	
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}| {<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port {<port1> | range <sPortMin> <sPortMax>}] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port {<port3> | range <dPortMin> <dPortMax>}] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>] [time-range<time-range-name>] В режиме глобальной конфигурации	Создать MAC-TCP правило для нумерованного extended MAC-IP ACL. Если ACL не был создан ранее, он будет создан после применения данной команды.
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}| {<dmac><dmac-mask>}}udp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port {<port1> | range <sPortMin> <sPortMax>}] {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [d-port {<port3> | range <dPortMin> <dPortMax>}] [precedence <precedence>] [tos <tos>][time-range<time-range-	Создать MAC-UDP правило для нумерованного extended MAC-IP ACL. Если ACL не был создан ранее, он будет создан после применения данной команды.

name>] В режиме глобальной конфигурации	
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}| {<dmac><dmac-mask>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<protocol-num>}} {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [precedence <precedence>] [tos <tos>] [time-range<time-range-name>] В режиме глобальной конфигурации	Создать правило для других протоколов, либо для всех IP протоколов для нумерованного extended MAC-IP ACL. Если ACL не был создан ранее, он будет создан после применения данной команды.
no access-list <num> В режиме глобальной конфигурации	Удалить нумерованный ACL

9. Настроить именованный extended MAC-IP access-list;
   i. Создать именованный extended MAC-IP access-list;

Команда	Описание
mac-ip-access-list extended <name> no mac-ip-access-list extended <name> В режиме глобальной конфигурации	Создать именованный extended MAC-IP access-list <name>, войти в режим конфигурирования созданного ACL <name>. Удалить ACL <name>

   ii. Создать permit и\или deny правила;

Команда	Описание
[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-	Создать MAC-ICMP правило для нумерованного extended

mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}| {<dmac><dmac-mask>}}icmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}| any-destination| {host-destination <destination-host-ip>}} [<icmp-type> [<icmp-code>]] [precedence <precedence>] [tos<tos>][time-range<time-range-name>] В режиме конфигурации ACL	MAC-IP ACL. Команда [no] удаляет это правило.
[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}| {<dmac><dmac-mask>}}igmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}| any-destination| {host-destination <destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>] [time-range<time-range-name>] В режиме конфигурации ACL	Создать MAC-IGMP правило для нумерованного extended MAC-IP ACL. Команда [no] удаляет это правило.
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}| {<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port {<port1> | range <sPortMin> <sPortMax>}] {{<destination><destination-wildcard>}| any-destination| {host-destination <destination-host-ip>}} [d-port {<port3> | range <dPortMin> <dPortMax>}] [ack+fin+psh+rst+urg+syn] [precedence<precedence>][tos<tos>][time-range<time-range-name>] В режиме конфигурации ACL	Создать MAC-TCP правило для нумерованного extended MAC-IP ACL. Команда [no] удаляет это правило.

[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}udp {{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}} [s-port {<port1> | range <sPortMin> <sPortMax>}] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port {<port3> | range <dPortMin> <dPortMax>}] [precedence <precedence>] [tos <tos>] [time-range<time-range-name>] В режиме конфигурации ACL	Создать MAC-UDP правило для нумерованного extended MAC-IP ACL. Команда [no] удаляет это правило.
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<protocol-num>}} {{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [precedence<precedence>][tos<tos>][time-range<time-range-name>] В режиме конфигурации ACL	Создать правило для других протоколов, либо для всех IP протоколов для нумерованного extended MAC-IP ACL. Команда [no] удаляет это правило.

10. Настроить нумерованный standard IPv6 access-list;

Команда	Описание
ipv6 access-list <num> {deny | permit} {{<sIPv6Addr> <sPrefixlen>} | any-source | {host-source <sIpv6Addr>}} no ipv6 access-list <num> В режиме глобальной конфигурации	Создать нумерованный standard ACL для IPv6. Если ACL был создан ранее, правило будет добавлено к данному ACL. Удалить данный ACL

11. Настроить именованный standard IPv6 access-list;
    i. Создать именованный standard IPv6 access-list;

Команда	Описание

`ipv6 access-list standard <name>`
 	
`no ipv6 access-list standard <name>`
 	
В режиме глобальной конфигурации
	Создать именованный standard ACL для IPv6.
	
	Удалить именованный standard ACL для IPv6.

    ii. Создать permit и\или deny правила;

Команда	Описание
`[no] {deny | permit} {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr> }}` В режиме конфигурации ACL	Создать правило именованного standard ACL для IPv6. Команда `[no]` удаляет это правило

2. Включить функцию фильтрации пакетов

Команда	Описание

`firewall enable`
 	
`firewall disable`
 	
В режиме глобальной конфигурации
	Включить функцию фильтрации пакетов
	
	Выключить функцию фильтрации пакетов

3. Настроить временной период действия

Команда	Описание
`time-range <time_range_name>`	Создать временной период `<time_range_name>`

`time-range <time_range_name>` В режиме глобальной конфигурации	Удалить временной период `<time_range_name>`
`[no] absolute-periodic {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <start_time> to {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <end_time>` В режиме конфигурации time-range	Задать периодичность действия текущего временного периода. Команда `[no]` удаляет эту периодичность.
`[no] periodic {{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday} | daily | weekdays | weekend} <start_time> to <end_time>` В режиме конфигурации time-range	Задать период действия текущего временного периода. Команда `[no]` удаляет эту периодичность.
`[no] absolute start <start_time> <start_data> [end <end_time> <end_data>]` В режиме конфигурации time-range	Задать время активации текущего временного периода действия и время его окончания. Команда `[no]` удалит настроенное время активации

4. Настроить access-group

Команда	Описание

`{ip|ipv6|mac|mac-ip} access-group <acl-name> in [traffic-statistic]`
 	
`no {ip|ipv6|mac|mac-ip} access-group <acl-name> {in}`
 	
В режиме конфигурации интерфейса
	Применить ACL `<acl-name>` на входящее направление трафика на интерфейсе. С включенной опцией `traffic-statistic` коммутатор будет подсчитывать совпадения этой `access-group`
	Удалить ACL `<acl-name>` с интерфейса

5. Просмотр статистики ACL

Команда	Описание
`show access-group statistic [ethernet <interface-name> ]`	Посмотреть статистику трафика, прошедшего через `access-group` интерфейса `ethernet <interface-name>`
`clear access-group statistic [ethernet <interface-name> ]` В привилегированном режиме	Очистить статистику трафика, прошедшего через `access-group` интерфейса `ethernet <interface-name>`

50.3 Пример настройки ACL

Сценарий 1: порт 1/0/10 относится к сегменту 10.0.0.0/24, протокол FTP не разрешен пользователю.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-
destination d-port 21
Switch(config)#firewall enable
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#ip access-group 110 in
```

Проверка результата применения конфигурации:

```
Switch#show firewall
      Firewall status: enable.

Switch#show access-lists
      access-list 110(used 1 time(s)) 1 rule(s)
      access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-
      port 21

Switch#show access-group interface ethernet 1/0/10
      interface name:Ethernet1/0/10
            the ingress acl use in firewall is 110, traffic-statistics
      Disable.
```

Сценарий 2: Коммутатор должен отбрасывать кадры 802.3 в интерфейсе 1/0/10 с MAC-адресами источника из диапазона от 00-12-11-23-00-00 до 00-00-00-00-ff-ff.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-
ff any-destination-mac untagged-802-3
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-
ff any tagged-802
Switch(config)#firewall enable
Switch(config)#interface ethernet1/0/10
Switch(Config-If-Ethernet1/0/10)#mac access-group 1100 in
```

Проверка результата применения конфигурации:

```
Switch#show firewall
     Firewall Status: Enable.

Switch #show access-lists
access-list 1100(used 1 time(s))
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
untagged-802-3
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
      MAC Ingress access-list used is 1100,traffic-statistics Disable.
```

Сценарий 3: необходимо запретить трафик протоколов FTP и ICMP для хостов с диапазоном мак-адресов 00-12-11-23-00-00 до 00-00-00-00-ff-ff и IP из сегмента 10.0.0.0/24.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-
ff any-destination-mac tcp 10.0.0.0 0.0.0.255 any-destination d-port
21
Switch(config)#access-list 3110 deny any-source-mac 00-12-11-23-00-00
00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255

Switch(config)#firewall enable
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#mac-ip access-group 3110 in
```

Проверка результата применения конфигурации:

```
Switch#show access-lists
access-list 3110(used 1 time(s))
```

```
access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-
ff icmp any-source 10.0.0.0 0.0.0.255

Switch #show access-group interface ethernet 1/0/10
     interface name:Ethernet1/0/10
MAC-IP Ingress access-list used is 3110, traffic-statistics Disable.
```

Сценарий 4. Протокол IPv6 запущен на интерфейсе interface vlan 600 с адресом 2003:1:1:1::0/64. Пользователям из подсети 2003:1:1:1:66::0/80 должен быть запрещен выход во внешнюю сеть.

Конфигурация будет выглядеть следующим образом

```
Switch(config)#ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-
destination
Switch(config)#ipv6 access-list 600 deny 2003:1:1:1::0/64 any-
destination

Switch(config)#firewall enable
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#ipv6 access-group 600 in
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#exit
```

Проверка результата применения конфигурации:

```
Switch#show firewall
Firewall Status: Enable.

Switch#show ipv6 access-lists
Ipv6 access-list 600(used 1 time(s))
ipv6 access-list 600 deny 2003:1:1:1::0/64 any-source
ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-source

Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
     IPv6 Ingress access-list used is 600, traffic-statistics
     Disable.
```

Сценарий 5. Интерфейсы 1/0/1, 2, 5, 7 относятся к VLAN 100, необходимо запретить хостам с IP адресом 192.168.0.1 доступ к этим интерфейсам.

Конфигурация будет выглядеть следующим образом:

```
Switch (config)#firewall enable
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/0/1;2;5;7
Switch (Config-Vlan100)#exit
Switch (config)#access-list 1 deny host-source 192.168.0.1
Switch (config)#interface ethernet1/0/1;2;5;7
Switch (config-if-port-range)#ip access-group 1 in
```

Проверка результата применения конфигурации:

```
Switch (config)#show access-group interface vlan 100
Interface VLAN 100:
Ethernet1/0/1: IP Ingress access-list used is 1, traffic-statistics
Disable.
Ethernet1/0/2: IP Ingress access-list used is 1, traffic-statistics
Disable.
Ethernet1/0/5: IP Ingress access-list used is 1, traffic-statistics
Disable.
Ethernet1/0/7: IP Ingress access-list used is 1, traffic-statistics
Disable.
```

50.4 Решение проблем с настройкой ACL

1. Проверка правил ACL выполняется сверху вниз и заканчивается после первого совпадения;
2. Правило по-умолчанию будет использоваться только в том случае, если ACL не привязан к интерфейсу или нет совпадения для правил ACL;
3. Каждый порт может быть связан только с одним ACL MAC-IP, одним ACL MAC, одним ACL IP и одним ACL IPv6;
4. При одновременном применении ACL разных типов на одном интерфейсе, приоритет ACL будет следующим:
    - IPv6 ACL
    - MAC-IP ACL
    - IP ACL
    - MAC ACL
5. Количество правил ACL, которое может быть успешно применено, зависит от ограничени содержимого ACL и предела аппаратного ресурса коммутатора. Коммутатор выведет предупреждение, если ACL не может быть применен из-за ограничение аппаратного ресурса;
6. Если один ACL содержит конфликтующие правила (например, “permit tcp any any-destination” и “deny tcp any any-destination”), при попытке привязки этого ACL к интерфейсу коммутатор выведет сообщение об ошибке;

51 Self-defined ACL

51.1 Общие сведения о self-defined ACL

В Self-defined ACL пользователь имеет возможность настроить окно (window) для сопоставления полей пакета. Окно задает смещение относительно начала заголовка одного из уровней: L2, L3 или L4. Далее пользователь создает непосредственно ACL, который определят какие значение в окне нужно проверить и какое действие при этом выполнить.

Данный коммутатор поддерживает конфигурацию 12 окон, каждое из которых может задавать значение смещения от 0 до 178, где шаг 2 байта. То есть 0 - смещение 0 байт, а 1 - смещение 2 байта. Для конфигурации правил Standard self-defined ACL должны быть настроены окна смещений до конфигурации списка правил. Правила окон глобальны и могут быть использованы в любом self-defined ACL. Окно, которое не сконфигурировано, недоступно для добавления в ACL. Когда окно добавлено в ACL, оно не может быть изменено до удаления из ACL. Для Ipv6 поддерживаются только окна с номерами 1 по 6. Наибольшее смещение l3start включает в себя заголовок L2, а наибольшее смещение l4start включает в себя заголовок L2 и L3 в любом self-defined ACL.

51.2 Конфигурация self-defined ACL

1. Задать окно смещения;
2. Настроить правила для ACL;
3. Назначить ACL на интерфейс;

1. Задать окно смещения;

Команда	Описание
`userdefined-access-list standard offset [window1 {l3start | l4start} <offset>] [window2 { l3start | l4start } <offset>] [window3 { l3start | l4start } <offset>] [window4 { l3start | l4start } <offset>] [window5 { l3start | l4start } <offset>] [window6 { l3start | l4start } <offset>] [window7 { l3start | l4start } <offset>] [window8 { l3start | l4start } <offset>] [window9 { l3start | l4start } <offset>] [window10 { l3start | l4start } <offset>] [window11 { l3start | l4start } <offset>] [window12 { l3start |`	Создать окна смещения для правила self-defined ACL. Если окно уже существует, оно может быть изменено. Если окно смещения не задано, правило создано не будет.

l4start } <offset>] no userdefined-access-list standard offset [window1] [window2] [window3] [window4] [window5] [window6] [window7] [window8] [window9] [window10] [window11] [window12] В режиме глобальной конфигурации	Удалить созданные окна смещения

2. Настроить правила для ACL;

Команда	Описание
userdefined-access-list standard <1200-1299> {permit|deny} {window1| window2|window3|window4| window5| window6|window7|window8| window9| window10|window11|window12} no userdefined-access-list standard <1200-1299> {permit|deny} {window1| window2|window3|window4| window5| window6|window7|window8| window9| window10|window11|window12} В режиме глобальной конфигурации	Создать правило для standard self-defined ACL. Если ACL не был создан ранее, он будет создан при создании правила. Удалить правило ACL

3. Назначить ACL на интерфейс;

Команда	Описание
[no] userdefined access-group <acl-name> in [traffic-statistic] В режиме конфигурации интерфейса	Применить ACL <acl-name> на входящее направление трафика на интерфейсе. С включенной опцией traffic-statistic коммутатор будет подсчитывать совпадения этой access-group Удалить ACL <acl-name> с интерфейса

51.3 Примеры настройки self-defined ACL

Сценарий 1: порт 1/0/10 относится к сегменту 10.0.0.0/24, протокол FTP не разрешен пользователю.
Конфигурация будет выглядеть следующим образом:

```
Switch(config)# userdefined-access-list standard offset window1
l3start 4 window2 l4start 1 window3 l3start 3
Switch(config)#userdefined-access-list standard 1300 deny window1
0006 00FF window2 0015 FFFF window3 0A000000 FFFFFF00
Switch(config)#firewall enable
Switch(config)#interface ethernet1/10
Switch(config-if-ethernet1/10)#userdefined access-group 1300 in
Switch(config-if-ethernet1/10)#exit
Switch(config)#exit
```

Проверка результата применения конфигурации:

```
Switch#show access-lists
userdefined-access-list standard 1300(used 1 time(s)) 1 rule(s)
     rule ID 1: window1 6 ff window2 15 ffff window3 a000000
ffffff00
Switch#show access-group interface ethernet 1/10
interface name:Ethernet1/10
     Userdefined Ingress access-list used is 1300,traffic-
statistics Disable.
```

52 802.1x

52.1 Общие сведения о 802.1x

Стандарт IEEE 802.1x определяет метод управления доступом к сети, он управляет аутентификацией и устройствами доступа на физическом уровне (порты коммутатора). Если пользовательские устройства, подключенные к этим портам, удается аутентифицировать, они получают доступ к ресурсам локальной сети, в противном случае доступ будет запрещен.

Стандарты IEEE 802.1x определяют протокол управления доступом к сети на основе портов. Протокол применим к соединению точка-точка между устройством доступа и портом доступа, при этом порт может быть логическим или физическим. В типичном случае один физический порт коммутатора присоединен только к одному терминирующему устройству (имеющему физические порты).

Архитектура IEEE 802.1x описана на рисунке ниже.

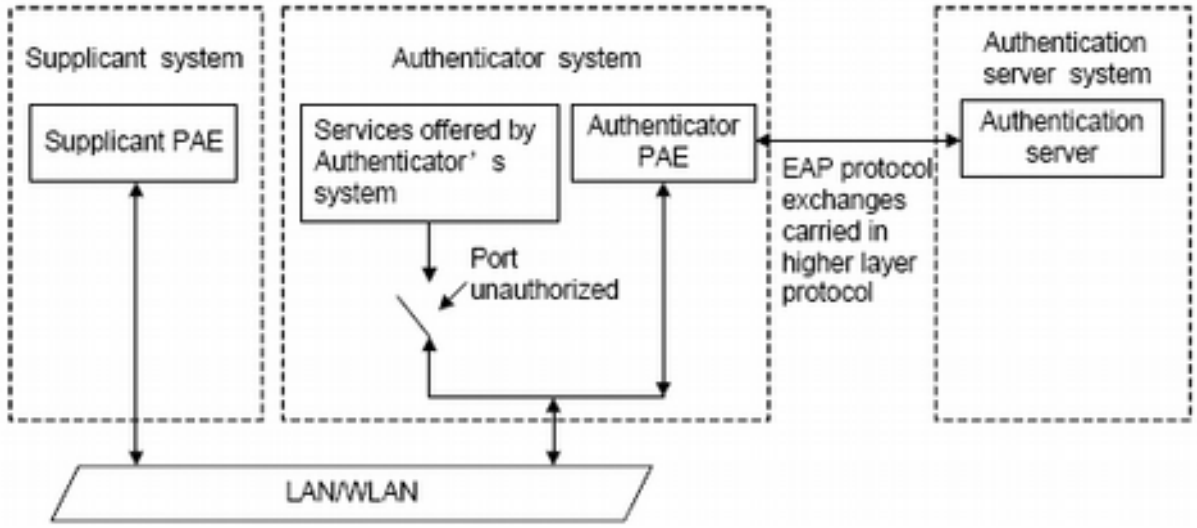


Рисунок 52.1 Архитектура IEEE 802.1x

Надписи на рисунке:

- Supplicant System – клиентская система;
- Supplicant PAE – Порт клиентской системы;
- Autenthicator system – система аутентификатора;
- Autenthicator PAE – Порт аутентификатора;
- Services offered by Autenthicator's system – услуги, предоставляемые системой аутентификатора;
- Controlled Port – управляемый порт;
- Uncontrolled port – неуправляемый порт;
- EAP protocol exchanges carried in higher layer protocol – обмен сообщениями протокола EAP происходит через протокол более высокого уровня;
- Authentication Server system – система сервера аутентификации;
- Authentication Server – сервер аутентификации.

802.1x имеет клиент-серверную архитектуру, которая имеет 3 составляющие: устройство, запрашивающее доступ, система аутентификации и сервер аутентификации.

- Устройство, запрашивающее доступ представляет собой объект на одном конце сегмента сети, который должен быть аутентифицирован блоком управления доступом на другом конце сегмента сети. Пользователь запускает аутентификацию 802.1X через программное обеспечение запрашивающей системы. Система, запрашивающая доступ, должна поддерживать EAPOL;
- Система аутентификации (в данном случае - коммутатор) представляет собой сетевое устройство, поддерживающее протокол 802.1X, к портам которого подключено устройство, запрашивающее доступ;
- Сервер аутентификации используется для аутентификации и авторизации пользователей. Обычно это сервер RADIUS, который может хранить информацию о пользователях (имя, пароль, VLAN, порт и т.д).

Взаимодействие устройства, запрашивающего доступ, и устройства управления доступом (коммутатором доступа) происходит по протоколу EAPOL, определенного стандартами IEEE 802.1x. Взаимодействие сервера аутентификации с устройством управления доступом происходит по протоколу EAP. Данные аутентификации инкапсулируются в пакеты EAP. Пакет EAP передается в пакетах протоколов более высоких уровней, например, RADIUS (EAPOR - EAP over RADIUS).

Система аутентификации (коммутатор доступа) предоставляет порты для доступа к сети запрашивающим пользовательским системам. Эти порты логически можно разделить на два вида: контролируемые и неконтролируемые:

- Неконтролируемый порт всегда находится в режиме двунаправленного соединения и в основном используется для передачи пакетов протокола EAPOL, чтобы гарантировать, что запрашивающие системы всегда могут отправлять или получать сообщения аутентификации.
- Контролируемый порт связан с состоянием аутентификации. При отсутствии аутентификации данные из запрашивающих доступ систем передаваться не могут. Данный коммутатор может осуществлять контроль только одного направления трафика.
- Управляемые и неконтролируемые порты представляют собой две логические части одного физического порта.

Реализованы методы аутентификации пользователей на основе MAC, на основе порта и на основе пользователя. Только аутентифицированные пользовательские системы, подключенные к одному и тому же физическому порту, могут получать доступ к сети. Таким образом, даже если к одному физическому порту подключено множество хостов, коммутатор может аутентифицировать их и управлять доступом каждой пользовательской системой индивидуально.

Существует 2 режима пользовательском управлении доступом имеется два режима: стандартное управление и расширенное управление. При стандартном (standard) пользовательском управлении доступ к определенным ресурсам не ограничивается до аутентификации. После аутентификации пользователи получают доступ ко всем ресурсам. При расширенном (advanced) пользовательском управлении доступом только специальные пользователи до аутентификации получат доступ к ограниченным ресурсам.

Реализована возможность использования гостевой VLAN: если устройство, запрашивающее доступ, не получит аутентификацию успешно в течение определенного промежутка времени, устройство будет добавлено в эту VLAN.

52.2 Настройка 802.1x

1. Включить IEEE 802.1x;
2. Конфигурация свойств блока управления доступом;
    a. Настроить метод контроля доступа на порту;
    b. Настроить расширенные функции;
3. Конфигурация свойств зависимых устройств пользователя.

1. Включить IEEE 802.1x:

Команда	Описание

`dot1x enable`
 	
`no dot1x enable`
 	
В режиме глобальной конфигурации
	Включить функцию dot1x на коммутаторе и портах
	Выключить функцию dot1x.

`dot1x privateclient enable`
`no dot1x privateclient enable`
 	
В режиме глобальной конфигурации
	Включить режим использования клиентским ПО специального формата сообщений 802.1x. Команда `no` включает режим использования стандартного формата (по-умолчанию)

`dot1x user free-resource <prefix> <mask>`
`no dot1x user free-resource`
 	
В режиме глобальной конфигурации
	Задать сеть `<prefix> <mask>`, доступную пользователям без аутентификации. Команда `no` удаляет сеть, доступную без аутентификации.

`dot1x unicast enable`
`no dot1x unicast enable`
 	
В режиме глобальной конфигурации
	Включить функцию одноадресной сквозной передачи `dot1x`. Команда `no` отключает эту функцию.

2. Конфигурация свойств блока управления доступом:
    a. Настроить метод контроля доступа на порту:

Команда	Описание

`dot1x port-method {macbased | portbased | userbased {standard | advanced}}`
`no dot1x port-method`
 	
В режиме конфигурации интерфейса
	Задать метод управления доступом к порту. Команда `no` восстанавливает значение по-умолчанию - `userbased advanced`.

`dot1x max-user macbased <number>`
`no dot1x max-user macbased`
 	
В режиме конфигурации интерфейса
	Задать максимальное число `<number>` пользователей, которые могут получить доступ к данному порту при управлении на основе MAC-адреса.
	Команда `no` возвращает значение по-умолчанию - 1.

`dot1x max-user userbased <number>`
`no dot1x max-user userbased`
 	
В режиме конфигурации интерфейса
	Задать максимальное число `<number>` пользователей, которые могут получить доступ к данному порту при управлении на основе пользователя..
	Команда `no` возвращает значение по-умолчанию - 10.

`dot1x guest-vlan <vlanID>`
`no dot1x guest-vlan`
 	
В режиме конфигурации интерфейса
	Задать VLAN, доступный при неаутентифицированном состоянии (гостевой) на данном интерфейсе.
	Команда `no` запрещает гостевой VLAN (по-умолчанию).

`dot1x portbased mode single-mode`
`no dot1x portbased mode single-mode`
 	
В режиме конфигурации интерфейса
	Включить на порту режим аутентификации единственного пользователя. Команда `no` отключает этот режим.

b. Настроить расширенные функции:

Команда	Описание

`dot1x macfilter enable`
`no dot1x macfilter enable`
 	
В режиме глобальной конфигурации
	Включает возможность фильтровать MAC-адреса на коммутаторе посредством dot1x. Команда `no` отключает эту возможность.

`dot1x macbased port-down-flush`
`no dot1x macbased port-down-flush`
 	
В режиме глобальной конфигурации
	Включить функцию автоматического удаления пользователей, аутентифицированных на основе MAC, при перемещении между портами. Команда `no` отключает эту функцию.

`dot1x accept-mac <mac-address> [interface <interface-name> ]`
`no dot1x accept-mac <mac-address> [interface <interface-name> ]`
 	
В режиме глобальной конфигурации
	Добавить адрес `<mac-address>` изученный с интерфейса `<interface-name>` в качестве разрешенного в таблицу фильтрации dot1x. Команда `no` удаляет этот адрес.

`dot1x eapor enable`
 	
`no dot1x eapor enable`
 	
В режиме глобальной конфигурации
	Включить функцию EAP-relay на коммутаторе. Команда `no` задает локальное окончание аутентификации.

3. Конфигурация свойств dot1q для устройств пользователя:

Команда	Описание

`dot1x max-req <count>`
 	
`no dot1x max-req`
 	
В режиме глобальной конфигурации
	Задать число `<count>` запросов или MD5 кадров, посылаемых при отсутствии ответа от клиентской системы до того, как коммутатор повторно инициирует аутентификацию. Команда `no` восстанавливает значения по-умолчанию - 2.

`dot1x re-authentication`
 	
`no dot1x re-authentication`
 	
В режиме глобальной конфигурации
	Включить периодическую повторную аутентификацию клиентской системы. Команда `no` отключает эту функцию.

`dot1x timeout quiet-period <seconds>`
 	
`no dot1x timeout quiet-period`
	Задать время в секундах бездействия при сбое аутентификации. Команда `no` восстанавливает значения по-

В режиме глобальной конфигурации	умолчанию - 10 секунд.

`dot1x timeout re-authperiod <seconds>`
`no dot1x timeout re-authperiod`
 	
В режиме глобальной конфигурации
	Задать время повторной периодической аутентификации пользователя в секундах. Команда `no` возвращает значение по-умолчанию - 3600 секунд.

`dot1x timeout tx-period <seconds>`
 	
`no dot1x timeout tx-period`
 	
В режиме глобальной конфигурации
	Позволяет задать интервал времени, по истечении которого клиентской системой выполняется повторная передача запроса или кадра идентичности EAP. Команда `no` восстанавливает значение по-умолчанию - 30 секунд.

`dot1x re-authenticate [interface <interface-name> ]` В режиме глобальной конфигурации	Повторно принудительно аутентифицировать все устройства. При указании интерфейса `<interface-name>` повторно аутентифицируются только устройства в указанном интерфейсе.

52.3 Примеры конфигурации 802.1x

52.3.1 Гостевая VLAN

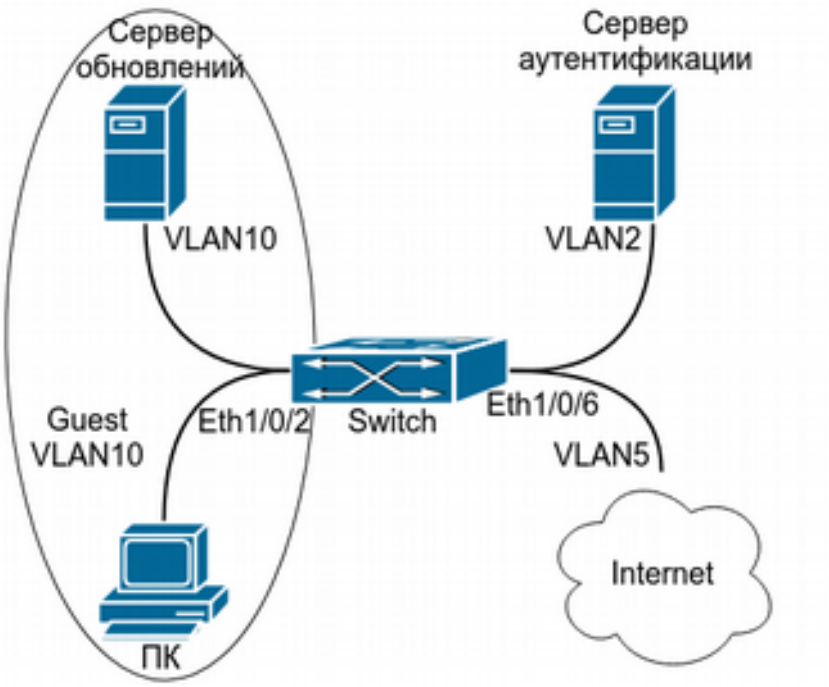


Рисунок 28.2 Гостевая VLAN

Как показано на рисунке 28.2, для доступа в сеть коммутатор использует 802.1x и сервер RADIUS в качестве сервера аутентификации. Порт подключения пользователей на коммутаторе - Ethernet1/0/2. Сервер аутентификации находится в VLAN2. Сервер обновлений находится в VLAN10, Ethernet1/0/6 - порт коммутатора, используемый для выхода в Интернет, принадлежит VLAN5. VLAN10 установлена как гостевая на порту Ethernet1/0/2, поэтому до аутентификации пользователя порт Ethernet1/0/2 добавлен во VLAN10, разрешая пользователю доступ к серверу обновлений.

После того, как пользователь успешно прошел аутентификацию, коммутатор добавляет порт пользователя во VLAN5, разрешая доступ в Интернет.

Конфигурация выглядит следующим образом:
Настроить коммутатор для работы с RADIUS:

```
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

создать VLAN100:
```
Switch(config)#vlan 100
```

Включить функцию 802.1x
```
Switch(config)#dot1x enable
Switch(config)#interface ethernet1/0/2
Switch(Config-If-Ethernet1/0/2)#dot1x enable
```

Настроить порт Ethernet1/0/2
```
Switch(Config-If-Ethernet1/0/2)#switchport mode access
Switch(Config-If-Ethernet1/0/2)#dot1x port-method portbased
Switch(Config-If-Ethernet1/0/2)#dot1x port-control auto Switch(Config-
If-Ethernet1/0/2)#dot1x guest-vlan 100
```

52.3.2 RADIUS

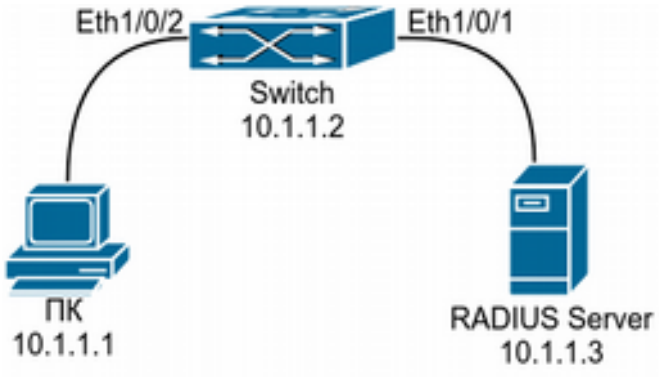


Рисунок 28.3 Dot1x RADIUS

Хост пользователя подключен к порту коммутатора Ethernet1/0/2, на котором задействована функция аутентификации IEEE 802.1x. В качестве метода доступа используется MAC-based. IP-адрес коммутатора 10.1.1.2. Порт коммутатора Ethernet1/0/1 подключен к RADIUS серверу, который имеет IP-адрес 10.1.1.3 и испольует порт 1813 по-умолчанию для аутентификации и аккаунинга. Хост пользователя использует специализированное программное обеспечение для аутентификации IEEE 802.1x.
Конфигурация будет выглядеть следующим образом:

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/2
Switch(Config-Ethernet1/0/2)#dot1x enable
Switch(Config-Ethernet1/0/2)#exit
```

52.4 Решение проблем с настройкой 802.1x

- Для включения 802.1x на порту должны быть выключены функции привязки MAC-адреса и агрегирования портов;
- Проверьте связь между коммутатором и RADIUS-сервером, между коммутатором и устройством пользователя, а также конфигурацию их портов и VLAN;
- Проверьте правильность указания ключа для RADIUS-сервера;
- Для поиска возможных причин неисправности проверьте журнал событий на сервере RADIUS;

53 Ограничение MAC и IP адресов на порту, конфигурация VLAN

53.1 Общие сведения о функции ограничения MAC и IP адресов на порту

Для повышения безопасности и улучшения контроля пользователей, на данном коммутаторе существуют функции контроля количества MAC-адресов и ARP/ND записей на портах, а также количества пользователей в VLAN.

Ограничение количества динамических MAC- и IP-адресов на портах:

1. Ограничение количества динамических MAC-адресов. Если количество динамических MAC-адресов, изученных коммутатором на порту, равно или превышает установленный предел, то функция изучения MAC-адресов на порту должна отключаться.
2. Ограничение количества динамических IP-адресов. Если количество динамических ARP/ND, изученных коммутатором на порту, равно или превышает установленный предел, то функция распознавания ARP/ND на порту должна отключаться.

Ограничение количества MAC, ARP и ND на интерфейсах:

1. Ограничение количества динамических MAC-адресов. Если количество динамических MAC-адресов, распознанных интерфейсом VLAN, равно или превышает установленный предел, то функция распознавания MAC-адресов для всех портов VLAN должна отключаться.
2. Ограничение количества динамических IP-адресов. Если количество динамических ARP/ND, распознанных интерфейсом VLAN, равно или превышает установленный предел, то функция распознавания ARP/ND на всех портах VLAN должна отключаться.

53.2 Конфигурация функции ограничения MAC и IP адресов

1. Включить функцию ограничения количества MAC и IP на портах;
2. Включить функцию ограничения количества MAC и IP на интерфейсах и VLAN;

3. Настроить действие при нарушении защиты;
4. Отображение информации и отладка функций ограничения MAC и IP на портах

1. Включить функцию ограничения количества MAC и IP на портах;

Команда	Описание

`switchport mac-address dynamic maximum`
 	
`no switchport mac-address dynamic maximum`
	Включить функцию ограничения количества динамических MAC-адресов. Команда `no` отключает эту функцию.

В режиме конфигурации интерфейса	

`switchport arp dynamic maximum`
`no switchport arp dynamic maximum`
 	
В режиме конфигурации интерфейса
	Включить функцию ограничения количества динамических ARP-записей. Команда `no` отключает эту функцию.

`switchport nd dynamic maximum`
`no switchport nd dynamic maximum`
 	
В режиме конфигурации интерфейса
	Включить функцию ограничения количества динамических ND-записей. Команда `no` отключает эту функцию.

2. Включить функцию ограничения количества MAC и IP на интерфейсах и VLAN:

Команда	Описание

`vlan mac-address dynamic maximum <value>`
`no vlan mac-address dynamic maximum`
 	
В режиме конфигурации VLAN
	Задать максимальное количество `<value>` MAC-адресов

`ip arp dynamic maximum <value>`
`no ip arp dynamic maximum`
 	
В режиме конфигурации интерфейса
	Задать максимальное количество `<value>` ARP записей. Команда `no` отменяет ограничение.

`ipv6 nd dynamic maximum <value>`
`no ipv6 nd dynamic maximum`
 	
В режиме конфигурации интерфейса
	Задать максимальное количество `<value>` ND записей. Команда `no` отменяет ограничение.

3. Настроить действие при нарушении защиты:

Команда	Описание

`switchport mac-address violation {protect | shutdown} [recovery <5-3600>]`
`no switchport mac-address violation`
 	
В режиме конфигурации интерфейса
	Задать действие при нарушении защиты: `protect` - новый MAC-адрес не будет изучен, `shutdown` - порт будет переведен в состояние Admin down, период, по истечении которого будет восстановлено первоначальное состояние - `[recovery <5-3600>`. Команда `no` восстанавливает знчаение по-умолчанию - `protect`.

4. Отображение информации и отладка функций ограничения MAC и IP на портах

Команда	Описание
`show mac-address dynamic count {vlan <vlan-id> | interface ethernet <portName> }` В привилегированном режиме	Отобразить текущее количество MAC-адресов, изученных через интерфейс `<portName>`, VLAN `<vlan-id>`
`show arp-dynamic count {vlan <vlan-id> | interface ethernet <portName> }` В привилегированном режиме	Отобразить текущее количество ARP записей, изученных через интерфейс `<portName>`, VLAN `<vlan-id>`
`show nd-dynamic count {vlan <vlan-id> | interface ethernet <portName> }`	Отобразить текущее количество ND записей, изученных через интерфейс `<portName>`, VLAN `<vlan-id>`

`debug switchport mac count`
`no debug switchport mac count`
 	
В привилегированном режиме
	Выводить отладочную информацию об ограничении MAC на портах

`debug switchport arp count`
`no debug switchport arp count`
 	
В привилегированном режиме
	Выводить отладочную информацию об ограничении ARP на портах

`debug switchport nd count`
`no debug switchport nd count`
 	
В привилегированном режиме
	Выводить отладочную информацию об ограничении ND на портах

`debug vlan mac count`
`no debug vlan mac count`
 	
В привилегированном режиме
	Выводить отладочную информацию об ограничении MAC во VLAN

`debug ip arp count`
`no debug ip arp count`
 	
В привилегированном режиме
	Выводить отладочную информацию об ограничении ARP для интерфейсов

`debug ipv6 nd count`
`no debug ipv6 nd count`
В привилегированном режиме
	Выводить отладочную информацию об ограничении ND для интерфейсов

53.3 Пример конфигурации функции ограничения MAC и IP адресов

К коммутатору SwitchA подключено множество пользователей. До включения функции ограничения на портах и VLAN коммутатор SwitchA может получить MAC-адреса, ARP и ND записи со всех ПК при отсутствии аппаратных ограничений. В данной ситуации существует возможность атаки на отказ в обслуживании, когда один из хостов пользователей будет отправлять кадры данных с множеством разных MAC-адресов источника, чем вызовет переполнение таблицы на коммутаторе SwitchA.

Так как предполагается, что к одному порту коммутатора может быть подключено не более 2х устройств пользователя коммутатора SwitchA, необходимо установить максимальное количество динамических MAC-адресов 2, динамических ARP-адресов – 2, ND – 1. В VLAN1 необходимо установить максимальное количество динамических MAC-адресов 70, динамических ARP-адресов – 70, ND – 40.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#interface ethernet 1/0/1-24
Switch(config-if-range)#switchport mac-address dynamic maximum 2
Switch(config-If-range)#switchport arp dynamic maximum 2
Switch(config-If-range)#switchport nd dynamic maximum 1
Switch(config-if-Vlan1)#vlan mac-address dynamic maximum 70
Switch(config-if-Vlan1)#ip arp dynamic maximum 70
Switch(config-if-Vlan1)#ip nd dynamic maximum 40
```

53.4 Решение проблем при конфигурации функции ограничения MAC и IP адресов

- Функция ограничения MAC, ARP и ND на портах и VLAN по-умолчанию отключена;
- Функция ограничения MAC, ARP и ND на портах и VLAN не работает одновременно с вышеперечисленными функциями Spanning-Tree, dot1x и агрегации портов;
- При необходимости получения полной информации о текущем состоянии на портах и VLAN с ограничениями используются отладочные и информационные команды, описанные в разделе 29.2.

54 Конфигурация AM

54.1 Общие сведения об AM

Функционал AM (Access Management) - управление доступом, заключается в сравнении информации из полученного сообщения (IP-адрес источника или IP-адрес источника + MAC-адрес источника) с записью в пуле адресов. При обнаружении совпадения сообщение передается, в противном случае – отбрасывается. Существует возможность сконфигурировать как список соответствия IP-адреса порту, так и IP-адреса и MAC адреса одновременно.

54.2 Конфигурация AM

1. Включить функцию AM;
2. Настроить записи в IP-таблице;
3. Настроить MAC-IP таблице;
4. Удалить таблицы AM;
5. Просмотр информации о настроенной функции AM.

1. Включить функцию AM:

Команда	Описание

`am enable`
`no am enable`
 	
В режиме глобальной конфигурации
	Включить функцию AM. Команда `no` отключает эту функцию.

`am port`
`no am port`
 	
В режиме конфигурации интерфейса
	Включить функцию AM на порту. Команда `no` отключает эту функцию.

2. Настроить записи в IP-таблице:

Команда	Описание

`am ip-pool <ip-address> <num>`
`no am ip-pool <ip-address> <num>`
 	
В режиме конфигурации интерфейса
	Добавить IP-адрес `<ip-address>` в таблицу разрешения доступа AM. Для добавления группы адресов необходимо указать количество адресов `<num>`, следующих за указанным `<ip-address>` по порядку. Команда `no` удаляет эту запись.

3. Настроить MAC-IP таблице:

Команда	Описание

`am mac-ip-pool <mac-address> <ipaddress>`
`no am mac-ip-pool <mac-address> <ip-address>`
 	
В режиме конфигурации интерфейса
	Добавить соответствие IP-адреса `<ip-address>` MAC-адресу `<mac-address>` в таблице разрешения доступа AM. Команда `no` удаляет эту запись.

4. Удалить таблицы AM:

Команда	Описание
`no am all [ip-pool|mac-ip-pool]` В режиме глобальной конфигурации	Удалить все записи для таблиц `ip-pool` или `mac-ip-pool`.

5. Просмотр информации о настроенной функции AM.

Команда	Описание
`show am [interface <interface-name>]` В режиме глобальной конфигурации	Просмотр информации об AM на интерфейсе `<interface-name>`

54.3 Пример конфигурации AM

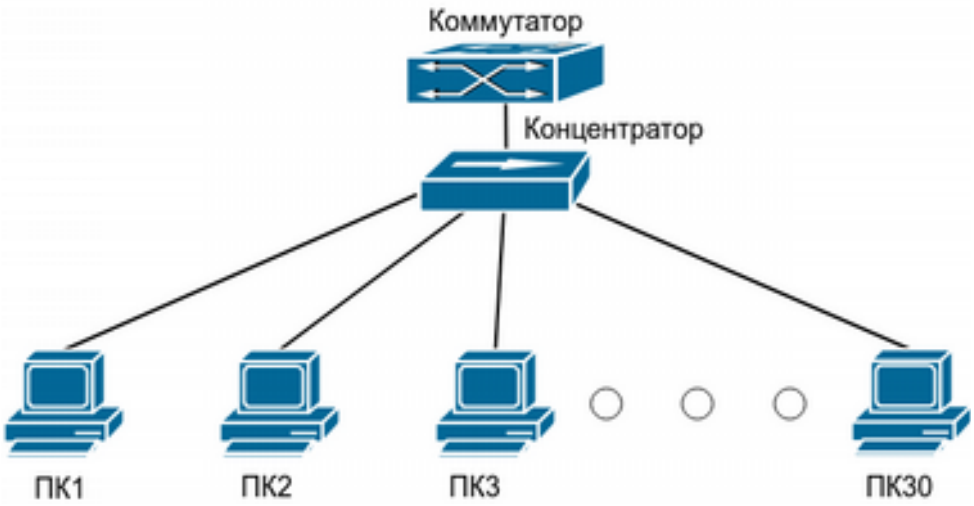


Рисунок 54.1 Конфигурация AM

Как показано на рисунке 54.1, 30 ПК подключены через концентратор к коммутатору через интерфейс Ethernet1/0/1. IP-адреса этих ПК находятся в диапазоне от 10.0.0.1 до 10.0.0.30. Согласно политике безопасности, администратор настраивает легальными только эти 30 адресов. Коммутатор будет пересылать только пакеты от этих IP-адресов, а пакеты от других адресов отбрасывать.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#am enable
Switch(config)#interface ethernet1/0/1
Switch(Config-If-Ethernet 1/0/1)#am port
Switch(Config-If-Ethernet 1/0/1)#am ip-pool 10.0.0.1 10
```

54.4 Решение проблем с конфигурацией AM

- По-умолчанию после включения функция AM отбрасывает сообщения от всех адресов. Для пропуска сообщений необходимо настроить ip-pool или mac-ip-pool.
- Для просмотра детальной информации о настроенном функционале AM используйте команду **show am [interface <interface-name>].**

55 Функции предотвращения атак

55.1 Общие сведения о функциях предотвращения атак

Функционал безопасности, описываемый в данной главе представляет собой проверку пакетов определенный протоколов по алгоритму, призванному предотвратить атаку на отказ в обслуживании DoS. Данный функционал не вызывает дополнительных задержек кадров во время своей работы.

55.2 Конфигурация функций предотвращения атак

1. Функция предотвращения атаки IP-spoofing;
2. Функция предотвращения атаки TCP unauthorized label;
3. Функция предотвращения атаки подмены порта;
4. Функция предотвращения атаки ICMP fragmentation;

1. Функция предотвращения атаки IP-spoofing:

Команда	Описание
`[no] dosattack-check srcip-equal-dstip enable` В режиме глобальной конфигурации	Отбрасывать пакеты, IP-адрес источника которых равен IP-адресу назначения. Команда `no` разрешает передачу таких пакетов.

2. Функция предотвращения атаки TCP unauthorized label:

Команда	Описание
`[no] dosattack-check tcp-flags enable` В режиме глобальной конфигурации	Отбрасывать следующие 4 вида пакетов: 1. пакеты, содержащие несанкционированную метку TCP: SYN = 1, когда порт источника меньше 1024; 2. позиции метки TCP - все 0, а его serial № = 0;3. FIN = 1, URG = 1, PSH = 1 и серийный номер TCP = 0; 4. SYN = 1 и FIN = 1. Команда `no` разрешает передачу таких пакетов.

3. Функция предотвращения атаки подмены порта:

Команда	Описание
`[no] dosattack-check srcport-equal-`	Отбрасывать пакеты, TCP|UDP порт

`dstport enable` В режиме глобальной конфигурации	источника которых равен порту назначения. Команда `no` разрешает передачу таких пакетов.

4. Функция предотвращения атаки ICMP fragmentation:

Команда	Описание
`[no] dosattack-check icmp-attacking enable` В режиме глобальной конфигурации	Отбрасывать фрагментированные ICMPv4 пакеты, чья длина меньше определенной. Команда `no` разрешает передачу таких пакетов
`dosattack-check icmpv4 <size>` В режиме глобальной конфигурации	Задать минимальный размер фрагментированного ICMPv4 пакета. По-умолчанию - 512.

56 TACACS+

56.1 Общие сведения о TACACS+

TACACS+ представляет собой похожий на RADIUS сеансовый протокол контроля доступа. Протокол TACACS+ использует три независимые функции: Аутентификация, Авторизация и Аккаунтинг (учёт). В отличие от RADIUS протокол TACACS+ использует TCP и шифрование передаваемых данных для обеспечения безопасности.
На данном коммутаторе TACACS+ может быть использован при авторизации и аутентификации пользователей для доступа к коммутатору по telnet или ssh.

56.2 Конфигурация TACACS+

1. Задать ключ сервера TACACS+;
2. Настроить тайм-аут аутентификации TACACS+;
3. Настроить параметры сервера TACACS+;
4. Настроить IP-адрес TACACS+ NAS.

1. Задать ключ аутентификации TACACS+:

Команда	Описание

`tacacs-server key {0 | 7} <string>`
`no tacacs-server key`
 	
В режиме глобальной конфигурации
	Задать глобальный ключ сервера TACACS+. Команда `no` удаляет этот ключ.

2. Настроить тайм-аут аутентификации TACACS+:

Команда	Описание

`tacacs-server timeout <seconds>`
`no tacacs-server timeout`
 	
В режиме глобальной конфигурации
	Задать глобальное время ожидания ответа от TACACS+ сервера в секундах. Команда `no` возвращает значение по-умолчанию - 3 секунды.

3. Настроить параметры сервера TACACS+:

Команда	Описание
`tacacs-server authentication host <ipaddress> [port <port-number>] [timeout <seconds>] [key {0 | 7}`	Сконфигурировать параметры обращения к серверу TACACS+: `<ipaddress>` - IP-адрес сервера; `[port <port-number>]` - порт назначения (по-умолчанию 49);

<string>] [primary] no tacacs-server authentication host <ip-address> В режиме глобальной конфигурации	[timeout <seconds>] - время ожидания ответа от сервера;key {0 | 7} <string>] - ключ сервера; primary – данный сервер будет использоваться в приоритетном порядке. Если параметры [timeout <seconds>] и key {0 | 7} <string>] не заданы, будут использоваться параметры, заданные глобально. Команда **no** удаляет заданный сервер с адресом <ip-address>.

4. Настроить IP-адрес TACACS+ NAS:

Команда	Описание
tacacs-server nas-ipv4 <ip-address> no tacacs-server nas-ipv4 В режиме глобальной конфигурации	Задать IP-адрес <ip-address> источника пакетов TACACS+, отправляемых коммутатором. Команда no устанавливает в качестве источника адрес IP-интерфейса, с которого были отправлены пакеты (по-умолчанию).

56.3 Пример конфигурации TACACS+

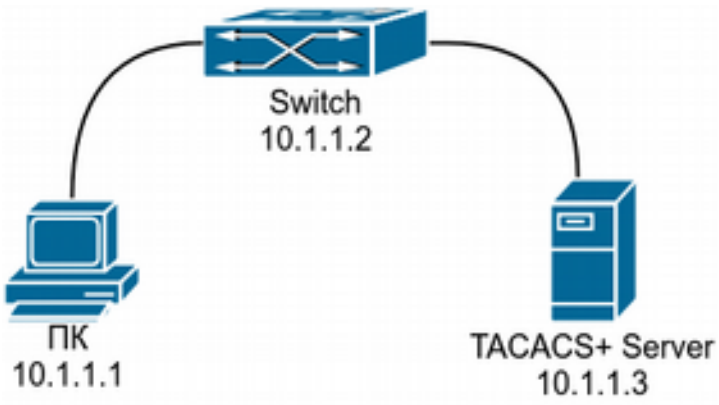


Рисунок 32.1 Аутентификация TACACS+

ПК подключен к коммутатору, который имеет IP-адрес 10.0.0.2 и подключен к серверу аутентификации TACACS+. IP-адрес сервера 10.0.0.3, используемый порт по-умолчанию - 49. Доступ на коммутатор по telnet контролируется сервером

аутентификации.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.0.0.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#tacacs-server authentication host 10.0.0.3
Switch(config)#tacacs-server key test
Switch(config)#authentication line vty login tacacs
```

56.4 Устранение проблем при конфигурации TACACS+

Убедитесь, что:

1. IP-связность коммутатора с сервером TACACS+ присутствует;
2. ключ аутентификации на коммутаторе совпадает с ключом на TACACS+ сервере;
3. подключение осуществляется к правильному TACACS+ серверу.

57 RADIUS

57.1 Общие сведения о RADIUS

57.1.1 Общие сведения о AAA и RADIUS

AAA - сокращение от Authentication, Authorization and Accounting (Аутентификация, Авторизация, учёт) и используется при предоставлении доступа в сеть, к управлению оборудованием и управления этим доступом. RADIUS - это один из сетевых клиент-серверных протоколов, используемый для централизованного управления авторизацией, аутентификацией и учетов при запросе доступа пользователей к различным сетевым службам. Клиент RADIUS обычно используется на сетевом устройстве для реализации AAA совместно с протоколом 802.1x. Сервер RADIUS хранит базу данных для AAA и связывается с клиентом RADIUS через протокол RADIUS, который является наиболее распространенным протоколом в рамках AAA.

57.1.2 Общие сведения о AAA и RADIUS

Протокол RADIUS использует UDP для транспорта. Формат заголовка пакета показан ниже.

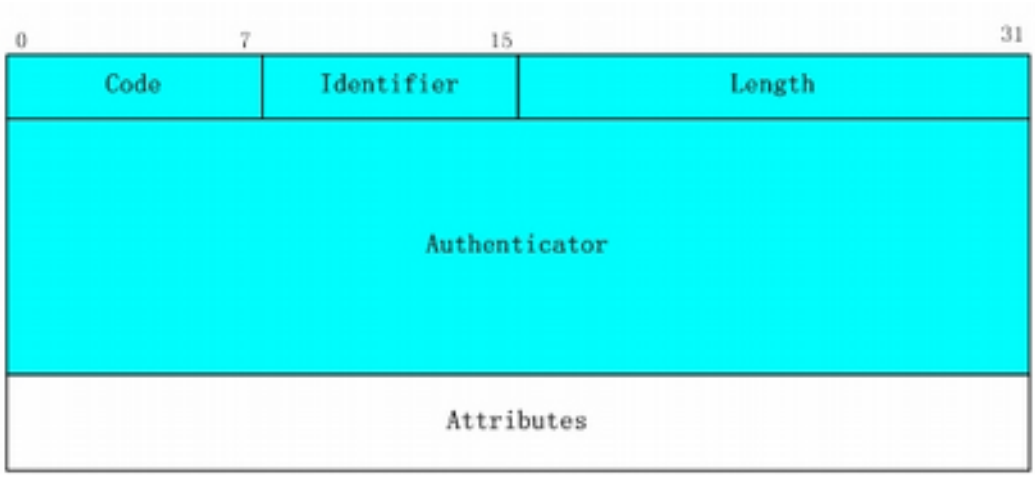


Рисунок 57.1 Формат пакета RADIUS

Code – тип пакета RADIUS, возможные значения для данного поля:

- 1 - Access-Request
- 2 - Access-Accept
- 3 - Access-Reject
- 4 - Accounting-Request
- 5 - Accounting-Response
- 11 - Access-Challenge

Identifier – идентификатор для пакетов запроса и ответа.
Length – длина всего пакета RADIUS.
Authenticator – поле используется для проверки пакетов, полученных от RADIUS-сервера, или для передачи зашифрованных паролей. Поле разделено на две части:

аутентификатор запроса и аутентификатор ответа.
Attribute – поле используется для передачи детальной информации о AAA. Значение поля формируется из значений полей **Type, Length, и Value**:
Type field - тип атрибута, значение типов атрибутов определены в **RFC 2865**;
Length field – длина атрибута;
Value field – значение атрибута.

57.2 Конфигурация RADIUS

1. Включить функцию аутентификации и учета;
2. Настроить ключ сервера RADIUS;
3. Настроить параметры RADIUS сервера;
4. Настроить параметры сервиса RADIUS;
5. Настроить адреса RADIUS NAS.

1. Включить функцию аутентификации и учета:

Команда	Описание

`aaa enable`
`no aaa enable`
 	
В режиме глобальной конфигурации
	Включить функцию аутентификации AAA. Команда `no` отключает эту функцию.

`aaa-accounting enable`
`no aaa-accounting enable`
 	
В режиме глобальной конфигурации
	Включить функцию учета AAA. Команда `no` отключает эту функцию.

`aaa-accounting update {enable|disable}` В режиме глобальной конфигурации	Включить или выключить (по-умолчанию) периодическую отправку данных об онлайн-пользователях.

2. Настроить ключ сервера RADIUS:

Команда	Описание

`radius-server key {0 | 7} <string>`
`no radius-server key`
 	
В режиме глобальной конфигурации
	Задать глобальный ключ RADIUS-сервера. Команда `no` удаляет заданный ключ.

3. Настроить параметры RADIUS сервера:

Команда	Описание

`radius-server authentication host {<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary] [access-mode {dot1x | telnet}]`
`no radius-server authentication host {<ipv4-address> | <ipv6-address>}`
 	
В режиме глобальной конфигурации
	Настроить параметры RADIUS-сервера `<ipv4-address> | <ipv6-address>` для аутентификации. Если параметр `[key {0 | 7} <string>]` не будет задан, то будет использован параметр заданный глобально. Команда `no` удаляет заданный сервер.

`radius-server accounting host {<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary]`
`no radius-server accounting host {<ipv4-address> | <ipv6-address>}`
 	
В режиме глобальной конфигурации
	Настроить параметры RADIUS-сервера `<ipv4-address> | <ipv6-address>` для учета. Если параметр `[key {0 | 7} <string>]` не будет задан, то будет использован параметр заданный глобально. Команда `no` удаляет заданный сервер.

4. Настроить параметры сервиса RADIUS:

Команда	Описание

`radius-server dead-time <minutes>`
`no radius-server dead-time`
 	
В режиме глобальной конфигурации
	Задать время восстановления статуса RADIUS-сервера после того, как коммутатор обнаружил его недоступность, в минутах. Команда `no` восстанавливает значение по-умолчанию - 5 минут.

`radius-server retransmit <retries>`
`no radius-server retransmit`
 	
В режиме глобальной конфигурации
	Задать число попыток `<retries>` повторной отправки пакетов на RADIUS-сервер. Команда `no` восстанавливает значение по-умолчанию - 3 попытки.

`radius-server timeout <seconds>`
`no radius-server timeout`
 	
В режиме глобальной конфигурации
	Задать время ожидания ответа от сервера перед повторной отправкой пакета, в секундах. Команда `no` восстанавливает значение по-умолчанию - 3 секунды.

`radius-server accounting-interim-update timeout <seconds>`
`no radius-server accounting-interim-update timeout`
 	
В режиме глобальной конфигурации
	Задать интервал отправки сообщений обновления учета пользователей онлайн, в секундах. Команда `no` восстанавливает значение по-умолчанию - 300 секунд.

5. Настроить адреса RADIUS NAS:

Команда	Описание

`radius nas-ipv4 <ip-address>`
`no radius nas-ipv4`
 	
В режиме глобальной конфигурации
	Задать IPv4-адрес `<ip-address>` источника пакетов RADIUS, отправляемых коммутатором. Команда `no` устанавливает в качестве источника адрес IP-интерфейса, с которого были отправлены пакеты (по-умолчанию

`radius nas-ipv6 <ip-address>`
`no radius nas-ipv6`
 	
В режиме глобальной конфигурации
	Задать IPv6-адрес `<ip-address>` источника пакетов RADIUS, отправляемых коммутатором. Команда `no` устанавливает в качестве источника адрес IP-интерфейса, с которого были отправлены пакеты (по-умолчанию

57.3 Пример конфигурации RADIUS

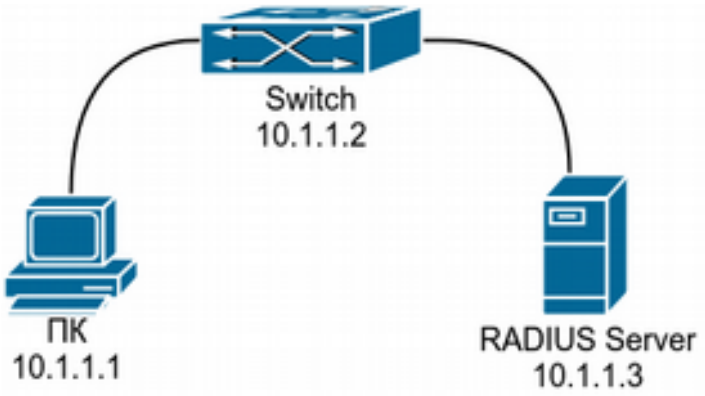


Рисунок 57.2 Конфигурация RADIUS

ПК подключен к коммутатору, который имеет IP-адрес 10.0.0.2 и подключен к серверу

аутентификации RADIUS. IP-адрес сервера 10.0.0.3, используемый порт для аутентификации по-умолчанию - 1812, для учета - 1812 . Доступ на коммутатор по telnet контролируется сервером аутентификации.

Конфигурация выглядит следующим образом:

```
Switch(config)#radius-server authentication host 10.0.0.3
Switch(config)#radius-server accounting host 10.0.0.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#authentication line vty login tacacs
```

57.4 Устранение проблем при конфигурации RADIUS

Убедитесь, что:

1. IP-связность коммутатора с сервером RADIUS присутствует;
2. ключ аутентификации на коммутаторе совпадает с ключом на RADIUS сервере;
3. подключение осуществляется к правильному RADIUS серверу.

Подробная отладочная информация может быть отображена после применения команды **debug aaa**.

58 SSL

58.1 Общие сведения об SSL

SSL (Secure Sockets Layer) - протокол, используемый для защищенной передачи информации в Интернет. На данном коммутаторе SSL может быть использован совместно с HTTP для доступа к WEB-интерфейсу управления коммутатором.

Протокол SSL использует протокол TCP для непосредственной передачи пакетов по сети. Поверх TCP инкапсулируется заголовок одного из SSL Record Protocol. Им может быть SSL Handshake Protocol, позволяющий согласовывать ключи и алгоритмы шифрования. SSL не зависит от протокола уровня приложений и является полностью прозрачным для них.

В общей модели SSL согласовывает алгоритм шифрования, ключ шифрования и аутентификацию сервера перед передачей данных, где используется SSL-сертификат доверенного центра. В настоящее время ключи, предоставляемые коммутатором, не являются официальными сертификационными ключами, а являются частными ключами сертификации, создаваемыми программным обеспечением SSL на коммутаторе, которые не могут быть распознаны браузером. Это не является обязательным условием работы HTTPS и достаточно для обеспечения безопасной связи между пользователем и коммутатором. Ключ шифрования и метод шифрования должны, которые будет использоваться для шифрования данных будут согласованы в момент установления соединения.

58.2 Конфигурация SSL

1. Включить функцию SSL;
2. Настроить номер порта для SSL;
3. Настроить набор методов шифрования для SSL;
4. Инструменты диагностики SSL;

1. Включить функцию SSL:

Команда	Описание

`ip http secure-server`
`no ip http secure-server`
 	
В режиме глобальной конфигурации
	Включить функцию SSL. Команда `no` отключает эту функцию.

2. Настроить номер порта для SSL:

Команда	Описание

`ip http secure-port <port-number>`
`no ip http secure-port`
 	
В режиме глобальной конфигурации
	Задать порт для использования SSL. Команда `no` возвращает значение по-умолчанию - 443.

3. Настроить набор методов шифрования для SSL:

Команда	Описание

`ip http secure-ciphersuite {des-cbc3-sha|rc4-128-sha| des-cbc-sha}`
`no ip http secure-ciphersuite`
 	
В режиме глобальной конфигурации
	Выбрать алгоритм шифрования. Команда `no` отменяет выбор.

4. Инструменты диагностики SSL:

Команда	Описание
`show ip http secure-server status` В привилегированном режиме	Отобразить информацию о конфигурации SSL.

`debug ssl`
`no debug ssl`
 	
В привилегированном режиме
	Отобразить отладочную информацию о SSL. Команда **no** отключает эту функцию.

58.3 Пример конфигурации SSL

После того, как WEB-интерфейс включен на коммутаторе, SSL может быть настроен для использования при получении более безопасного доступа пользователей к коммутатору.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)# ip http secure-server
Switch(config)# ip http secure-port 1025
Switch(config)# ip http secure-ciphersuite rc4-128-sha
```

58.4 Решение проблем при конфигурации SSL

1. Убедитесь в наличии физического соединения между коммутатором и пользователем, в том, что пользователь находится в нужной VLAN и L3-интерфейс на коммутаторе находится в состоянии UP;
2. Убедитесь, что пользователь использует верный порт;
3. Убедитесь, что WEB-интерфейс и SSL активированы на коммутаторе;
4. После изменения метода шифрования или порта, перезапустите SSL;
5. Для получения отладочной информации воспользуйтесь командой **debug ssl.**
6.

59 IPv6 RA Security

59.1 Общие сведения об IPv6 RA Security

Обычно IPv6 сеть включает маршрутизаторы, коммутаторы 2 уровня и IPv6 хосты. Маршрутизаторы объявляют о своём статусе сообщениями RA (Router Advertisement), которое содержит информацию о сетевом префиксе, адресе шлюза, MTU и множестве других параметров. При получении RA сообщения IPv6 хост устанавливает маршрутизатор по умолчанию в качестве рассылающего RA сообщения для реализации сетевой связности IPv6. Если вредоносный IPv6 хост посылает RA сообщения с целью подмены легитимного RA маршрутизатора, злоумышленник может получить доступ к пользовательской информации и заблокировать доступ к сети для пользователей. Поэтому, с целью сохранения безопасности и сохранения нормальной работы сети необходимо проверять и отбрасывать подозрительные RA сообщения.

59.2 Конфигурация IPv6 RA Security

1. Включить функцию IPv6 RA Security глобально;
2. Включить функцию IPv6 RA Security на порту;
3. Отобразить информацию о настройке и информацию отладки.

1. Включить функцию IPv6 RA Security глобально:

Команда	Описание

`ipv6 security-ra enable`
`no ipv6 security-ra enable`
 	
В режиме глобальной конфигурации
	Включить IPv6 RA Security глобально. Команда `no` отключает эту функцию.

2. Включить функцию IPv6 RA Security на порту:

Команда	Описание

`ipv6 security-ra enable`
`no ipv6 security-ra enable`
 	
В режиме глобальной конфигурации
	Включить IPv6 RA Security на порту. Команда `no` отключает эту функцию.

3. Отобразить информацию о настройке и информацию отладки:

Команда	Описание
`debug ipv6 security-ra` `no debug ipv6 security-ra`	Отображать отладочную информацию.

В привилегированном режиме	
`show ipv6 security-ra [interface <interface-list>]` В привилегированном режиме	Отобразить подробную информацию о функции IPv6 RA Security на интерфейсе `<interface-list>`

59.3 Пример конфигурации IPv6 RA Security

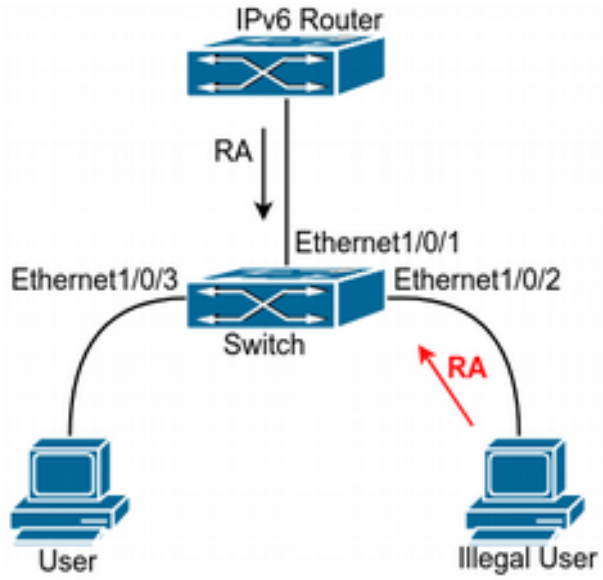


Рисунок 59.1 IPv6 RA Security

Если злоумышленник на схеме посылает RA-сообщения, то при получении такого сообщения обычным пользователем маршрутизатор по-умолчанию подменяется вредоносным IPv6 хостом. Вследствие этого пользователь не получает доступ в сеть. Необходимо установить функцию RA Security на порту коммутатора Ethernet1/0/2, чтобы RA сообщения от злоумышленников не смогли влиять на обычных пользователей.

Конфигурация будет выглядеть следующим образом:

```
Switch#config
Switch(config)#ipv6 security-ra enable
Switch(Config-If-Ethernet1/0/2)# ipv6 security-ra enable
```

60 Конфигурация MAB

60.1 Общие сведения о MAB

Во многих сетях присутствуют устройства (такие как сетевые принтеры, мобильные устройства и т.д), не имеющие возможности использовать проверку подлинности 802.1x К таким устройствам может быть применена аутентификация MAB (MAC Authentication Bypass), которая основывается на MAC-адресе устройства и порте доступа. Пользователю не нужно устанавливать ПО клиента аутентификации или вводить логин и пароль в процессе. Для аутентификации коммутатору достаточно получить ARP-пакет от MAB-пользователя и, после обнаружения соответствия аутентификационной информации на сервере, пользователю будет разрешен доступ.

В настоящий момент MAB поддерживает использование только RADIUS аутентификации. Используйте MAC-адрес пользователя в качестве логина и пароля, при настройке RADIUS-сервера.

60.2 Конфигурация MAB

1. Включить MAB функцию;
2. Настроить MAB username и password;
3. Настроить параметры MAB.

1. Включить MAB функцию:

Команда	Описание

`mac-authentication-bypass enable`
`no mac-authentication-bypass enable`
 	
В режиме глобальной конфигурации
	Включить функцию MAB глобально.
	Команда `no` отключает эту функцию.

`mac-authentication-bypass enable`
`no mac-authentication-bypass enable`
 	
В режиме конфигурации интерфейса
	Включить функцию MAB на порту.
	Команда `no` отключает эту функцию.

2. Настроить MAB username и password;

Команда	Описание
`mac-authentication-bypass username-format {mac-address | {fixed username WORD password WORD}}` В режиме глобальной конфигурации	Задать формат имени пользователя MAB: `mac-address` - будет передаваться MAC-адрес пользователя (по-умолчанию); `fixed username WORD password WORD` – передавать заданное имя пользователя и пароль

3. Настроить параметры MAB:

Команда	Описание

`mac-authentication-bypass guest-vlan <1-4094>`
`no mac-authentication-bypass guest-vlan`
 	
В режиме конфигурации интерфейса
	Задать гостевой VLAN. Команда `no` удаляет гостевой VLAN.

`mac-authentication-bypass binding-limit <1-100>`
`no mac-authentication-bypass binding-limit`
 	
В режиме конфигурации интерфейса
	Задать максимальное количество записей MAB на интерфейсе. Команда `no` возвращает значение по-умолчанию - 3 записи.

`mac-authentication-bypass timeout reauth-period <1-3600>`
`no mac-authentication-bypass timeout reauth-period`
 	
В режиме глобальной конфигурации
	Задать время начала повторной аутентификации после неудачной аутентификации. Команда `no` возвращает значение по-умолчанию - 30 секунд.

`mac-authentication-bypass timeout offline-detect (0 | <60-7200>)`
`no mac-authentication-bypass timeout offline-detect`
 	
В режиме глобальной конфигурации
	Задать время обнаружения пользователей offline и удаления записи MAB. Если задано значение 0, коммутатор не обнаруживает offline статус. Команда `no` возвращает значение по-умолчанию - 180 секунд

`mac-authentication-bypass timeout quiet-period <1-60>`
`no mac-authentication-bypass timeout quiet-period`
 	
В режиме глобальной конфигурации
	Задать время, в течении которого коммутатор не будет реагировать на запрос аутентификации от MAC после неудачной аутентификации этого MAC. Команда `no` возвращает значение по-умолчанию - 30 секунд

`mac-authentication-bypass timeout stale-period <0-60>`
`no mac-authentication-bypass timeout stale-period`
 	
В режиме глобальной конфигурации
	Задать время удаления записи MAB после перехода порта в состояние down. Команда `no` возвращает значение по-умолчанию - 30 секунд.

`mac-authentication-bypass timeout linkup-period <0-30>`
`no mac-authentication-bypass timeout linkup-period`
 	
В режиме глобальной конфигурации
	Задать время, восстановления состояния порта. Если период задан, то после обновления привязки VLAN порт будет переведен в состояние down, а по истечении заданного периода в up. Команда `no` отключает эту функцию.

`mac-authentication-bypass spoofing-garp-check enable`
`no mac-authentication-bypass spoofing-garp-check enable`
 	
В режиме глобальной конфигурации
	Включить функцию обнаружения атаки GARP-spoofing. Команда `no` отключает эту функцию.

`authentication mab {radius | local | none}`
`no authentication mab`
 	
В режиме глобальной конфигурации
	Задать порядок и приоритет методов аутентификации MAB. Чем ранее в команде прописан метод, тем он приоритетней. Команда **no** восстанавливает значение по-умолчанию (только radius).

60.3 Пример конфигурации MAB

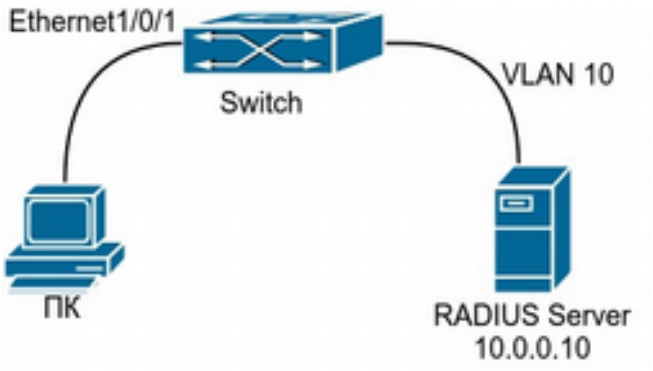


Рисунок 35.1 MAB

ПК пользователя подключен к порту Ethernet1/0/1 коммутатора. В соответствии с политикой безопасности, доступ в офисную сеть через VLAN10 предоставляется только после аутентификации на RADIUS-сервере, но для гостевых устройств предусмотрен гостевой VLAN 8. Сеть управления коммутатором, как и RADIUS-сервер, находится во VLAN 9.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)# mac-authentication-bypass enable
Switch(config)#vlan 8-10
Switch(config)#interface vlan 9
Switch(config-if-vlan9)ip address 10.0.0.9 255.255.255.0
Switch(config-if-vlan9)exit
Switch(config)#radius-server authentication host 10.0.0.10
Switch(config)#radius-server accounting host 10.0.0.10
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport mode hybrid
Switch(config-if-ethernet1/0/1)#switchport hybrid native vlan 8
Switch(config-if-ethernet1/0/1)#switchport hybrid allowed vlan 8;10
untag
Switch(config-if-ethernet1/0/1)#mac-authentication-bypass enable
Switch(config-if-ethernet1/0/1)#mac-authentication-bypass enable
guest-vlan 8
Switch(config-if-ethernet1/0/1)#exit
```

60.4 Решение проблем при конфигурации MAB

- Убедитесь, что функция MAB включена глобально;
- Убедитесь, что имя пользователя и пароль заданы верно;
- Убедитесь, что конфигурация пользователя на RADIUS-сервере верна.

61 PPPoE Intermediate Agent

61.1 Общие сведения о PPPoE Intermediate Agent

Протокол **PPPoE (Point to Point Protocol over Ethernet)** - протокол канального уровня передачи PPP кадров через Ethernet. PPPoE — это туннелирующий протокол, который позволяет инкапсулировать IP или другие протоколы через соединения Ethernet, устанавливая соединение «точка-точка», которое используется для транспортировки IP-пакетов. Такое соединение может быть установлено с BRAS, предоставляя пользователю широкополосный доступ и использующее аутентификацию.
PPPoE Intermediate Agent предоставляет возможность инкапсулировать в пакеты PPPoE данные о местоположении пользователя, что обеспечивает дополнительные возможности для проверки подлинности.
Существует 2 этапа в работе PPPoE: этап обнаружения и этап сеанса.
Этап обнаружения используется для получения MAC-адреса удаленного сервера для установления соединения «точка-точка» и идентификатора сеанса с сервером, а этап сеанса использует этот идентификатор сеанса для связи. PPPoE Intermediate Agent относится только к стадии обнаружения.

Этап обнаружения состоит из четырех шагов:

1. Клиент отправляет пакет **PADI (PPPoE Active Discovery Initiation)**. На первом шаге клиент использует широковещательный адрес как адрес назначения и широковещательный PADI (инициация активного обнаружения PPPoE) пакет для обнаружения концентратора доступа;
2. Сервер отправляет в ответ **PADO (PPPoE Active Discovery Offer).** Как только пользовательская машина отослала PADI-пакет, сервер отвечает, посылая PADO-пакет, используя MAC-адреса, пришедшие с PADI. PADO-пакет содержит MAC-адреса сервера, его имя и имя сервиса;
3. Клиент выбирает сервер, отсылая **PADR (PPPoE Active Discovery Request);**
4. Подтверждая полученный PADR-пакет, сервер посылает **PADS (PPPoE Active Discovery Session-confirmation)**, содержащий идентификатор сессии - Session ID

PPPoE Intermediate Agent перехватывает PADI и PADR пакеты, добавляя дополнительные данные, идентифицирующие местоположение пользователя, например MAC коммутатора, порт коммутатора, VLAN пользователя. PPPoE Intermediate Agent также включает в себя функцию доверенного порта, который позволяет заблокировать прием нежелательных PADO и PADS пакетов с недоверенных портов.

61.2 Конфигурация PPPoE Intermediate Agent

1. Настроить PPPoE Intermediate Agent глобально;
2. Настроить PPPoE Intermediate Agent на интерфейсе.

1. Настроить PPPoE Intermediate Agent глобально:

Команда	Описание

`pppoe intermediate-agent`
`no pppoe intermediate-agent`
 	
В режиме глобальной конфигурации
	Включить фунцию PPPoE Intermediate Agent, команда `no` отключает эту функцию

`pppoe intermediate-agent type tr-101 circuit-id access-node-id <string>`
`no pppoe intermediate-agent type tr-101 circuit-id access-node-id`
 	
В режиме глобальной конфигурации
	Настроить идентификатор узла доступа `<string>` с circuit-id tr-101 Команда no удаляет этот идентификатор.
	Формат circuit-id по-умолчанию: access-node-id +" eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID. Пример тега: "abcd eth 01/003:0003"

`pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp | sv | pv | spv} delimiter <WORD> [delimiter <WORD> ]`
`no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter`
 	
В режиме глобальной конфигурации
	Настроить добавляемые поля circuit-id формата tr-101. `sp` - слот и порт, `sv` - слот и vlan, `pv` - порт и vlan, `spv` - слот и порт и vlan. В случае использования `spv` может быть указано 2 различных разделителя `delimiter` друг за другом.
	
	Команда `no` возвращает формат по-умолчанию - `spv`. Формат circuit-id по-умолчанию: access-node-id +" eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID. Пример тега: "abcd eth 01/003:0003"

`pppoe intermediate-agent type self-defined circuit-id {vlan| port|id (switch-id (mac | hostname)| remote-mac) | string WORD}`
`no pppoe intermediate-agent type self-defined circuit-id`
 	
В режиме глобальной конфигурации
	Задать собственный формат circuit-id. Команда `no` удаляет эту конфигурацию.

`pppoe intermediate-agent type self-defined remoteid {mac | vlan-mac | hostname| string WORD}` `no pppoe intermediate-agent type self-defined remote-id`	Задать собственный формат remote-id. Команда `no` удаляет эту конфигурацию.

В режиме глобальной конфигурации	

`pppoe intermediate-agent delimiter <WORD>`
`no pppoe intermediate-agent delimiter`
 	
В режиме глобальной конфигурации
	Задать разделитель (#|.|,|;|:|/|space). Команда no возвращает разделитель по-умолчанию - '\'

`pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii)`
`no pppoe intermediate-agent format (circuit-id | remote-id)`
 	
В режиме глобальной конфигурации
	Задать формат представления circuit-id или remote-id. Команда `no` удаляет эту конфигурацию.

2. Настроить PPPoE Intermediate Agent на интерфейсе:

Команда	Описание

`pppoe intermediate-agent`
`no pppoe intermediate-agent`
 	
В режиме конфигурации интерфейса
	Включить фунцию PPPoE Intermediate Agent, команда `no` отключает эту функцию

`pppoe intermediate-agent vendor-tag strip`
`no pppoe intermediate-agent vendor-tag strip`
 	
В режиме конфигурации интерфейса
	Включить функцию снятия тега вендора на порту. Команда `no` отключает эту функцию.

`pppoe intermediate-agent trust`
`no pppoe intermediate-agent trust`
 	
В режиме конфигурации интерфейса
	Выбрать порт в качестве доверенного. Команда `no` выбирает порт в качестве недоверенного.

`pppoe intermediate-agent circuit-id <string>`
`no pppoe intermediate-agent circuit-id`
 	
В режиме конфигурации интерфейса
	Задать строку circuit-id, для добавления на порту. Команда no удаляет эту конфигурацию.

`pppoe intermediate-agent remote-id`	Задать строку remote-id, для

<string> no pppoe intermediate-agent remote-id В режиме конфигурации интерфейса	добавления на порту. Команда no удаляет эту конфигурацию.

61.3 Пример конфигурации PPPoE Intermediate Agent

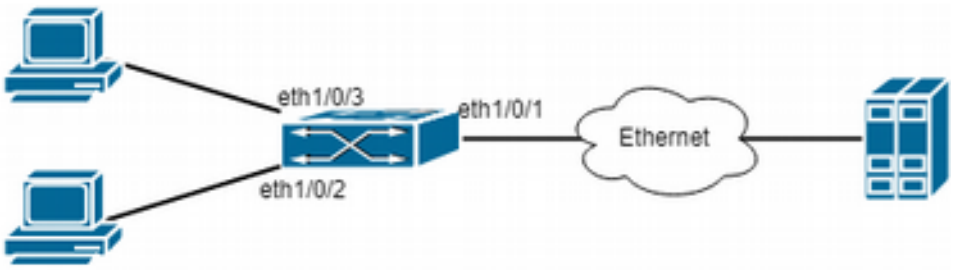


Рисунок 61.1 Конфигурация PPPoE IA

Как показано на рисунке 61.1, PPPoE клиент и сервер подключены к одной L2 Ethernet сети. На коммутаторе, к которому подключен клиент, активирована функция PPPoE Intermediate Agent.

Пример конфигурации 1:

```
Switch(config)#pppoe intermediate-agent
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust vendor-tag strip
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id abcd
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id aaaa
Switch (config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id xyz
```

В результате circuit-id для клиента в порту eth1/0/2 будет выглядеть как ”abcd eth 01/002:0001”, remote-id - MAC коммутатора ”0a0b0c0d0e0f”.
Для клиента в порту eth1/0/3 будет добавляться circuit-id ”aaaa”, remote-id ”xyz”.

Пример конфигурации 2:

```
Switch(config)#pppoe intermediate-agent
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent
Switch(config-if-ethernet1/0/3)#exit
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-
node-id abcd
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id
identifier-string efgh option spv delimiter # delimiter /
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent circuit-id
bbbb
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id xyz
```

В результате circuit-id для клиента в порту eth1/0/2 будет выглядеть как ”bbbb”, remote-id - MAC коммутатора ”0a0b0c0d0e0f”.
Для клиента в порту eth1/0/3 будет добавляться circuit-id ”efgh eth 01#003/1234, remote-id ”xyz”.

62 VLAN-ACL

62.1 Общие сведения о VLAN-ACL

Вы можете использовать ACL для VLAN, чтобы осуществлять контроль всех портов в этой VLAN, не применяя при этом ACL на каждом порту по-отдельности.

Если ACL для VLAN и ACL для порта применены одновременно, ACL для порта будет обработан раньше, чем ACL для VLAN.

Данный коммутатор поддерживает IP VLAN-ACL, MAC VLAN-ACL, IP-MAC VLAN-ACL и IPv6 ACL. Также на VLAN может быть применен userdefined ACL. На один VLAN может быть применен как один, так и несколько VLAN-ACL на входящее (ingress) направление трафика.

62.2 Конфигурация VLAN-ACL

1. Настроить IP VLAN-ACL;
2. Настроить MAC VLAN-ACL;
3. Настроить MAC-IP VLAN-ACL;
4. Настроить IPv6 VLAN-ACL;
5. Просмотр конфигурации и статистики VLAN-ACL;
6. Очистка статистики VLAN-ACL.

1. Настроить IP VLAN-ACL:

Команда	Описание

`vacl ip access-group {<1-299> | WORD} in [traffic-statistic] vlan <vlan-range>`
`no vacl ip access-group {<1-299> | WORD} м vlan <vlan-range>`
 	
В режиме глобальной конфигурации
	Применить IP-ACL `{<1-299> | WORD}` на входящее направление трафика на VLAN `<vlan-range>`. С включенной опцией `traffic-statistic` коммутатор будет подсчитывать совпадения этой `access-group`
	Удалить IP-ACL `{<1-299> | WORD}` с VLAN

2. Настроить MAC VLAN-ACL:

Команда	Описание
`vacl mac access-group {<700-1199> | WORD} in [traffic-statistic] vlan <vlan-range>` `no vacl mac access-group {<700-1199> | WORD} in vlan <vlan-range>`	Применить IP-ACL `{<700-1199> | WORD}` на входящее направление трафика на VLAN `<vlan-range>`. С включенной опцией `traffic-statistic` коммутатор будет подсчитывать совпадения этой

В режиме глобальной конфигурации	`access-group` Удалить IP-ACL `{<700-1199> | WORD}` с VLAN

3. Настроить MAC-IP VLAN-ACL:

Команда	Описание

`vacl mac-ip access-group {<3100-3299> | <acl-name>} in [traffic-statistic] vlan <vlan-range>`
`no vacl mac-ip access-group {<3100-3299> | <acl-name>} in vlan <vlan-range>`
 	
В режиме глобальной конфигурации
	Применить MAC-IP-ACL `{<3100-3299> | <acl-name>}` на входящее направление трафика на VLAN `<vlan-range>`. С включенной опцией `traffic-statistic` коммутатор будет подсчитывать совпадения этой `access-group`. Удалить ACL `{<3100-3299> | <acl-name>}` с VLAN `<vlan-range>`

4. Настроить IPv6 VLAN-ACL:

Команда	Описание

`vacl ipv6 access-group {<500-699> | <acl-name>} in [traffic-statistic] vlan <vlan-range>`
`no ipv6 access-group {<500-699> | <acl-name>} in vlan <vlan-range>`
 	
В режиме глобальной конфигурации
	Применить IPv6 ACL `<{<500-699> | <acl-name>}` на входящее направление трафика на VLAN `<vlan-range>`. С включенной опцией `traffic-statistic` коммутатор будет подсчитывать совпадения этой `access-group`. Удалить ACL `{<500-699> | <acl-name>}` с VLAN

5. Назначить ACL на VLAN:

Команда	Описание
`[no] vacl userdefined access-group <1200-1399> in vlan <vlan-range> [traffic-statistic]` В режиме глобальной конфигурации	Применить ACL `<1200-1399>` на входящее направление трафика на VLAN `<vlan-range>`. С включенной опцией `traffic-statistic` коммутатор будет подсчитывать совпадения этой `access-group`. Удалить ACL `<1200-1399>` с VLAN

6. Просмотр конфигурации и статистики VLAN-ACL:

Команда	Описание
`show vacl in vlan [<vlan-id>]` В привилегированном режиме	Отобразить конфигурацию и статистику VLAN-ACL для VLAN, при указании `<vlan-id>` информация будет отображена только для конкретной VLAN.

7. Очистка статистики VLAN-ACL:

Команда	Описание
`clear vacl in statistic vlan [<vlan-id>]` В привилегированном режиме	Очистить статистику VLAN-ACL для VLAN, при указании `<vlan-id>` информация будет очищена только для конкретной VLAN.

62.3 Пример конфигурации VLAN-ACL

Для VLAN 1 и 2 необходимо разрешить прохождение только трафика сети 192.168.1.0\24, весь остальной трафик необходимо запретить.

Конфигурация будет выглядеть следующим образом:

```
Switch(config)#ip access-list extended vacl_a
Switch(config-ip-ext-nacl-vacl_a)#permit ip any-source 192.168.1.0
0.0.0.255
Switch(config-ip-ext-nacl-vacl_a)#deny ip any-source any-destination
Switch(config-ip-ext-nacl-vacl_a)#exit
Switch(config)#firewall enable
Switch(config)#vacl ip access-group vacl_a in vlan 1-2
```

63 SAVI

63.1 Общие сведения о SAVI

SAVI (Source Address Validation Improvement) - технология, которая позволяет осуществлять проверку подлинности IP-адресов в пределах локальной сети и контролировать их валидность. Когда устройство начинает передавать данные через порт, где задействован функционал SAVI, протокол SAVI инициирует проверку по таблице доверенных хостов: если данный адрес ранее не был привязан ни к одному порту, SAVI создает запись соответствия. Если информация об этом адресе уже содержится в таблице, SAVI осуществляет проверку присутствия адреса на порту, информация о котором содержится в таблице. Если адрес более не отвечает на запросы, SAVI создает новую запись в таблице взамен старой.

Для корректной работы SAVI необходимо включить функцию ND Snooping, DHCPv6 Snooping или RA Snooping в соответствии с типом протокола обрабатываемого пакета.

63.2 Конфигурация SAVI

1. Включить функцию SAVI;
2. Задать метод обнаружения SAVI;
3. Добавить записи в таблицу SAVI;
4. Задать время обнаружения в таблице SAVI;
5. Задать время перезаписи в таблице SAVI;
6. Задать время жизни для записи SLAAC;
7. Задать время защиты записи;
8. Включить функцию проверки префикса;
9. Задать префикс CPS вручную;
10. Задать максимальное количество записей с одним MAC;
11. Настроить метод проверки при обнаружении конфликта записей;
12. Включить контроль проверки подлинности;
13. Назначить доверенный порт DHCPv6;
14. Назначить доверенный порт ND;
15. Задать максимальное количество записей SAVI для порта.

1. Включить функцию SAVI:

Команда	Описание

`savi enable`
`no savi enable`
 	
В режиме глобальной конфигурации
	Включить функцию SAVI; Команда `no` отключает эту функцию.

2. Задать метод обнаружения SAVI:

Команда	Описание

`savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable`
`no savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable`
 	
В режиме глобальной конфигурации
	Включить метод обнаружения: `dhcp-only` - коммутатор будет проверять только DHCPv6 пакеты и DAD NS пакеты link-local адреса с назначенным IPv6 адресом; `slaac-only` - проверять только не link-local DAD NS; `dhcp-slaac` – проверять DHCPv6 и все типы пакетов DAD NS. Команда `no` отключает метод обнаружения.

3. Добавить записи в таблицу SAVI

Команда	Описание

`savi ipv6 check source binding ip <ipv6-address> mac <mac-address> interface <if-name> {type [slaac | dhcp] lifetime <lifetime> | type static}`
`no savi ipv6 check source binding ip <ipv6-address> interface <if-name>`
 	
В режиме глобальной конфигурации
	Создать запись в таблице SAVI для IP-адреса `<ipv6-address>`, MAC-адреса `<mac-address>` и интерфейса `<if-name>`. `type [slaac | dhcp] lifetime <lifetime>` создает динамическую запись выбранного типа с временем жизни в секундах `<lifetime>`, `type static` создает статическую запись. Команда `no` удаляет эту запись.

4. Задать время обнаружения в таблице SAVI:

Команда	Описание

`savi max-dad-delay <max-dad-delay>`
`no savi max-dad-delay`
 	
В режиме глобальной конфигурации
	Настроить время нахождения динамической записи в состоянии DETECTION. Команда `no` восстанавливает значение по-умолчанию - 1 секунда.

5. Задать время перезаписи в таблице SAVI:

Команда	Описание
`savi max-dad-prepare-delay <max-dad-prepare-delay>` `no savi max-dad-prepare-delay`	Задать время повторного обнаружения динамической записи в секундах. Команда `no` восстанавливает значение по-

В режиме глобальной конфигурации	умолчанию - 1 секунда.

6. Задать время жизни для записи SLAAC:

Команда	Описание

`savi max-slaac-life <max-slaac-life>`
`no savi max-slaac-life`
 	
В режиме глобальной конфигурации
	Задать время жизни записи типа SLAAC, в секундах.Команда `no` восстанавливает значение по-умолчанию - 14400 секунд (4 часа).

7. Задать время защиты записи:

Команда	Описание

`savi timeout bind-protect <protect-time>`
`no savi timeout bind-protect`
 	
В режиме глобальной конфигурации
	Задать время хранения записи в таблице SAVI после обнаружения перехода порта в состояние DOWN. Команда `no` восстанавливает значение по-умолчанию - 30 секунд.

8. Включить функцию проверки префикса:

Команда	Описание

`ipv6 cps prefix check enable`
`no ipv6 cps prefix check enable`
 	
В режиме глобальной конфигурации
	Включить функцию проверки соответствия префикса адреса заданному префиксу vlan. Команда `no` отключает эту функцию.

9. Задать префикс CPS вручную:

Команда	Описание

`ipv6 cps prefix <ip-address> vlan <vid>`
`no ipv6 cps prefix <ip-address>`
 	
В режиме глобальной конфигурации
	Задать префикс для vlan вручную. Команда `no` удаляет эту запись.

10. Задать максимальное количество записей с одним MAC:

Команда	Описание
`savi ipv6 mac-binding-limit <limit-`	Задать максимальное количество

num> no savi ipv6 mac-binding-limit В режиме глобальной конфигурации	записей в таблице SAV с одним MAC адресом. Команда no восстанавливает значение по-умолчанию - 32 записи.

11. Настроить метод проверки при обнаружении конфликта записей:

Команда	Описание
savi check binding <simple | probe> mode no savi check binding mode В режиме глобальной конфигурации	Задать метод проверки существующей записи если присутствует конфликт в вновь создаваемой: simple - проверить только состояние порта; probe - отправить NS пакет.

12. Включить контроль проверки подлинности для double-stack:

Команда	Описание
savi ipv6 check source [ipv6-address mac-address | ipv4-address | mac-address] no savi ipv6 check source В режиме конфигурации интерфейса	Включить функцию контроля проверки подлинности пользователя для double-stack сети, создать запись в таблице. Команда no отключает эту функцию. .

13. Назначить доверенный порт DHCPv6:

Команда	Описание
ipv6 dhcp snooping trust no ipv6 dhcp snooping trust В режиме конфигурации интерфейса	Назначить доверенный порт DHCPv6 Snooping. Команда no назначает порт как недоверенный.

14. Назначить доверенный порт ND:

Команда	Описание
ipv6 nd snooping trust no ipv6 nd snooping trust В режиме конфигурации интерфейса	Назначить доверенный порт ND Snooping. Команда no назначает порт как недоверенный.

15. Задать максимальное количество записей SAVI для порта:

Команда	Описание

`savi ipv6 binding num <limit-num>`
`no savi ipv6 binding num`
 	
В режиме конфигурации интерфейса
	Задать лимит записей SAVI для порта; Команда `no` восстанавливает значение по-умолчанию - 65535 записей.

63.2 Пример конфигурации SAVI

На рабочих станциях ПК1 и ПК2, которые подключены к портам коммутатора доступа “Switch” Ethernet1/0/12 и Ethernet1/0/13 соответственно, установлен IPv6 протокол. На коммутаторе включена функция SAVI. Порты Ethernet1/0/1 магистральный порт коммутатора, поэтому него необходимо назначить доверенным для протоколов DHCPv6 и ND. На коммутаторе агрегации “Switch_Aggr” запущен DHCPv6 сервер и включена функция RA.
Конфигурация коммутатора доступа будет выглядеть следующим образом:

```
Switch(config)#savi enable
Switch(config)#savi ipv6 dhcp-slaac enable
Switch(config)#savi check binding probe mode
Switch(config)#interface ethernet1/0/1
Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust
Switch(config-if-ethernet1/0/1)#ipv6 nd snooping trust
Switch(config-if-ethernet1/0/1)#exit
Switch(config)#interface ethernet1/0/12-13
Switch(config-if-port-range)#savi ipv6 check source ip-address mac-
address
Switch(config-if-port-range)#savi ipv6 binding num 4
Switch(config-if-port-range)#exit
```

63.2 Решение проблем при конфигурации SAVI

- Если после включения SAVI IPv6 пакеты фильтруются некорректно, удостоверьтесь, что функция SAVI включена глобально, выбрана верный метод обнаружения и/или проверка подлинности пользователя на порту включена;
- Если пользователи не могут корректно получить адрес через DHCPv6, удостоверьтесь, что порт в сторону DHCPv6 сервера назначен как доверенный;
- Если новый пользователь не может быть добавлен в таблицу SAVI, убедитесь, что количество записей в таблице (как для MAC, так и для порта) не достигло максимального значения.

64 MRPP

64.1 Общие сведения о MRPP

MRPP (Mult-layer Ring Rrotection Protocol), протокол канального уровня применяемый для защиты от петель в кольцевой топологии Ethernet. Он позволяет предотвратить возникновение широковещательного шторма в кольце, при этом восстановить связность при разрыве одного из линков в кольце.

Протокол MRPP по функциональному назначению похож на STP, но предназначен для использования только в топологии кольца и имеет низкое время сходимости, в некоторых условиях не превышающее 50-100мс.

64.1.1 Основные понятия

1. **Control VLAN**

Control VLAN - это виртуальная VLAN, которая используется только я идентификации пакетов MRPP, передаваемых в сети. Номер VLAN MRPP может пересекаться с номером VLAN, уже используемой в сети, но во избежании путаницы рекомендуется использовать для MRPP уникальную VLAN.

2. **MRPP Ring**

Под MRPP ring понимается используемая в Ethernet сети кольцевая топология. MRPP ring может находиться в двух состояниях: Health state - замкнутое состояние, все соединения кольца активны; Break state - разомкнутое состояние, одно или несколько соединений кольца нарушены.

3. **Node type**

Каждый коммутатор выполняет одну из двух ролей в MRPP ring: Primary node и Transfer node. Primary node - основной узел, который выполняет рассылку MRPP сообщений и принимает решение о разрыве или соединении линка кольца. Transfer node - каждый узел, не являющийся Primary node. Роль узла определяется конфигурацией пользователя. Как показано на рисунке 38.1, коммутатор SwitchA является Primary node, а все остальные - Transfer node.

4. **Primary и Secondary порты**

Каждый коммутатор в кольце имеет 2 подключенных к сети порта Primary (первичный) и Secondary (вторичный). Роли портов определяются конфигурацией пользователя.

Первичный порт коммутатора Primary Node используется для отправки пакета проверки работоспособности кольца (Hello), вторичный порт используется для приема этого пакета. Когда кольцо находится в замкнутом состоянии, вторичный порт на Primary Node блокирует весь остальной трафик, кроме пакетов Hello. Когда кольцо находится в разомкнутом состоянии, вторичный порт Primary Node пересылает пакеты данных.

5. **Таймер**

MRPP предусматривает 2 таймера: Hello-Timer - определяет интервал отправки Hello пакетов; Fail-Timer - определяет время разблокировки Secondary порта при неполучении Hello пакета, равен трем интервалам Hello.

64.1.2 Типы пакетов MRPP

Hello packet - рассылается первичным портом (Primary port) и используется для

обнаружения кольца. Если вторичный порт Primary Node может принимать Hello-пакеты, кольцо считается замкнутым;

LINK-DOWN event packet - после того, как Transfer node обнаружил событие Down на порту, он посылает этот пакет на Primary Node для информирования о разрыве кольца;

LINK-DOWN-FLUSH-FDB packet - рассылается Primary Node для обновления таблицы MAC-адресов после того, как Primary Node обнаружил разрыв кольца или принял LINK-DOWN event packet и разблокировал Secondary порт;

LINK-UP-FLUSH-FDB packet - рассылается Primary Node для обновления таблицы MAC-адресов после того, как Primary Node обнаружил замыкание кольца и заблокировал Secondary порт.

64.1.3 Операций протокола MRPP

1. **Обнаружение разрыва линка:**

Когда Transfer Node обнаруживает состояние DOWN на кольцевом порту, он отправляет LINK-DOWN пакет на Primary Node. Получив LINK-DOWN пакет Primary Node немедленно освобождает Secondary порт из состояния Block, а также отправляет LINK-DOWN-FLUSH-FDB пакет для информирования транзитных узлов о необходимости обновить таблицу MAC.

2. **Опрос кольца:**

Primary Node отправляет через первичный порт Hello пакет в соответствии с настроенным интервалом. Если кольцо замкнуто, Secondary порт на Primary Node получает Hello-пакеты, и Primary Node блокирует трафик на это порту. Если кольцо разомкнуто, Secondary порт на Primary Node не может принимать Hello-пакеты и он выходит из состояния Block.

3. **Восстановление кольца:**

После того, как Primary Node обнаружил разрыв кольца, если Secondary порт получает Hello пакет, это будет означать, что кольцо восстановлено. Поэтому Primary Node блокирует свой Secondary порт и отправляет своим соседям LINK-DOWN-FLUSH-FDB.
Если порт на транзитном узле в MRPP кольце перешел в состояние UP, Primary Node не сразу найти замкнутое состояние кольца и создать широковещательный шторм. Чтобы избежать такого нежелательного поведения, транзитный узел блокирует измениший свое состояние порт до получения LINK-DOWN-FLUSH-FDB, пропуская только трафик MRPP VLAN.

64.2 Конфигурация MRPP

1. Включить MRPP;
2. Настроить MRPP кольцо;
3. Настроить метод обнаружения падения порта;
4. Настроить режим совместимости;
5. Просмотр информации о конфигурации и отладка.

1. Включить MRPP:

Команда	Описание

`mrpp enable`
`no mrpp enable`
 	
В режиме глобальной конфигурации
	Выключить MRPP на коммутаторе, команда no отменяет это действие.

2. Настроить MRPP кольцо:

Команда	Описание

`mrpp ring <ring-id>`
`no mrpp ring <ring-id>`
 	
В режиме глобальной конфигурации
	Создать кольцо MRPP `<ring-id>` и войти в режим его конфигурирования. Команда `no` удаляет кольцо MRPP.

`control-vlan <vid>`
`no control-vlan`
 	
в режиме конфигурации кольца MRPP
	Задать VLAN для управления MRPP, команда `no` удаляет эту VLAN.

`node-mode {master | transit}` в режиме конфигурации кольца MRPP	Задать тип узла MRPP

`hello-timer < timer>`
`no hello-timer`
 	
в режиме конфигурации кольца MRPP
	Задать интервал отправки Hello пакетов. Команда `no` возвращает значение по-умолчанию - 1 секунда.

`fail-timer <timer>`
`no fail-timer`
 	
в режиме конфигурации кольца MRPP
	Задать время, по истечении которого кольцо будет считаться разорванным. Команда `no` возвращает значение по-умолчанию - 3 секунды.

`enable`
`no enable`
 	
в режиме конфигурации кольца MRPP
	Задействовать кольцо MRPP, команда no переводит кольцо в неактивный режим (по-умолчанию)

`mrpp ring <ring-id> primary-port`
`no mrpp ring <ring-id> primary-port`
в режиме конфигурации интерфейса
	Выбрать текущий порт в качестве Primary. Команда `no` отменяет выбор.

`mrpp ring <ring-id> secondary-port`
`no mrpp ring <ring-id> secondary-port`
 	
в режиме конфигурации интерфейса
	Выбрать текущий порт в качестве Secondary. Команда `no` отменяет выбор.

3. Настроить метод обнаружения падения порта:

Команда	Описание
`port-scan-mode {interrupt | poll}` В режиме глобальной конфигурации	Задать метод обнаружения падения порта: `interrupt` – по событию, `poll` - по опросу.
`mrpp poll-time <20-2000>` В режиме глобальной конфигурации	Настроить интервал опроса состояния порта MRPP (в миллисекундах)

4. Настроить режим совместимости:

Команда	Описание

`mrpp errp compatible`
`no mrpp errp compatible`
 	
В режиме глобальной конфигурации
	Включить режим совместимости с ERPP, команда `no` отключает режим совместимости.

`mrpp eaps compatible`
`no mrpp eaps compatible`
 	
В режиме глобальной конфигурации
	Включить режим совместимости с EARS, команда `no` отключает режим совместимости.

`errp domain <domain-id>`
`no errp domain <domain-id>`
 	
В режиме глобальной конфигурации
	Создать домен ERPP, команда `no` удаляет этот домен

5. Просмотр информации о конфигурации и отладка:

Команда	Описание
`debug mrpp` `no debug mrpp`	Включить вывод отладки MRPP, команда `no` выключает вывод

В привилегированном режиме	отладки.
`show mrpp {<ring-id>}` В привилегированном режиме	Вывести информацию о конфигурации кольца MRPP
`show mrpp statistics {<ring-id>}` В привилегированном режиме	Вывести статистику о переданных и принятых пакетах MRPP
`clear mrpp statistics {<ring-id>}` В привилегированном режиме	Очистить статистику о переданных и принятых пакетах MRPP

64.3 Пример конфигурации MRPP

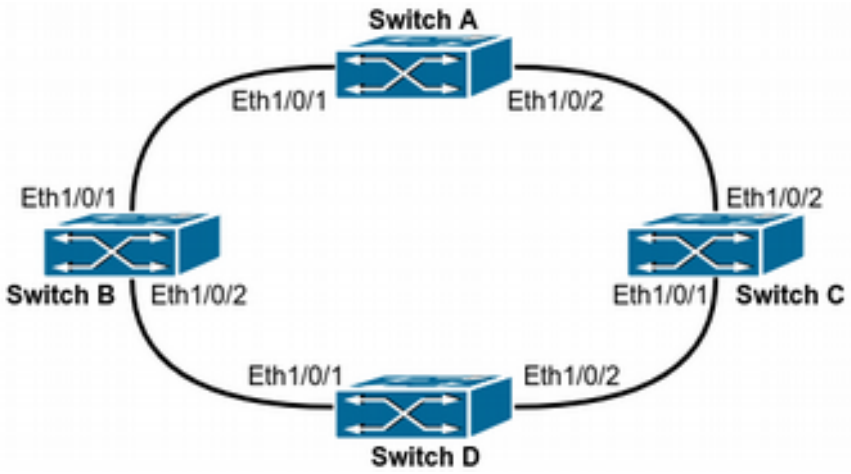


рисунок 64.1 Конфигурация MRPP

Представленная выше топология позволяет использовать MRPP в качестве протокола защиты от петли. Коммутатор Switch A является основным узлом MRPP-кольца 4000, порт Eth 1/0/1 – Primary порт, E1/0/2 – Secondary. Остальные узлы являются транзитными (Transfer) узлами MRPP-кольца 4000 с настроенными основным и дополнительным портами.

Конфигурация коммутатора Switch A:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#fail-timer 18
Switch(mrpp-ring-4000)#hello-timer 5
Switch(mrpp-ring-4000)#node-mode master
```

```
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
```

Конфигурация коммутаторов Switch B, C и D:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
```

64.4 Решение проблем при конфигурации MRPP

Нормальная работа MRPP-протокола зависит от корректной конфигурации коммутаторов внутри MRPP-кольца, однако есть вероятность возникновения широковещательного шторма и петель:

- Не замыкайте кольцо до полной конфигурации всех коммутаторов в нем;
- Если при корректной конфигурации возникает широковещательный шторм или блокирование кольца, используйте функцию отладки на основном узле MRPP, а также информационные команды, отображающие статистику по основному узлу и транспортным узлам сети;

65 ULPP

65.1 Общие сведения о ULPP

Протокол ULPP (User Level Protocol Process) предназначен резервирования каналов и защиты от петель в Ethernet сетях. Каждая группа ULPP имеет два uplink порта – основной (master) и дополнительный порт (slave). Порт может быть как физическим портом, так и port-channel. Порты группы могут иметь три статуса: передача (forwarding), ожидание (standby) и выключен (down). Для резервирования, как правило, один порт имеет статус передачи, а другой заблокирован в режиме ожидания. Если появляется проблема с линком на основном порту и он переходит в статус DOWN, дополнительный порт переключается в режим передачи.

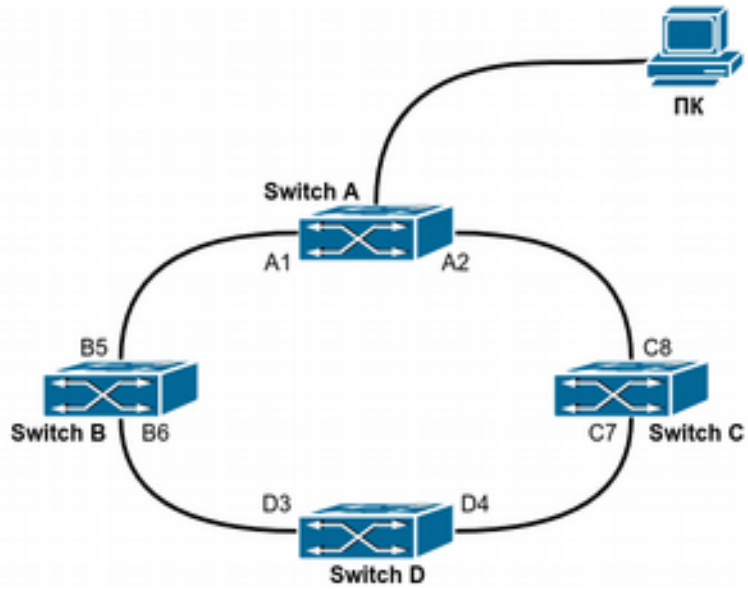


рисунок 65.1 ULPP

Типичная схема применения ULPP показана на рисунке 65.1. Коммутатор Switch A соединяется с коммутатором Switch D через коммутаторы Switch B и Switch C, порты A1 и A2 – uplink порты. На коммутаторе Switch A настраивается ULPP, порт A1 устанавливается как основной порт, порт A2 – как дополнительный. Если на порту A1 появляется проблема, порт A2 незамедлительно переключается в статус передачи. Если приоритетный режим не сконфигурирован на основном порту, то после его восстановления порт A2 останется в статусе передачи, порт A1 будет по-прежнему заблокирован в режиме ожидания. Если приоритетный режим на основном порту сконфигурирован, то порт A1 меняет статус с режима ожидания на режим передачи. Чтобы избежать частого переключения режимов на uplink порту, может быть настроен механизм отложенного приоритетного режима.

После восстановления порта в приоритетном режиме, если через дополнительный порт осуществлялась передача данных к Switch A от коммутатора Switch D, коммутатор продолжит отправлять данные в сторону дополнительного порта, который будет закрыт. Чтобы этого избежать, при переключении uplink коммутатор отправит flush-пакеты через

порт, переключившийся в режим передачи, чтобы обновить таблицы MAC-адресов и ARP-таблицы на остальных устройствах в сети.

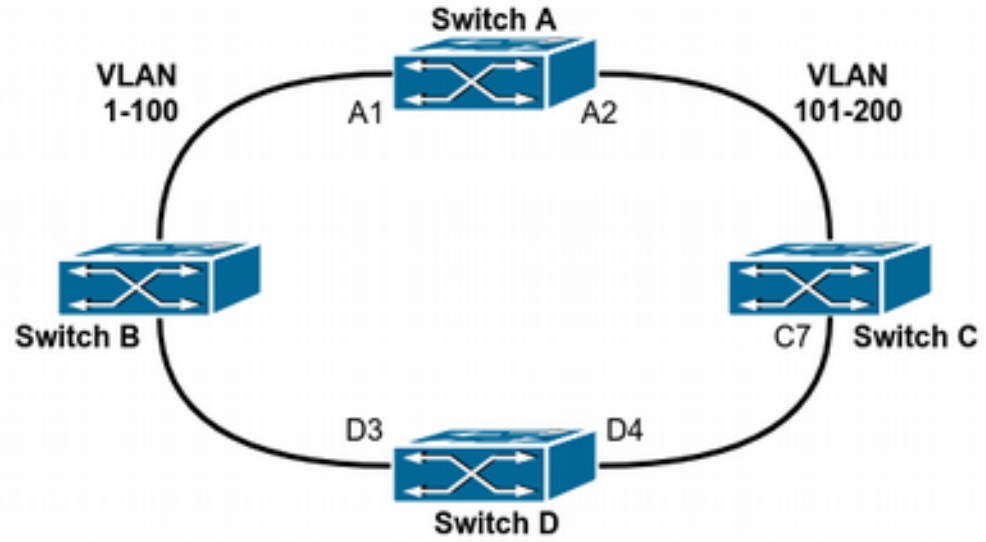


рисунок 65.2 ULPP VLAN

Для более эффективного распределения ресурсов ULPP может балансировать нагрузку по VLAN. Как показано на рисунке 65.2, коммутатор Switch A поддерживает две ULPP-группы: порт A1 является основным портом, порт A2 – дополнительным в группе 1; порт A2 является основным портом, порт A1 – дополнительным в группе 2. Сети VLAN защищены группами 1 и 2, на схеме соответственно 1-100 и 101-200. В данном случае оба порта A1 и A2 имеют взаимное резервирование и находятся в режиме переадресации, а также выполняют передачу пакетов разных VLAN. Когда на порту A1 возникает проблема, трафик из VLAN 1-100 передается через порт A2. После восстановления порта A1 данные из VLAN 101-200 продолжают передаваться через порт A2, но данные из VLAN 1-100 переключаются на порт A1

65.2 Конфигурация ULPP

1. Создать ULPP группу;
2. Настроить ULPP группу;
3. Просмотр информации и отладка.

1. Создать ULPP группу:

Команда	Описание

`ulpp group <integer>`
`no ulpp group <integer>`
 	
В режиме глобальной конфигурации
	Создать нумерованную ULPP группу и войти в режим её конфигурирования, команда `no` удаляет эту группу

2. Настроить ULPP группу:

Команда	Описание

`preemption mode`
`no preemption mode`
 	
В режиме конфигурации ULPP группы
	Включить режим приоритетного переключения, команда `no` отключает этот режим

`preemption delay <integer>`
`no preemption delay`
 	
В режиме конфигурации ULPP группы
	Задать время задержки перед приоритетным переключением. Команда no возвращает значение по-умолчанию - 30 секунд.

`control vlan <integer>`
`no control vlan`
 	
В режиме конфигурации ULPP группы
	Задать VLAN отправки служебных пакетов. Команда no возвращает значение по-умолчанию - 1.

`protect vlan-reference-instance <instance-list>`
`no protect vlan-reference-instance <instance-list>`
 	
В режиме конфигурации ULPP группы
	Задать VLAN, защищаемые ULPP группой. Команда `no` удаляет эти VLAN из группы.

`flush enable mac`
`flush disable mac`
 	
В режиме конфигурации ULPP группы
	Включить\выключить функцию отправки flush пакета для обновления MAC-таблицы.

`flush enable arp`
`flush disable arp`
 	
В режиме конфигурации ULPP группы
	Включить\выключить функцию отправки flush пакета для обновления ARP-таблицы.

`flush enable mac-vlan`
`flush disable mac-vlan`
 	
В режиме конфигурации ULPP группы
	Включить\выключить функцию отправки flush пакета для удаления MAC из MAC-VLAN.

`description <string>`
`no description`
 	
В режиме конфигурации ULPP группы
	Задать описание. Команда `no` удаляет описание.

`ulpp control vlan <vlan-list>` `no ulpp control vlan <vlan-list>`	Задать список управляющих VLAN, которые принимают flush-пакеты.

В режиме конфигурации интерфейса	Команда no возвращает настройки по умолчанию – 1.

`ulpp flush enable mac`
`ulpp flush disable mac`
 	
В режиме конфигурации интерфейса
	Включить\выключить функцию приема flush пакета для обновления MAC-таблицы.

`ulpp flush enable arp`
`ulpp flush disable arp`
 	
В режиме конфигурации интерфейса
	Включить\выключить функцию приема flush пакета для обновления ARP-таблицы.

`ulpp flush enable mac-vlan`
`ulpp flush disable mac-vlan`
 	
В режиме конфигурации интерфейса
	Включить\выключить функцию приема flush пакета для удаления MAC из MAC-VLAN.

`ulpp group <integer> master`
`no ulpp group <integer> master`
 	
В режиме конфигурации интерфейса
	Выбрать порт как основной для группы `<integer>`. Команда `no` отменяет этот выбор.

`ulpp group <integer> slave`
`no ulpp group <integer> slave`
 	
В режиме конфигурации интерфейса
	Выбрать порт как дополнительный для группы `<integer>`. Команда `no` отменяет этот выбор.

3. Просмотр информации и отладка:

Команда	Описание
`show ulpp group [group-id]` В привилегированном режиме	Отобразить информацию о конфигурации ULPP группы.
`show ulpp flush counter interface {ethernet <IFNAME> | <IFNAME>}` В привилегированном режиме	Отобразить счетчики flush пакетов на интерфейсе.
`show ulpp flush-receive-port` В привилегированном режиме	Отобразить информацию о порте, получившем flush-пакет, типе пакета и управляющем VLAN.
`clear ulpp flush counter interface <name>`	Очистить счетчики flush пакетов на интерфейсе

В привилегированном режиме	

`debug ulpp flush {send | receive} interface <name>`
`no debug ulpp flush {send | receive} interface <name>`
 	
В привилегированном режиме
	Выводить отладочную информацию о принятых или полученных flush пакетах. Команда `no` отключает вывод отладочной информации.

`debug ulpp flush content interface <name>`
`no debug ulpp flush content interface <name>`
 	
В привилегированном режиме
	Выводить отладочную информацию о содержании flush пакетов. Команда `no` отключает вывод отладочной информации.

`debug ulpp error`
`no debug ulpp error`
 	
В привилегированном режиме
	Выводить отладочную информацию о ошибках ULPP. Команда `no` отключает вывод отладочной информации.

`debug ulpp event`
`no debug ulpp event`
 	
В привилегированном режиме
	Выводить отладочную информацию о событиях ULPP. Команда `no` отключает вывод отладочной информации.

65.3 Пример конфигурации ULPP

Пример 1

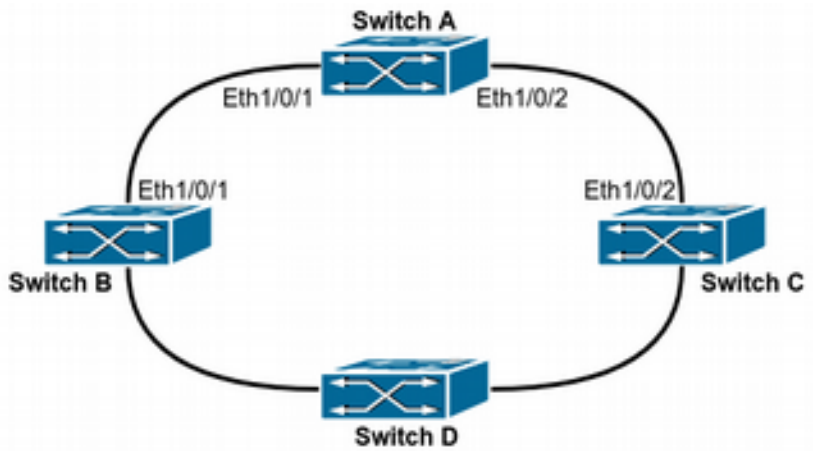


рисунок 65.3 Пример ULPP

Как показано на рисунке 65.3, коммутатор Switch A имеет два uplink – коммутаторы Switch B и Switch C. На коммутаторе Switch A настроен протокол ULPP и основной и

дополнительный порты в ULPP-группе. Когда оба порта в находятся состоянии UP, основной порт работает в режиме передачи, а дополнительный порт находится в режиме ожидания. Если основной порт переходит в состояние DOWN, дополнительный порт незамедлительно переключается в режим передачи. На коммутаторах Switch B и Switch C выполняется команда, позволяющая получать flush пакеты, и используемая для связывания ULPP-протокола с Switch A и немедленного переключения uplink.

Конфигурация коммутатора Switch A:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/1; 1/0/2
Switch(Config-vlan10)#exit
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 10
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#control vlan 10
Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)#exit
```

Конфигурация коммутатора Switch B:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/1
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/1)# ulpp flush enable arp
Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10
```

Конфигурация коммутатора Switch C：

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/2
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/2)# ulpp flush enable arp
Switch(config-If-Ethernet1/0/2)# ulpp control vlan 10
```

Пример 2:

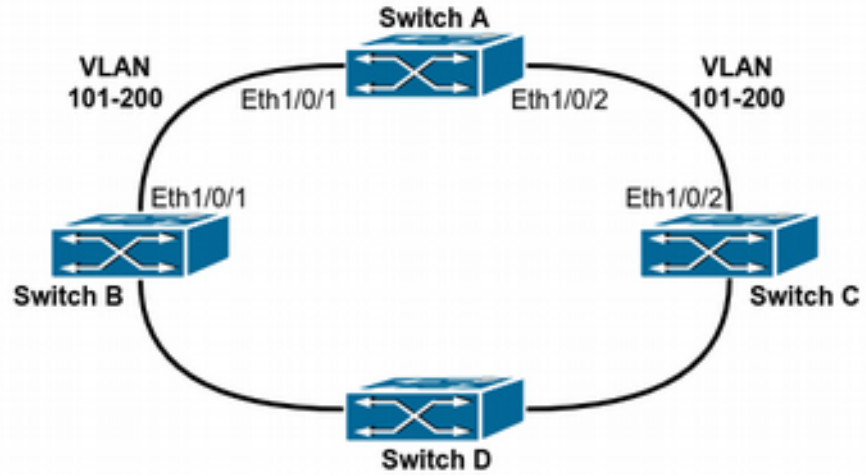


рисунок 65.4 Пример ULPP per VLAN

ULPP может балансировать нагрузку по VLAN. Как показано на рисунке 39.4, порт Eth1/0/1 основной, а порт Eth1/0/2 - дополнительный в группе 1, порт Eth1/0/2 - основной, порт Eth1/0/1 - дополнительный в группе 2. Группа 1 защищает диапазон VLAN 1-100, группа 2 защищает диапазон VLAN 101-200. В данном случае оба порта Eth1/0/1 и Eth1/0/2 имеют взаимное резервирование и находятся в режиме передачи, а также выполняют передачу пакетов разных VLAN. Когда на порту Eth1/0/1 возникает проблема, трафик из VLAN 1-100 передается через порт Eth1/0/2. После восстановления порта Eth1/0/1 данные из VLAN 101-200 продолжают передаваться через порт Eth1/0/2, но данные из VLAN 1-100 переключаются на порт Eth1/0/1.

Конфигурация коммутатора Switch A:

```
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1-100
Switch(Config-Mstp-Region)#instance 2 vlan 101-200
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#preemption mode
Switch(ulpp-group-1)#exit
Switch(Config)#ulpp group 2
Switch(ulpp-group-2)#protect vlan-reference-instance 2
Switch(ulpp-group-1)#preemption mode
Switch(ulpp-group-2)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#switchport mode trunk
Switch(config-If-Ethernet1/0/1)#ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#ulpp group 2 slave
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
```

```
Switch(config-If-Ethernet1/0/2)#switchport mode trunk
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)# ulpp group 2 master
Switch(config-If-Ethernet1/0/2)#exit
```

Конфигурация коммутатора Switch B:

```
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#switchport mode trunk
Switch(config-If-Ethernet1/0/1)#ulpp flush enable mac
Switch(config-If-Ethernet1/0/1)#ulpp flush enable arp
```

Конфигурация коммутатора Switch C:

```
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#switchport mode trunk
Switch(config-If-Ethernet1/0/2)#ulpp flush enable mac
Switch(config-If-Ethernet1/0/2)#ulpp flush enable arp
```

65.4 Решение проблем с конфигурацией ULPP

- В конфигурации разрешено использование более чем двух uplink, однако есть риск возникновения петель, поэтому такую конфигурацию не рекомендуется использовать;
- При возникновении широковещательного шторма или разрывов соединения в кольце используйте информационные и отладочные команды для выявления причин сбоя.

66 ULSM

66.1 Общие сведения о ULSM

ULSM (Uplink State Monitor) используется для синхронизации статуса портов. Каждая ULSM группа состоит из uplink-портов и downlink-портов, которых может быть несколько. Uplink-порт прослушивается ULSM группой, если все uplink-порты в группе находятся в статусе Down, или в группе нет uplink портов, то ULSM группе присваивается статус Down. Группа имеет статус UP до тех пор, пока uplink-порт имеет такой же статус. Downlink порт является контролируемым портом в ULSM-группе, статус порта зависит от статуса группы и меняется одновременно со статусом ULSM-группы.

66.2 Конфигурация ULSM

1. Создать ULSM группу;
2. Настроить ULSM группу;
3. Просмотр информации и отладка.

1. Создать ULSM группу:

Команда	Описание

`ulsm group <group-id>`
`no ulsm group <group-id>`
 	
В режиме глобальной конфигурации
	Создать ULSM группу. Команда `no` удаляет эту группу.

2. Настроить ULSM группу:

Команда	Описание

`ulsm group <group-id> {uplink | downlink}`
`no ulsm group <group-id> {uplink | downlink}`
 	
В конфигурации интерфейса
	Выбрать порт в качестве uplink или downlink для ULSM группы

3. Просмотр информации и отладка:

Команда	Описание
`show ulsm group [group-id]`	Вывести информацию о конфигурации ULSM группы

В привилегированном режиме	

`debug ulsm event`
`no debug ulsm event`
 	
В привилегированном режиме
	Выводить отладочную информацию о событиях ULSM. Команда `no` отключает вывод отладочной информации.

66.3 Пример конфигурации ULSM

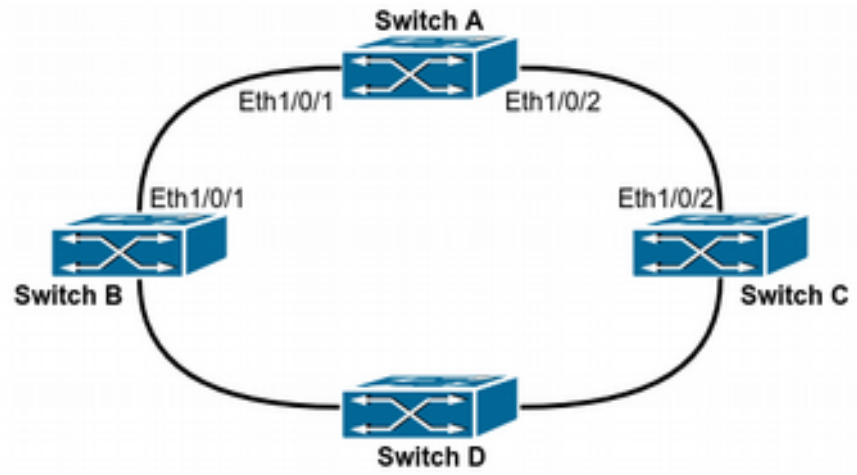


Рисунок 66.1

Как правило, ULSM используется вместе с протоколом ULPP. Как показано на рисунке 66.1, на коммутаторе Switch A настроен ULPP. Коммутаторы Switch B и Switch C используют протокол ULSM для мониторинга статуса Down у uplink. Если статус у uplink Down, то ULSM переводит downlink порты в down, чтобы ULPP-протокол на коммутаторе Switch A выполнил операцию по переключению uplink.

Конфигурация коммутатора Switch A:

```
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)#exit
```

Конфигурация коммутатора Switch B:

```
Switch(Config)#ulsm group 1
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#ulsm group 1 downlink
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)#ulsm group 1 uplink
Switch(config-If-Ethernet1/0/3)#exit
```

Конфигурация коммутатора Switch C:

```
Switch(Config)#ulsm group 1
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#ulsm group 1 downlink
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#interface ethernet 1/0/4
Switch(config-If-Ethernet1/0/4)#ulsm group 1 uplink
Switch(config-If-Ethernet1/0/4)#exit
```

67 NTP, SNTP и летнее время

67.1 Общие сведения о NTP, SNTP и летнем времени

NTP (Network Time Protocol) - протокол сетевого времени, используемый с целью синхронизации времени среди распределенных серверов и клиентов. Благодаря используемым алгоритмам способен достичь точности до 10мс. События, состояния, функции передачи и действия определены в RFC-1305. Время на коммутаторе может быть синхронизировано с внешним сервером, также коммутатор может выполнять роль эталона времени в качестве NTP сервера.
SNTP (Simple Network Time Protocol) - простой протокол сетевого времени. Используется в системах и устройствах, не требующих высокой точности. SNTP протокол является упрощением NTP протокола, поэтому SNTP клиент может обращаться к любому NTP серверу, как к серверу SNTP.
Летнее и зимнее время - смещение времени на 1 час вперед весной и на 1 час назад осенью для экономии энергии. В настоящее время большая часть стран мира испольуют переход на летнее время и обратно.

67.2 Конфигурация NTP, SNTP и летнего времени

1. Включить и настроить NTP клиент;
    a. включить NTP клиент;
    b. настроить NTP клиент;
    c. просмотр информации и отладка;
2. Включить и настроить SNTP клиент;
3. Включить и настроить переход на летнее время.

1. Включить и настроить NTP клиент:
    a. включить NTP клиент:

Команда	Описание

`ntp enable`
`ntp disable`
 	
В режиме глобальной конфигурации
	Включить функцию NTP.
	Выключить функцию NTP.

    b. настроить NTP клиент:

Команда	Описание
`ntp server {<ip-address> | <ipv6-address>} [version <version_no>] [key <key-id>]` `no ntp server {<ip-address> | <ipv6-address>}`	Задать IP адрес и ключ сервера, команда `no` удаляет эту конфигурацию.

В режиме глобальной конфигурации	

`ntp broadcast server count <number>`
`no ntp broadcast server count`
 	
В режиме глобальной конфигурации
	Задать максимальное количество broadcast и multicast NTP серверов, поддерживаемых клиентом. Команда `no` возвращает значение по-умолчанию - 50.

`clock timezone WORD {add | subtract} <0-23> [<0-59>]`
`no clock timezone WORD`
 	
В режиме глобальной конфигурации
	Задать смещение часового пояса относительно UTC. `subtract` - отрицательное смещение, `add` - положительное смещение. Команда `no` удаляет настроенное смешение.

`ntp access-group server <acl>`
`no ntp access-group server < acl>`
 	
В режиме глобальной конфигурации
	Установить фильтрацию по ACL, когда коммутатор работает в режиме NTP-сервера. Команда `no` отменяет эту конфигурацию.

`ntp authenticate`
`no ntp authenticate`
 	
В режиме глобальной конфигурации
	Включить функцию аутентификации NTP. Команда `no` отключает эту функцию.

`ntp authentication-key <key-id> md5 <value>`
`no ntp authentication-key <key-id>`
 	
В режиме глобальной конфигурации
	Задать ключ для аутентификации NTP. Команда `no` удаляет сконфигурированный ключ.

`ntp trusted-key <key-id>`
`no ntp trusted-key <key-id>`
 	
В режиме глобальной конфигурации
	Задать идентификатор безопасного ключа. Команда no удаляет сконфигурированный идентификатор..

`ntp multicast client`
`no ntp multicast client`
 	
В режиме конфигурации интерфейса VLAN
	Настроить интерфейс для приема multicast NTP пакетов. Команда `no` отменяет эту конфигурацию.

`ntp ipv6 multicast client`
`no ntp ipv6 multicast client`
 	
В режиме конфигурации интерфейса VLAN
	Настроить интерфейс для приема IPv6 multicast NTP пакетов. Команда `no` отменяет эту конфигурацию.

`ntp disable`	Отключить функцию NTP во VLAN.

`no ntp disable` В режиме конфигурации интерфейса VLAN	Команда `no` включает функцию NTP во VLAN (по-умолчанию).

c. просмотр информации и отладка:

Команда	Описание
`show ntp status` В привилегированном режиме	Отобразить информацию о статусе и конфигурации NTP.
`show ntp session [ <ip-address> | <ipv6-address> ]` В привилегированном режиме	Отобразить информацию о сессиях NTP.

`debug ntp authentication`
`no debug ntp authentication`
 	
В привилегированном режиме
	Выводить отладочную информацию о аутентификации NTP. Команда `no` отменяет вывод отладочной информации.

`debug ntp packets [send | receive]`
`no debug ntp packets [send | receive]`
 	
В привилегированном режиме
	Выводить отладочную информацию о локальных настройках времени. Команда `no` отменяет вывод отладочной информации.

`debug ntp adjust`
`no debug ntp adjust`
 	
В привилегированном режиме
	Выводить отладочную информацию о событиях NTP. Команда `no` отменяет вывод отладочной информации.

`debug ntp sync`
`no debug ntp sync`
 	
В привилегированном режиме
	Выводить отладочную информацию о синхронизации времени. Команда `no` отменяет вывод отладочной информации.

`debug ntp events`
`no debug ntp events`
 	
В привилегированном режиме
	Выводить отладочную информацию о событиях NTP. Команда `no` отменяет вывод отладочной информации.

2. Настроить SNTP клиент:
   a. Настроить SNTP клиент:

Команда	Описание

`sntp server {<ip-address> | <ipv6-address>} [source {vlan | loopback }] [version ]`
`no sntp server {<ip-address> | <ipv6-address>} [source {vlan | loopback }] [version]`
 	
В режиме глобальной конфигурации
	Включить функцию SNTP клиента и задать адрес сервера `{<ip-address> | <ipv6-address>}`, а также источника SNTP пакетов `[source {vlan | loopback }` и версию клиента. Команда `no` удаляет сконфигурированный SNTP сервер.

`sntp polltime <interval>`
`no sntp polltime`
 	
В режиме глобальной конфигурации
	Задать интервал синхронизации SNTP в секундах. Команда `no` возвращает значение по-умолчанию - 64 секунды.

`clock timezone WORD {add | subtract} <0-23> [<0-59>]`
`no clock timezone WORD`
 	
В режиме глобальной конфигурации
	Задать смещение часового пояса относительно UTC. `subtract` - отрицательное смещение, `add` - положительное смещение. Команда `no` удаляет настроенное смешение.

b. Просмотр информации и отладка:

Команда	Описание
`show sntp` В привилегированном режиме	Отобразить информацию о конфигурации и синхронизации SNTP.

`debug sntp`
`no debug sntp`
 	
В привилегированном режиме
	Выводить отладочную информацию о SNTP. Команда `no` прекращает вывод отладочной информации

3. Включить и настроить переход на летнее время:

Команда	Описание
`clock summer-time <word> absolute <HH:MM> <YYYY.MM.DD> <HH:MM> <YYYY.MM.DD> [<offset>]` `no clock summer-time`	Задать абсолютное время начала и окончания летнего времени, а также его смещение `<offset>` Команда `no` удаляет эту

В режиме глобальной конфигурации	конфигурацию.

`clock summer-time <word> recurring <HH:MM> {<week> <day> <month>| <MM.DD>} <HH:MM> {<week> <day> <month>|<MM.DD>} [<offset>]`
`no clock summer-time`
 	
В режиме глобальной конфигурации
	Задать повторяющееся время начала и окончания летнего времени, а также его смещение `<offset>`
	Команда `no` удаляет эту конфигурацию.

67.3 Пример конфигурации NTP, SNTP и летнего времени

67.3.1 NTP и SNTP

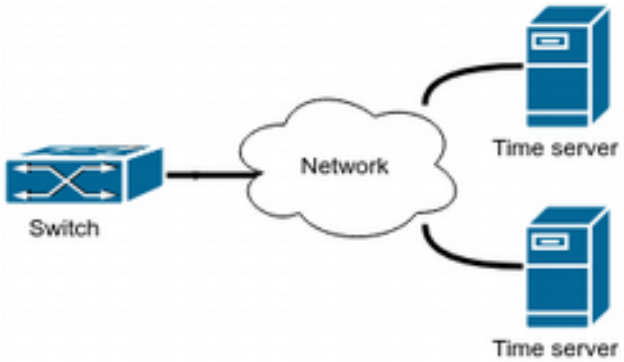


Рисунок 41.1 Синхронизация времени

В сети расположены 2 сервера времени: один находится в активном режиме и используется, другой находится в режиме ожидания. На коммутаторе “Switch A” требуется синхронизировать локальное время.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#ntp enable
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 192.168.1.12 255.255.255.0
Switch(config)#interface vlan 2
Switch(Config-if-Vlan1)#ip address 192.168.2.12 255.255.255.0
Switch(config)#ntp server 192.168.1.11
Switch(config)#ntp server 192.168.2.11
```

Вместо NTP на коммутаторе аналогично может быть настроен STP:

```
Switch(config)#sntp server 192.168.1.11
Switch(config)#sntp server 192.168.2.11
```

67.3.2 Летнее время

Пример 1.

Переход на летнее время однократно осуществляется 1го апреля 2019 года в 23:00, переход на зимнее время однократно осуществляется 1го октября 2019 года в 00:00. Смещение времени - 1 час.

Конфигурация коммутатор будет выглядеть следующим образом:

```
Switch(config)# clock summer-time 2019 absolute 23:00 2019.4.1 00:00
2019.10.1
```

Пример 2.

Переход на летнее время каждый год осуществляется в первую субботу апреля в 23:00, переход на зимнее время каждый год осуществляется в последнее воскресенье октября в 00:00. Смещение времени - 2 часа.

```
Switch(config)#clock summer-time time_travel recurring 23:00 first sat
apr 00:00 last sun oct 120
```

68 Зеркалирование трафика

68.1 Общие сведения о зеркалировании трафика

Функция зеркалирования трафика позволяет дублировать трафик, отправляемый или принимаемый портом или CPU коммутатора в другой порт. К порту назначения дублированного трафика может быть подключен анализатор трафика для диагностики проблем в сети.
На данном коммутаторе также существует возможность дублировать входящий в порт трафик на основе разрешающих правил ACL.

68.2 Конфигурация зеркала

1. Задать порт (CPU) источника трафика;
2. Задать порт назначения зеркала;
3. Задать скорость дискретизации;
4. Выбрать порт-источник трафика с использованием ACL.

1. Задать порт источника трафика:

Команда	Описание

`monitor session <session> source {interface <interface-list> | cpu} {rx| tx| both}`
`no monitor session <session> source {interface <interface-list> | cpu}`
 	
В режиме глобальной конфигурации
	Задать интерфейс или CPU в качестве источника трафика зеркала для сессии `<session>`. `{rx| tx| both}` указывают направление трафика. Команда `no` удаляет источник трафика для сессии `<session>`.

2. Задать порт (CPU) назначения зеркала:

Команда	Описание

`monitor session <session> destination interface <interface-number>`
`no monitor session <session> destination interface <interface-number>`
 	
В режиме глобальной конфигурации
	Задать интерфейс назначения трафика зеркала для сессии `<session>`. Команда `no` удаляет интерфейс назначения для сессии `<session>`.

3. Задать число захватываемых пакетов:

Команда	Описание

`monitor session <session> sample rate <num>`
`no monitor session <session> sample rate`
 	
В режиме глобальной конфигурации
	Задать скорость дискретизации <0-65535> для зеркала `<session>`. Команда `no` отменяет дискретизацию - каждый пакет из источника попадет в зеркало.

4. Выбрать порт-источник трафика с использованием ACL:

Команда	Описание

`monitor session <session> source {interface <interface-list>} access-group <num> {rx}`
`no monitor session <session> source {interface <interface-list>} access-group <num>`
 	
В режиме глобальной конфигурации
	Задать интерфейс в качестве источника трафика зеркала для сессии `<session>`. `access-group <num> rx` применяет ACL на входящее направление трафика в интерфейсе источника зеркала. Команда `no` удаляет источник трафика для сессии `<session>`.

68.3 Пример конфигурации зеркала

В порт 1/0/1 необходимо отправлять следующий трафик:

1. трафик поступающий на порт 1/0/7 (ingress);
2. трафик уходящий с порта 1/0/9 (egress);
3. трафик в CPU всех направлений;
4. трафик TCP с адресом источника 1.2.3.4/24, адресом назначение 5.6.7.8/24 входящий (ingress) в порт 1/0/5.

Конфигурация коммутатора будет выглядеть следующим образом:

```
Switch(config)#monitor session 1 destination interface ethernet 1/0/1
Switch(config)#monitor session 1 source interface ethernet 1/0/7 rx
Switch(config)#monitor session 1 source interface ethernet 1/0/9 tx
Switch(config)#monitor session 1 source cpu
Switch(config)#access-list 120 permit tcp 1.2.3.4 0.0.0.255 5.6.7.8
0.0.0.255
Switch(config)#monitor session 1 source interface ethernet 1/0/15
access-list 120 rx
```

68.4 Решение проблем при зеркалировании трафика

- На данный момент отсутствует возможность использовать Port-channel или его

член в качестве назначения зеркала;
- Убедитесь, что пропускная способность интерфейса назначения удовлетворяет суммарному количеству трафика всех источников, учитывая возможные кратковременные всплески трафика;
- На данном коммутаторе возможно применение ACL только на трафик направления ingress по отношению к порту коммутатора;
- Для одной сессии возможен выбор только одного интерфейса назначения трафика. Если требуется использовать большее количество интерфейсов назначения, см. главу 42 RSPAN.

69 RSPAN

69.1 Общие сведения об RSPAN

RSPAN (Remote Switched Port ANalyzer) - предоставляет возможность использовать в качестве источника и назначения трафика зеркала интерфейсы, находящиеся на разных коммутаторах, а также отправлять трафик зеркала в несколько интерфейсов на одном коммутаторе. Функционал использует такие понятия как **reflector port** и **remote-span VLAN.**

Remote-span VLAN, это та VLAN, в которую будет отправляться зеркалируемый трафик в порту назначения зеркала. Эта VLAN может быть назначена в режиме trunk одновременно с другими пользовательскими VLAN. Изучение MAC-адресов в remote-span VLAN отключено. Remote-span VLAN также может быть использован для передачи трафика из зеркала через несколько промежуточных коммутаторов - для этого потребуется пробросить remote-span VLAN по пути к порту мониторинга.

Reflector port используется в качестве порта назначения зеркала и имитирует прием трафика из зеркала. Если существует потребность использовать несколько портов назначения зеркала, этого можно достичь, назначив Remote-span VLAN на Reflector port и на все те порты, в которые требуется передать трафик - он будет продублирован во все эти порты.

69.2 Конфигурация RSPAN

1. Назначить VLAN в качестве remote VLAN;
2. Выбрать порт (CPU) в качестве источника зеркала;
3. Выбрать порт в качестве назначения зеркала;
4. Выбрать reflector порт;
5. Задать remote VLAN для мониторинговой сессии.

1. Назначить VLAN в качестве remote VLAN:

Команда	Описание

`remote-span`
`no remote-span`
 	
В режиме конфигурации VLAN
	Назначить VLAN в качестве remote-span VLAN. Команда `no` удаляет эту конфигурацию.

2. Выбрать порт (CPU) в качестве источника зеркала:

Команда	Описание
`monitor session <session> source {interface <interface-list> | cpu }`	Задать интерфейс или CPU в качестве источника трафика зеркала

{rx| tx| both} no monitor session <session> source {interface <interface-list> | cpu} В режиме глобальной конфигурации	для сессии <session>. {rx| tx| both} указывают направление трафика. Команда no удаляет источник трафика для сессии <session>.

3. Выбрать порт в качестве назначения зеркала:

Команда	Описание
monitor session <session> destination interface <interface-number> no monitor session <session> destination interface <interface-number> В режиме глобальной конфигурации	Задать интерфейс назначения трафика зеркала для сессии <session>. Команда no удаляет интерфейс назначения для сессии <session>.

4. Выбрать reflector порт:

Команда	Описание
monitor session <session> reflector-port <interface-number> no monitor session <session> reflector-port В режиме глобальной конфигурации	Выбрать интерфейс в качестве reflector порта. Команда no отменяет выбор.

5. Задать remote VLAN для мониторинговой сессии:

Команда	Описание
monitor session <session> remote vlan <vlan_id> no monitor session <session> remote vlan В режиме глобальной конфигурации	Задать для мониторинговой сессии <session> remote VLAN <vlan_id>. Команда no отменяет выбор.

69.3 Пример конфигурации RSPAN

Пример 1

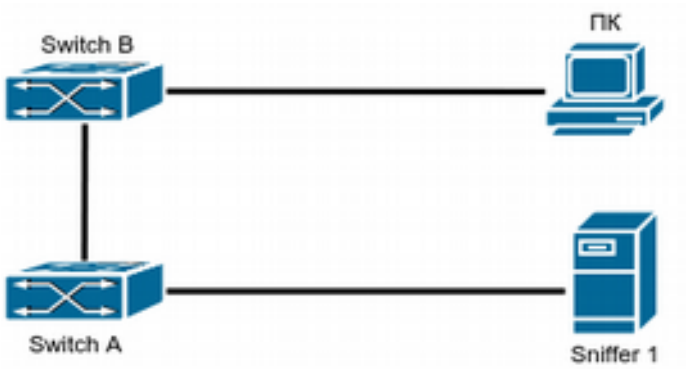


Рисунок 69.1 RSPAN VLAN

Как показано на рисунке 69.1, сервер мониторинга “Sniffer 1” подключен к коммутатору “Switch B”, а ПК пользователя - к коммутатору “Switch A”. Для диагностики проблем подключения требуется зеркалировать трафик с порта ПК пользователя на сервер мониторинга.

Конфигурация коммутатора Switch A:

```
SwitchA(config)#vlan 5
SwitchA(Config-Vlan5)#remote-span
SwitchA(Config-Vlan5)#exit
SwitchA(config)#interface ethernet 1/0/9
SwitchA(Config-If-Ethernet1/0/9)#switchport mode trunk
SwitchA(Config-If-Ethernet1/0/9)#switchport trunk allowed vlan add 5
SwitchA(Config-If-Ethernet1/0/9)#exit
SwitchA(config)#monitor session 1 source interface ethernet1/0/1
SwitchA(config)#monitor session 1 destination interface ethernet1/0/9
SwitchA(config)#monitor session 1 remote vlan 5
```

Конфигурация коммутатор Switch B:

```
SwitchA(config)#vlan 5
SwitchA(Config-Vlan5)#remote-span
SwitchA(Config-Vlan5)#exit
SwitchA(config)#interface ethernet 1/0/9
SwitchA(Config-If-Ethernet1/0/9)#switchport mode trunk
SwitchA(Config-If-Ethernet1/0/9)#switchport trunk allowed vlan add 5
SwitchA(Config-If-Ethernet1/0/9)#interface ethernet 1/0/1
SwitchA(Config-If-Ethernet1/0/9)#switchport access vlan 5
```

Пример 2

Серверы мониторинга “Sniffer 1” и “Sniffer 2” а также ПК пользователя подключены к коммутатору “Switch A” к портам к портам 1/0/8, 1/0/9 и 1/0/1 соответственно. Порт 1/0/7 на коммутаторе не занят. Для мониторинга требуется зеркалировать трафик с порта ПК пользователя одновременно на оба сервера.

Конфигурация коммутатора Switch A:

```
SwitchA(config)#vlan 5
SwitchA(Config-Vlan5)#remote-span
SwitchA(Config-Vlan5)#exit
SwitchA(config)#interface ethernet 1/0/8-9
SwitchA(Config-If-range)#switchport mode trunk
SwitchA(Config-If-range)#switchport trunk allowed vlan add 5
SwitchA(Config-If-range)#exit
SwitchA(config)#monitor session 1 source interface ethernet1/0/1
SwitchA(config)#monitor session 1 reflector-port interface ethernet
1/0/7
SwitchA(config)#monitor session 1 remote vlan 5
```

69.4 Решение проблем с конфигурацией RSPAN

- В качестве remote VLAN не может быть выбрать multicast VLAN, default VLAN, dynamic VLAN, private VLAN и VLAN с L3 интерфейсом;
- VLAN, передающая трафик зеркала, должна быть настроена как remote VLAN (отключено изучение MAC) на всех коммутаторах по пути передачи трафика зеркала;
- Порт, используемый в качестве reflector порт должен быть свободен.

70 sFlow

70.1 Общие сведения об sFlow

SFlow (RFC 3176) - это протокол, используемый для сбора, отправки и анализа информации о сетевом трафике в целях мониторинга.
Система мониторинга sFlow включает в себя: агент sFlow, центральный сборщик данных (sFlow collector) и анализатор sFlow (sFlow analyzer). Прокси sFlow собирает данные с коммутатора с использованием технологий выборки. Сборщик sFlow предназначен для форматирования статистики отобранных данных, которая должна быть отправлена на анализатор sFlow, который будет анализировать данные выборки и выполнять действие в соответствии с результатом. Данный коммутатор может работать как прокси и центральный сборщик данных в системе sFlow.
Данный коммутатор поддерживает sFlow версии 4 в соответствии с RFC 3176.

70.2 Конфигурация sFlow

1. Задать IP адрес сборщика sFlow (collector);
2. Задать IP адрес прокси sFlow;
3. Задать приоритет sFlow прокси;
4. Настроить длину заголовка пакета, копируемого в sFlow:
5. Настроить максимальную длину группы выборок sFlow:
6. Настроить частоту дискретизации;
7. Настроить интервал сборе статистики;
8. Настроить тип используемого анализатора.

1. Задать IP адрес сборщика sFlow (collector):

Команда	Описание

`sflow destination <collector-address> [<collector-port>]`
`no sflow destination`
 	
В режиме глобальной конфигурации
	Указать адрес и порт назначения для отправки данных sFlow. Порт по-умолчанию 6343. Команда `no` удаляет эту конфигурацию.

2. Задать IP адрес агента sFlow:

Команда	Описание

`sflow agent-address <collector-address>`
`no sflow agent-address`
 	
В режиме глобальной конфигурации
	Задать идентификатор агента sFlow на коммутаторе. Команда `no` удаляет эту конфигурацию.

3. Задать приоритет sFlow прокси:

Команда	Описание

`sflow priority <priority-value>`
`no sflow priority`
 	
В режиме глобальной конфигурации
	Задать внутренний приоритет, с которым коммутатор будет передавать данные sFlow в CPU из интерфейсов. Команда `no` восстанавливает значение по-умолчанию - 0.

4. Настроить длину заголовка пакета, копируемого в sFlow:

Команда	Описание

`sflow header-len <length-vlaue>`
`no sflow header-len`
 	
В режиме глобальной конфигурации
	Настроить длину копируемого в sFlow заголовка пакета при невозможности определить тип протокола в CPU. Команда `no` возвращает значение по-умолчанию - 128 байт.

5. Настроить максимальную длину группы выборок sFlow:

Команда	Описание

`sflow data-len <length-vlaue>`
`no sflow data-len`
 	
В режиме глобальной конфигурации
	Задать максимальное значение длины группы выборок sFlow, не включая заголовки 2 и 3 уровней. Команда no восстанавливает значение по-умолчанию - 1400 байт.

6. Настроить частоту дискретизации:

Команда	Описание

`sflow rate {input <input-rate> |`
`output <output-rate >}`
`no sflow rate [input | output]`
 	
В режиме глобальной конфигурации
	Настроить частоту дискретизации sFLow для входящего или исходящего потока. Команда `no` удаляет эту конфигурацию.

7. Настроить интервал сбора статистики:

Команда	Описание

`sflow counter-interval <interval-value>`
`no sflow counter-interval`
 	
В режиме глобальной конфигурации
	Настроить интервал сбора статистики sFlow. Команда `no` удаляет эту конфигурацию.

8. Задать тип используемого анализатора:

Команда	Описание

`sflow analyzer sflowtrend`
`no sflow analyzer sflowtrend`
 	
В режиме глобальной конфигурации
	Задать тип используемого анализатора sFlow. Команда `no` удаляет эту конфигурацию.

70.3 Пример конфигурации sFlow

Сбор данных sFlow включен на портах 1/0/1 и 1/0/2 коммутатора. Анализатор sFlow запущен на хосте с адресом 192.168.1.200. Адрес интерфейса уровня 3 на коммутаторе, для VLAN, подключенного к анализатору - 192.168.1.100. Также на коммутаторе настроен интерфейс уровня 3 с адресом 10.1.144.2.

Конфигурация коммутатора выглядит следующим образом:

```
Switch#config
Switch(config)#sflow agent-address 10.1.144.2
Switch(config)#sflow destination 192.168.1.200
Switch(config)#sflow priority 1
Switch(config)#interface ethernet1/0/1
Switch(Config-If-Ethernet1/0/1)#sflow rate input 10000
Switch(Config-If-Ethernet1/0/1)#sflow rate output 10000
Switch(Config-If-Ethernet1/0/1)#sflow counter-interval 20
Switch(Config-If-Ethernet1/0/1)#exit
Switch(config)#interface ethernet1/0/2
Switch(Config-If-Ethernet1/0/2)#sflow rate input 20000
Switch(Config-If-Ethernet1/0/2)#sflow rate output 20000
Switch(Config-If-Ethernet1/0/2)#sflow counter-interval 40
```

70.4 Решение проблем при конфигурации sFlow

- Убедитесь, что связность с sFlow анализатором существует;
- Удостоверьтесь, что в необходимом для мониторинга порту присутствует трафик;

- Если требуется выборка на основе трафика, необходимо настроить частоту дискретизации интерфейса;
- Если требуется статистическая выборка, необходимо настроить интервал сбора статистики интерфейса.

71 Мониторинг и отладка

71.1 Show

Команды show могут быть применены для вывода информации о конфигурации, операциях и протоколах. В данной главе приведены команды show для общих функций коммутатора. Команды остальных функций приведены в соответствующих главах.

Следующие команды могут быть применены в привилегированном режиме, либо любом режиме конфигурации.

Команда	Описание
`show debugging`	Вывести информацию о протоколах и событиях, для которых включена отладка
`show flash`	Вывести информацию о содержимом flash-памяти
`show history [all-users [detail]]`	Вывести информацию о истории действий текущего пользователя. `all-users` выводит информацию о истории действий всех пользователей. `detail` выводит детальную информацию.
`show memory usage`	Вывести информацию об используемой памяти
`show running-config [current-mode]`	Отобразить текущую конфигурацию коммутатора. `current-mode` выводит информацию о конфигурации текущего режима конфигурации.
`show startup-config`	Отобразить текущую загрузочную конфигурацию
`show switchport interface [ethernet <IFNAME>]`	Отобразить информацию о VLAN принадлежащих к интерфейсу `<IFNAME>`
`show tcp` `show tcp ipv6`	Отобразить информацию о текущих TCP сессиях
`show udp` `show udp ipv6`	Отобразить информацию о текущих UDP сессиях

`show user`	Отобразить информацию о пользователях, подключенных в данный момент
`show tech-support`	Отобразить информацию для отправки в обращение support.nag.ru
`show version`	Отобразить информацию о коммутаторе

71.2 System log

71.2.1 Общие сведения о system log

System log, или системный журнал, представляет собой записи в текстовом формате о действиях и событиях в работе коммутатора. Все записи на данном коммутаторе подразделяются на четыре уровня срочности, в зависимости от которого может быть настроен вывод в определенный канал.
Коммутатор может выводить записи в следующие каналы:

- Консольный порт коммутатора - в этот порт происходит вывод записей всех уровней, это не настраивается;
- В терминал telnet или ssh;
- В область журнала в памяти SDRAM или FLASH-памяти;
- На удаленный хост.

Уровни срочности коммутатора соответствуют стандарту syslog UNIX систем.
Информация журнала делится на восемь уровней по степени срочности. Один уровень на одно значение и чем выше уровень записи журнала, тем меньше будет его значение. Правило, применяемое при фильтрации записей журнала по уровню срочности, заключается в следующем: выводятся только записи журнала с уровнем, равным или превышающим заданное значение. Поэтому, фильтр уровня debugging включает все записи журнала.
Уровни срочности коммутатора соответствуют стандарту syslog UNIX систем.

Поддерживаемые коммутатором уровни срочности и их краткое описание приведены в таблице ниже:

2	critical	События перезагрузки коммутатора, записи о ненормальном состоянии компонентов коммутатора
4	warnings	События изменения состояний интерфейсов, изменения топологии и т.д.
7	informational	Записи действий пользователя
8	debugging	Информация отладки

71.2.2 Конфигурация system log

1. Вывод и очистка записей в буфере;
2. Настроить сервер для отправки system log;
3. Включить логирование действий пользователя;
4. Вывод информации о конфигурации;

1. Вывод и очистка записей в буфере:

Команда	Описание
`show logging {buffered|flash} [ level {critical | warnings} | range <begin-index> <end-index>]` В привилегированном режиме	Отобразить журнал system log, сохраненный в буфере. `level {critical | warnings` - задает уровень отображаемых записей. `range <begin-index> <end-index>` - позволяет выбрать номера отображаемых записей
`clear logging sdram` В привилегированном режиме	Очистить журнал сохраненный в sdram

2. Настроить сервер для отправки system log:

Команда	Описание

`logging {<ipv4-addr> | <ipv6-addr>} [ facility <local-number> ] [level <severity>]`
`no logging {<ipv4-addr> | <ipv6-addr>} [ facility <local-number>]`
 	
В режиме глобальной конфигурации
	Задать адрес сервера для отправки логов, а также их уровень и добавляемый `facility`. Команда `no` отменяет эту конфигурацию.

`logging loghost sequence-number`
`no logging loghost sequence-number`
 	
В режиме глобальной конфигурации
	Добавлять номер записи при отправке записей на сервер. Команда `no` отключает эту функцию (по-умолчанию).

`logging source-ip { <A.B.C.D> | <X:X::X:X> }` В режиме глобальной конфигурации	Задать адрес источника при отправке логов

3. Включить логирование действий пользователя:

Команда	Описание
`logging executed-commands {enable| disable}` В режиме глобальной конфигурации	Включить/выключить логирование действий пользователя. По-умолчанию выключено.

4. Настройка и вывод system log на flash:

Команда	Описание

`logging flash level <severity>`
`no logging flash`
 	
В режиме глобальной конфигурации
	Включить запись system log на flash. Команда `no` отключает эту функцию (по-умолчанию).

`show logging flash` В привилегированном режиме	Вывести записи system log, сохраненные на flash.

5. Вывод информации о конфигурации:

Команда	Описание
`show logging source mstp` В привилегированном режиме	Отобразить информацию о статусе и уровне источника для канала логирования.
`show logging executed-commands state` В привилегированном режиме	Отобразить статус логирования действий пользователя.

71.3 Перезагрузка коммутатора через заданное время

Перезагрузка коммутатора через заданное время может применяться для предотвращения потери управления коммутатором при ошибках конфигурации или для перезагрузки коммутатора в час наименьшей нагрузки для обновления ПО.

Команда	Описание

`reload after {[<HH:MM:SS>] [days <days>]}` В привилегированном режиме	Задать время перезагрузки коммутатора.
`reload cancel` В привилегированном режиме	Отменить перезагрузку коммутатора в заданное время.

71.4 Отладка и диагностика трафика отправленного и принятого CPU

Следующие команды позволяют использовать диагностику и отладку пакетов в CPU:

Команда	Описание

`cpu-rx-ratelimit protocol <protocol-type> <packets>`
`no cpu-rx-ratelimit protocol [ <protocol-type> ]`
 	
В режиме глобальной конфигурации
	Задать лимит пропускной способности (пакетов в секунду) для типа протокола `<protocol-type>` принятого CPU. Команда `no` возвращает значение по-умолчанию.

`clear cpu-rx-stat protocol [ <protocol-type> ]` В привилегированном режиме	Очистить статистику пакетов, принятых в CPU
`show cpu-rx protocol [ <protocol-type> ]` В привилегированном режиме	Отобразить информацию о счетчиках и лимите для пакетов, принимаемых в CPU

`debug driver {receive|send} [interface {<interface-name> |all}] [protocol {<protocol-type> |discard |all}][detail]`
 	
`no debug driver {receive |send}`
 	
В привилегированном режиме
	Отображать отладочную информацию о принятых `receive` в CPU или отправленных `send` из CPU пакетах через интерфейс `{<interface-name> |all}`. Команда `no` отключает вывод отладочной информации.