QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Ethernet коммутаторы доступа

QSW-3750-10T-AC
QSW-3750-18T-AC
QSW-3750-28T-AC
QSW-3750-28T-DC
QSW-3750-52T-AC
QSW-3750-10T-POE-AC
QSW-3750-28T-POE-AC

www.qtech.ru

Оглавление

1. УПРАВЛЕНИЕ КОММУТАТОРОМ

1.1. Варианты Управления

Для управления необходимо настроить коммутатор. Коммутатор обеспечивает два варианта управления: внеполосное (out-of-band) или внутриполосное (in-band).

1.1.1. Внеполосное управление

Внеполосное управление — это управление через консольный интерфейс. Внеполосное управление, в основном используется для начального конфигурирования коммутатора, либо когда внутриполосное управление недоступно. Например, пользователь может через консольный порт присвоить коммутатору IP-адрес для доступа по Telnet.

Процедура управления коммутатором через консольный интерфейс, описана ниже:

Шаг 1: Подключить персональный компьютер к консольному (серийному) порту коммутатора

Подключение ПК к консольному порту коммутатора

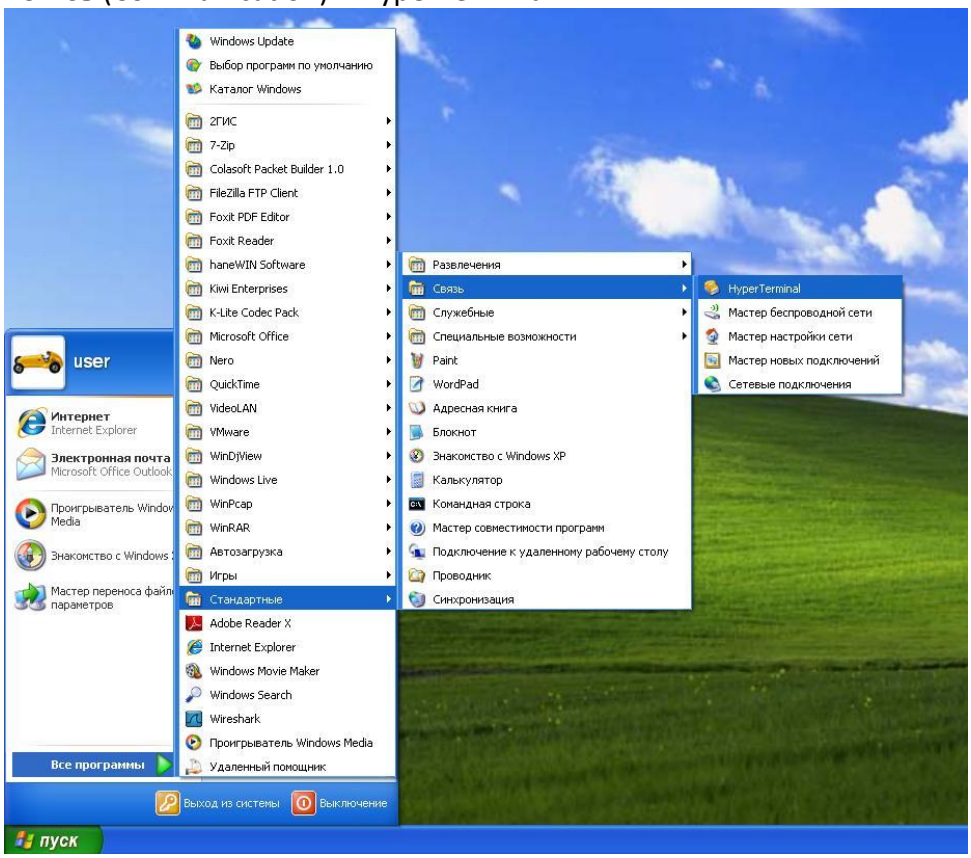
Как показано выше, серийный порт (RS-232) подключен к коммутатору через серийный кабель. В таблице ниже указаны все устройства использующийся в подключении.

Название устройства	Описание
Персональный компьютер (PC)	Имеет функциональную клавиатуру и порт RS-232, с установленным эмулятором терминала, таким как HyperTerminal, входящий в комплект Windows 9x/NT/2000/XP.
Кабель серийного порта	Один конец подключается к серийному порту RS-232, а другой к порту консоли.
Коммутатор	Требуется работающий консольный порт.

Шаг 2: Включение и настройка HyperTerminal.

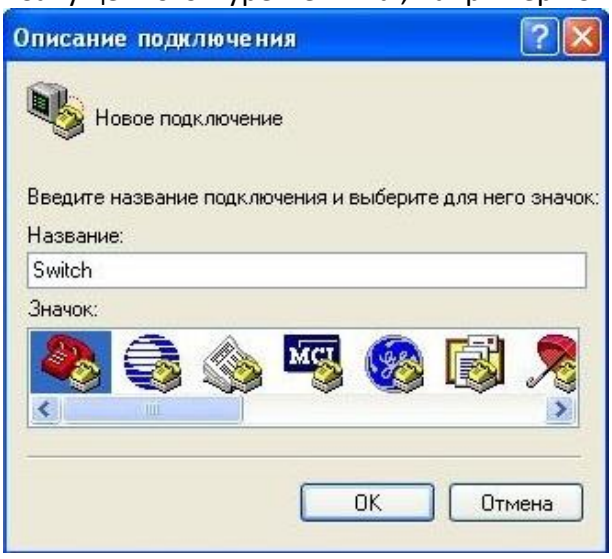
После установки соединения, запустите HyperTerminal, входящий в комплект Windows. Пример приведенный далее основан на HyperTerminal входящий в комплект Windows XP.

1. Нажмите «Пуск»(Start menu) – Все программы (All Programs) – Стандартные (Accessories) – Связь (Communication) – HyperTerminal



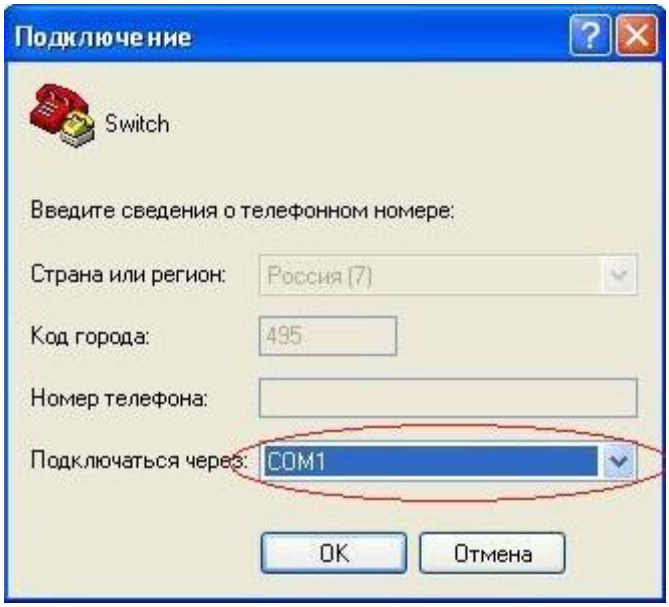
Запуск HyperTerminal.

2. Наберите имя для запущенного HyperTerminal, например «Switch».



Запуск HyperTerminal.

3. В выпадающем меню «Подключение» выберите, серийный порт RS-232 который используется PC, например, COM1 и нажмите «OK»



Запуск HyperTerminal

4. Настройте свойства COM1 следующим образом: Выберите скорость «9600» для «Baud rate»; «8» для «Data bits»; «none» для «Parity checksum»; «1» для «stop bit»; «none» для «traffic control»; или вы можете нажать «Restore default», а после нажать «OK».

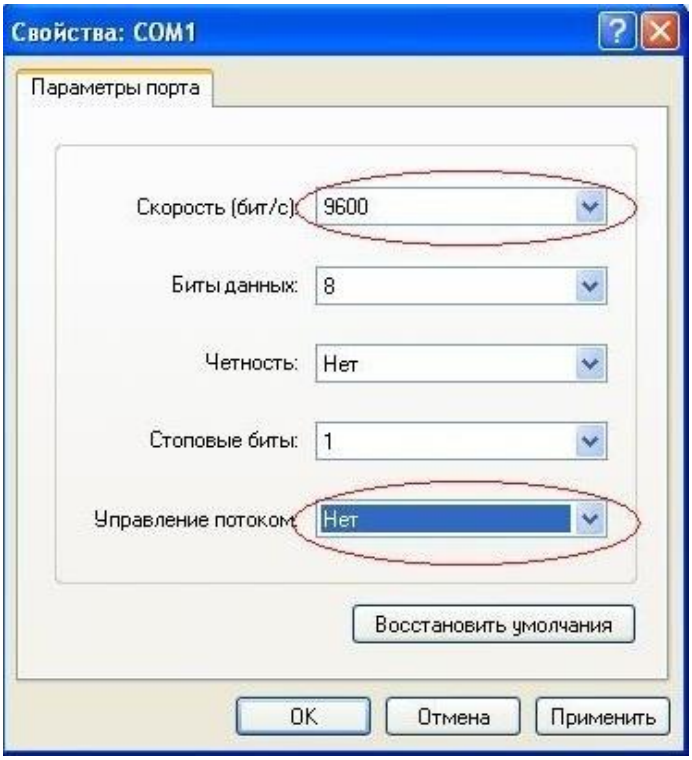


Рисунок 1-5. Запуск HyperTerminal.

Шаг 3: Вызов командного интерфейса (CLI) коммутатора.

Включите коммутатор, после чего следующие сообщения появятся в окне HyperTerminal – это режим конфигурации для коммутатора.

```
Testing RAM...
0x08000000 RAM OK.

Loading flash:/nos.img ...
### JFFSWITCHB loading 'nos.img' to 0x81000000
### JFFSWITCHB load complete: 10235495 bytes loaded to 0x81000000
## Booting kernel from Legacy Image at 81000100 ...
   Image Name:
   Image Type:   MIPS Linux Kernel Image (gzip compressed)
   Data Size:    10157391 Bytes = 9.7 MiB
   Load Address: 80000000
   Entry Point:  80003710
   Verifying Checksum ... OK
   Uncompressing Kernel Image ... OK

Starting kernel ...

Current time: Sun Jan 01 00:00:00 2006 [UTC]

Switch>
```

Теперь можно вводить команды управления коммутатором. Детальное описание команд приведено в последующих главах.

1.1.2 In-band управление.

In-band управление относится к удалённому управлению посредством доступа к коммутатору с использованием таких протоколов как Telnet, SSH, HTTP, а также SNMP. В тех случаях, когда In-band управление из-за изменений, сделанных в конфигурации коммутатора, работает со сбоями, для управления и конфигурирования коммутатора можно использовать Out-band управление (Console/Management port).

1.1.1.1. Управление по Telnet

Чтобы управлять коммутатором по Telnet, должны выполняться следующие условия:

1. Коммутатор должен иметь сконфигурированный IPv4/IPv6 адрес;

2. IP адрес хоста (Telnet клиент) и VLAN интерфейс коммутатора, должны иметь IPv4/IPv6 адреса в одном сегменте сети;

3. Если второй пункт не может быть выполнен, Telnet клиент должен быть подключен к IPv4/IPv6 адресу коммутатора с других устройств, таких как маршрутизатор.

- Коммутатор третьего уровня может быть настроен с несколькими IPv4/IPv6 адресами, метод настройки описан в посвященной этому главе. Следующий пример предполагает состояние коммутатора после поставки с заводскими настройками, где присутствует только VLAN1.
- Последующие шаги описывают подключение Telnet клиента к интерфейсу VLAN1 коммутатора посредством Telnet (пример адреса IPv4):

Управление коммутатором по Telnet

Шаг 1: Настройка IP адресов для коммутатора и запуск функции Telnet Server на коммутаторе.

❖ Первым делом идет настройка IP адреса хоста. Он должен быть в том же сегменте сети, что и IP адрес VLAN1 интерфейса коммутатора. Предположим, что IP адрес интерфейса VLAN1 коммутатора 10.1.128.251/0/24. Тогда IP адрес хоста может быть 10.1.128.252/24. С помощью команды «ping 10.1.128.251» можно проверить, доступен коммутатор или нет.

❖ Команды настройки IP адреса для интерфейса VLAN1 указаны ниже. Перед началом In-band управления, IP-адрес коммутатора должен быть настроен посредством Out-band управления (например, через порт Console). Команды конфигурирования следующие (Далее считается, что все приглашения режима конфигурирования коммутатора начинаются со слова «switch», если отдельно не указано иного):

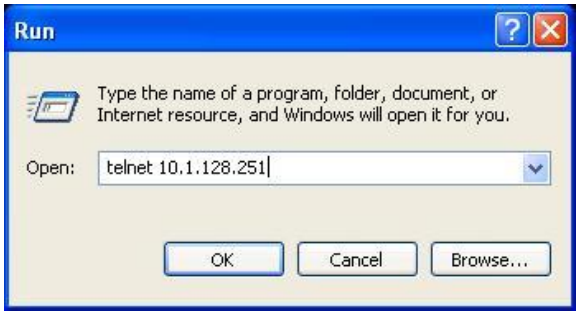
```
Switch>enable
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.128.251 255.255.255.0
Switch(Config-if-Vlan1)#no shutdown
```

Для активации функции Telnet сервера пользователь должен включить её в режиме глобального конфигурирования, как показано ниже:

```
Switch>enable
Switch#config
Switch(config)# telnet-server enable
```

Шаг 2: Запуск программы Telnet Client

Необходимо запустить программу Telnet клиент в Windows с указанием адреса хоста.



Запуск программы Telnet клиент в Windows.

Шаг 3: Получить доступ к коммутатору.

Для того что бы получить доступ к конфигурации через интерфейс Telnet необходимо ввести достоверный логин (login) и пароль (password). В противном случае в доступе будет отказано. Этот метод помогает избежать неавторизованного получения доступа. Как результат, когда Telnet включен для настройки и управления коммутатора, имя пользователя (username) и пароль (password) для авторизованных пользователей должны быть настроены следующей командой: «`username <username> privilege <privilege> [password (0|7) <password>]`».

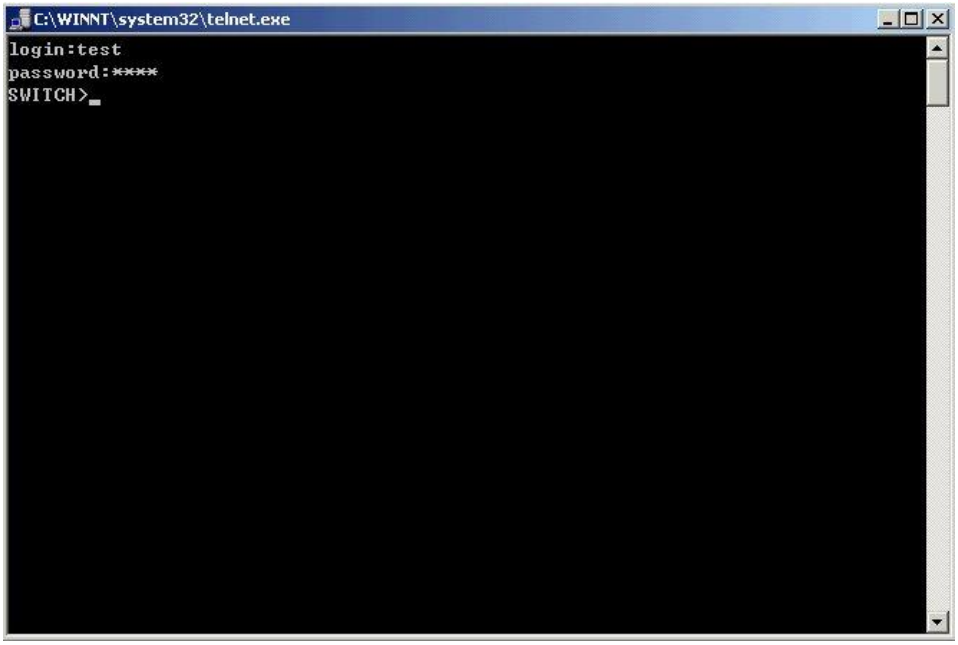
Для локальной аутентификации можно использовать следующую команду: `authentifcation line vty login local.`

Для доступа в привелигерованный режим необходимо и задан уровень привилегий 15.

Допустим, авторизованный пользователь имеет имя «test» и пароль «test», тогда процедура задания имени и пароля для доступа по Telnet:

```
Switch>enable
Switch#config
Switch(config)#username test privilege 15 password 0 test
Switch(config)#authentication line vty login local
```

После ввода имени и пароля для интерфейса конфигурирования Telnet, пользователь сможет вызвать командный интерфейс CLI настройки коммутатора. Команды, используемые в командном интерфейсе Telnet CLI, которые становятся доступны после ввода имени и пароля — те же самые, что и в консольном интерфейсе



Настройка Telnet интерфейса

1.1.1.2. Управление через HTTP

Чтобы управлять коммутатором через Web-интерфейс должны быть выполнены следующие условия:

1. Коммутатор должен иметь сконфигурированный IPv4/IPv6 адрес.

2. IP адрес хоста (HTTP клиент) и VLAN интерфейс коммутатора, должны иметь IPv4/IPv6 адреса в одном сегменте сети.

3. Если второй пункт не может быть выполнен, HTTP клиент должен быть подключен к IPv4/IPv6 адресу коммутатора с других устройств, таких, как маршрутизатор.

Как и в управлении, коммутатором через Telnet, как только удается ping/ping6 хоста к IPv4/IPv6 адресам коммутатора и вводится правильный логин и пароль, возможно получить доступ к коммутатору через HTTP. Ниже описан способ настройки:

Шаг 1: Настройка IP адресов для коммутатора и запуск функции HTTP сервера.

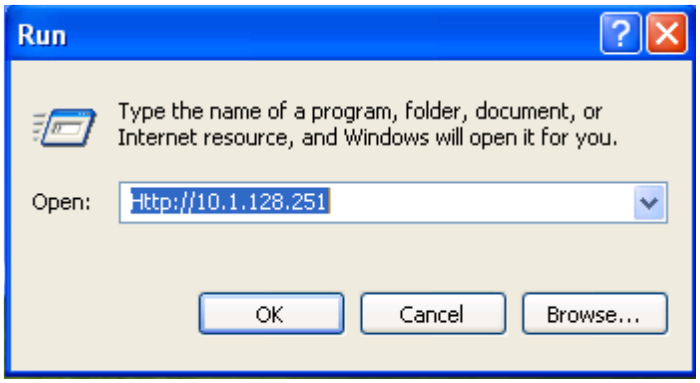
О настройке IP-адреса коммутатора с помощью внеполосного управления, смотри главу о настройке Telnet управления.

Чтобы конфигурирование по Web стало возможным, нужно ввести команду ip http server в глобальном режиме конфигурирования:

```
Switch>enable
Switch#config
Switch(config)#ip http server
```

Шаг 2: Запуск Web-браузера на хосте.

Необходимо открыть Web-браузер на хосте и ввести IP адрес коммутатора, или непосредственно запустить HTTP протокол в Windows. К примеру, IP адрес коммутатора «10.1.128.251»;



Запуск HTTP протокола

При обращении коммутатора с IPv6 адреса рекомендуется использовать браузер Firefox версии 1.5 или позднее. Например, если адрес коммутатора 3ffe:506:1:2::3. Введите адрес IPv6 коммутатора http:// [3ffe: 506:1:2:: 3], адрес обязательно должен быть заключен в квадратные скобки.

Шаг 3: Получение доступа к коммутатору.

Для того чтобы получить доступ конфигурации с использованием WEB интерфейса, необходимо ввести достоверный логин (login) и пароль (password), в противном случае будет отказано в доступе. Этот метод помогает избежать неавторизованного доступа. Как результат, когда Telnet включен для настройки и управления коммутатора, имя пользователя (username) и пароль (password) для авторизованных пользователей должны быть настроены следующей командой:

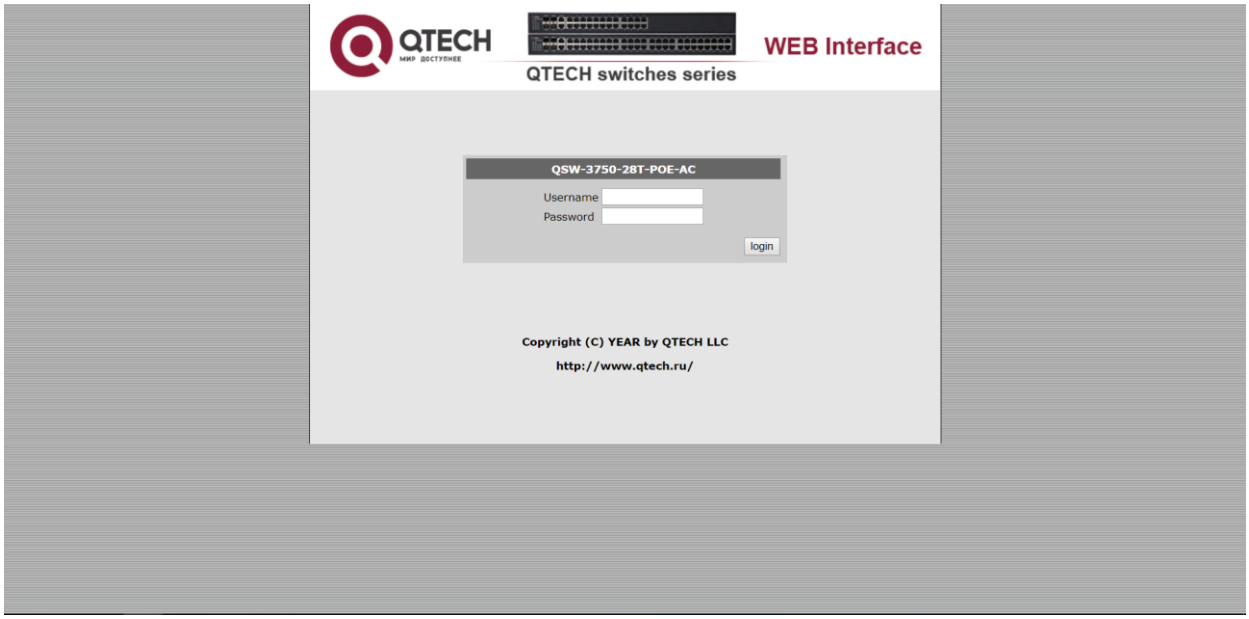
```
username <username> privilege <privilege> [password (0|7) <password>].
```

Для локальной аутентификации можно использовать следующую команду: authentication line vty login local.

Для доступа в привелигерованный режим необходимо и задан уровень привилегий 15. Допустим, авторизованный пользователь имеет имя «admin» и пароль «admin», тогда процедура настройки, следующая:

```
Switch>enable
Switch#config
Switch(config)#username admin privilege 15 password 0 admin
Switch(config)#authentication line web login local
```

Web интерфейс страницы ввода учётных данных выглядит следующим образом:



После ввода корректных учётных данных, вы попадаете в главное меню Web интерфейса, как это показано ниже:

1.1.1.3. Управление коммутатором через сетевое управление SNMP

Необходимые требования:

1. Коммутатор должен иметь сконфигурированный IPv4/IPv6 адрес.
2. IP адрес хоста (HTTP клиент) и VLAN интерфейс коммутатора, должны иметь IPv4/IPv6 адреса в одном сегменте сети.
3. Если второй пункт не может быть выполнен, HTTP клиент должен быть подключен к IPv4/IPv6 адресу коммутатора с других устройств, таких как роутер.

Хост с программным обеспечением SNMP для управления сетью должен уметь pingовать IP адрес коммутатора так, чтобы при работе программного обеспечения SNMP, оно было доступно для осуществления операций чтения/записи на нем. Подробности о том, как управлять коммутаторами через SNMP, не будут рассмотрены в этом руководстве, их можно найти в «Snmp network management software user manual»(Инструкция по сетевому управлению SNMP).

1.2. CLI интерфейс

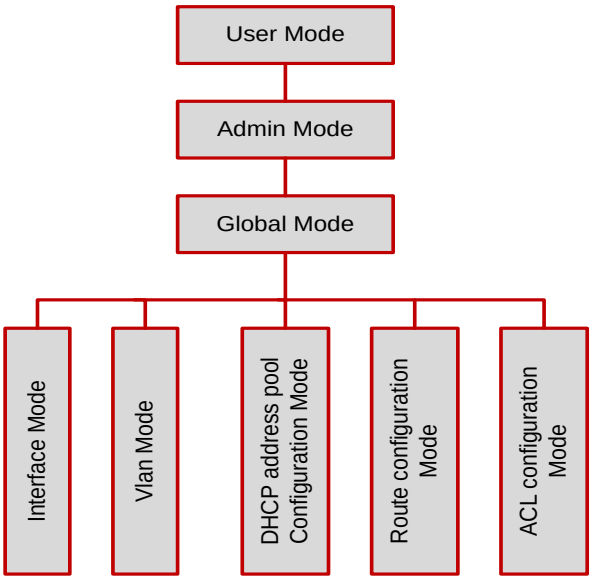
Коммутатор обеспечивает три интерфейса управления для пользователя: CLI (Command Line Interface) интерфейс, веб-интерфейс, сетевое управление программным обеспечением SNMP. Мы познакомим вас с CLI(Консолью), веб-интерфейсом и их конфигурациями в деталях, SNMP пока не будет рассматриваться. CLI интерфейс знаком большинству пользователей. Как упомянуто выше, при управлении по независимым каналам связи и Telnet управление коммутатором осуществляется через интерфейс командной строки (CLI).

CLI интерфейс поддерживает оболочку Shell, которая состоит из набора команд конфигурации. Эти команды относятся к разным категориям в соответствии с их функциями в конфигурации коммутатора. Каждая категория представляет свой, отличный от всех, режим конфигурации.

Возможности Shell для коммутаторов описаны ниже:

- Режим настройки;
- Настройка синтаксиса;
- Поддержка сочетания клавиш;
- Справка;
- Проверка ввода;
- Поддержка язык нечеткой логики (Fuzzy math).

1.2.1 Режим настройки



Режимы настройки Shell

1.2.1.1. Режим пользователя

При входе в командную строку в первую очередь пользователь оказывается в режиме пользователя. Если он входит в качестве обычного пользователя, который стоит по умолчанию, тогда в строке отображается «Switch>», где символ «>» является запросом для режима пользователя. Когда команда выхода запускается под режимом администратора, она будет также возвращена в режим пользователя.

В режиме пользователя, без дополнительных настроек, пользователю доступны только запросы, например время или информация о версии коммутатора.

1.2.1.2. Режим администратора

Для того чтобы попасть в режим Администратора (привилегированный) существует несколько способов: вход с использованием в качестве имени пользователя «Admin»; ввод команды «enable» из непривилегированного (пользовательского) интерфейса, при этом необходимо будет ввести пароль администратора (если установлен). При работе в режиме администратора приглашение командной строки коммутатора будет выглядеть как «Switch#». Коммутатор также поддерживает комбинацию клавиш «Ctrl + Z», что позволяет простым способом выйти в режим администратора из любого режима конфигурации (за исключением пользовательского).

При работе с привилегиями администратора пользователь может давать команды на вывод конфигурационной информации, состоянии соединения и статистической информации обо всех портах. Также пользователь может перейти в режим глобального конфигурирования и изменить любую часть конфигурации коммутатора. Поэтому, определение пароля для доступа к привилегированному режиму является обязательным для предотвращения неавторизованного доступа и злонамеренного изменения конфигурации коммутатора.

1.2.1.3. Режим глобального конфигурирования.

Наберите команду «Switch#config» в режиме администратора для того, чтобы войти в режим глобального конфигурирования. Используйте команду выхода в соответствии с другими режимами конфигурации, такими, как режим порта, VLAN режим, вернутся в режим глобального конфигурирования. Пользователь может выполнять глобальные настройки конфигурации в этом режиме, такие как настройка таблиц MAC-адресов, зеркалирование портов, создание VLAN, запуск IGMP Snooping и STP, и т. д. Также пользователь может войти в режим конфигурирования порта для настройки всех интерфейсов.

Режим конфигурирования интерфейса

Использование команды интерфейса в режиме глобального конфигурирования позволяет входить в режим конфигурирования указанного интерфейса. Коммутатор поддерживает три типа интерфейсов: 1. VLAN; 2. Ethernet порт; 3. Порт-канал, соответствующий трем режимам конфигурации интерфейса.

Тип Интерфейса	Команда	Действие команды	Выход
VLAN	Наберите команду **interface vlan <*Vlan-id*>** в режиме глобального конфигурирования.	Настройка IP адресов коммутатора и т.д.	Используйте команду **exit** для возвращения в глобальный режим.
Ethernet порт	Наберите команду **interface ethernet <interface-list>** в режиме глобального конфигурирования.	Настройка поддерживаемого дуплексного режима, скорости Ethernet порта и т.п.	Используйте команду **exit** для возвращения в глобальный режим.
Порт-канал	Наберите команду **interface port-channel <port-channel-number>** в режиме глобального конфигурирования.	Конфигурирование порт-канала: дуплексный режим, скорость и т.д.	Используйте команду **exit** для возвращения в глобальный режим.

Режим VLAN

Использование команды <vlan-id> в режиме глобального конфигурирования, помогает войти в соответствующий режим конфигурирования VLAN. В этом режиме администратор может настраивать все порты пользователей соответствующего VLAN. Выполните команду выхода, чтобы выйти из режима VLAN в режим глобального конфигурирования.

Режим DHCP Address Pool

Введите команду ip dhcp pool <name> в режиме глобального конфигурирования для входа в режим DHCP Address Pool. Приглашение этого режима «Switch(Config-<name>-

dhcp)#». В этом режиме происходит конфигурирование DHCP Address Pool. Выполните команду выхода, чтобы выйти из режима конфигурирования DHCP Address Pool в режим глобального конфигурирования.

ACL режим

Тип ACL	Команда	Действие команды	Выход
Стандартный режим IP ACL	Наберите команду **ip access-list standard** в режиме глобального конфигурирования.	Настройка параметров длястандартного режима IP ACL	Используйте команду **exit** для возвращения в глобальный режим.
Расширенный режим IP ACL	Наберите команду **ip access-list extended** в режиме глобального конфигурирования.	Настройка параметров для расширенного режима IP ACL	Используйте команду **exit** для возвращения в глобальный режим.

1.2.2 Настройка синтаксиса

Коммутатор различает множество команд конфигурации. Несмотря на то, что все команды разные, необходимо соблюдать синтаксис их написания. Общий формат команды коммутатора приведен ниже:

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

Расшифровка: **cmdtxt** жирным шрифтом указывает на ключевое слово команды; **<variable>** указывает на изменяемый параметр; **{enum1 | … | enumN}** означает обязательный параметр, который должен быть выбран из набора параметров enum1~enumN, а в квадратные скобки «[]»**[option1 | … | optionN]** заключают необязательный параметр. В этом случае в командной строке может быть комбинация "<>", "{}" и "[]" например: [<variable>], {enum1 <variable>| enum2}, [option1 [option2]], и так далее.

Вот примеры некоторых актуальных команд конфигурации:

`show version`, параметры не требуется. Это команда, состоящая только из ключевых слов и без параметров;

`vlan <vlan-id>`, необходим ввод значения параметров после ключевого слова.

`firewall {enable | disable}`, этой командой пользователь может включить или выключить брандмауэр, следует лишь выбрать нужный параметр.

`snmp-server community {ro | rw} <string>`, ниже приведены возможные варианты:

```
snmp-server community ro public
snmp-server community rw private
```

1.2.3 Сочетания клавиш

Коммутатор поддерживает множество сочетаний клавиш для облегчения ввода конфигурации пользователем. Если командная строка не признает нажатия вверх и вниз, то Ctrl + P и Ctrl + N могут быть использованы вместо них.

Клавиша (и)	Функция	
Back Space	Удалить символ перед курсором. Курсор перемещается назад.	
Вверх «↑»	Показать предыдущую введенную команду. Отображение до десяти недавно набранных команд.	
Вниз «↓»	Показать следующую введенную команду. При использовании клавиши вверх «↑», вы получаете ранее введенные команды, при использовании клавиши вниз «↓», вы возвращаетесь к следующей команде.	
Влево «←»	Курсор перемещается на один символ влево.	Вы можете использовать клавиши влево «←» и вправо «→» для изменения введенных команд.
Вправо «→»	Курсор перемещается на один символ вправо.	
Ctrl +p	Такая же, как и у клавиши вверх «↑».	
Ctrl +n	Такая же, как и у клавиши вниз «↓».	
Ctrl +b	Такая же, как и у клавиши влево «←».	
Ctrl +f	Такая же, как и у клавиши вправо «→».	
Ctrl +z	Вернуться в Режим администратора непосредственно из других режимов настройки (за исключением пользовательского режима)	
Ctrl +c	Остановка непрерывных процессов команд, таких как ping и т.д.	
Tab	В процессе ввода команды Tab может быть использован для ее завершения, если нет ошибок.	

1.2.4 Справка

Существуют два способа получить доступ к справочной информации: Командами «help» и «?».

Доступ к справке	Использование и функции
Help	Под любой командной строкой введите "help" и нажмите Enter, вы получите краткое описание из справочной системы.
«?»	1. Под любой командной строкой введите "?", чтобы получить список команд для текущего режима с кратким описанием. 2. Введите "?" после команды. Если позиция должна быть параметром, описание этого параметра типа, масштаба и т.д., будут отображены, если позиция должна быть ключевым словом, то будет отображен набор ключевых слов с кратким описанием, если вышло "<cr>", то команда

	введена полностью, нажмите клавишу Enter, чтобы выполнить команду. 3. Введите "?" сразу после строки. Это покажет все команды, которые начинаются с этой строки.

1.2.5 Проверка ввода

1.2.5.1 Отображаемая информация: успешное выполнение (successfull)

Все команды, вводимые через клавиатуру, проходят проверку синтаксиса в Shell. Ничего не будет отображаться, если пользователь ввел правильные команды при соответствующих режимах и что привело к их успешному выполнению.

1.2.5.2 Отображаемая информация: ошибочный ввод (error)

Отображаемое сообщение ошибки	Пояснение
Unrecognized command or illegal parameter!	Введенной команды не существует или есть ошибка в параметре масштаба, типа или формата.
Ambiguous command	Доступно по крайней мере две интерпретации смысла на основе введенного текста.
Invalid command or parameter	Команда существует (признается), но задан неправильный параметр.
This command is not existing in current mode	Команда существует (признается), но не может быть использована в данном режиме.
Please configure precursor command "*»at first!	Команда существует (признается), но отсутствует условие команды.
syntax error: missing '"' before the end of command line!	Ошибка синтаксиса: кавычки не могут использоваться в паре.

1.2.6 Поддержка языка нечеткой логики (Fuzzy math)

Shell на коммутаторе имеет поддержку языка нечеткой логики в поиске команд и ключевых слов. Shell будет распознавать команды и ключевые слова в том случае, если введенная строка не вызывает никаких конфликтов.

Например:

1. Команда `«show interface ethernet status»`, будет работать даже в том случае, если набрать `«sh in ethernet status»`.

2. Однако, при наборе команды `«show running-config»` как `«show r»` система сообщит «%Ambiguous command», т.к. Shell будет не в состоянии определить, что имелось ввиду «show radius» или «show running-config». Таким образом, Shell сможет правильно распознать команду только если будет набрано «sh ru».

2. ОСНОВНЫЕ НАСТРОЙКИ КОММУТАТОРА

2.1 Основные настройки

Основные настройки коммутатора включают в себя команды для входа и выхода из режима администратора, команды для входа и выхода из режима конфигурирования интерфейса, для настройки и отображения времени в коммутаторе, отображения информации о версии системы коммутатора и так далее.

Команда	Пояснение
Обычный пользовательский режим/ Режим администратора	
Enable [<1-15>] **disable**	Пользователь использует команду **enable** для того, чтобы войти в режим администратора. А команду **disable** для выхода из него.
Режим администратора	
config [terminal]	Входит в режим глобального конфигурирования из режима администратора.
Различные режимы	
exit	Выход из текущего режима и вход в предыдущий режим, например если применить эту команду в режиме глобального конфигурирования, то она вернет вас в режим администратора, если набрать еще раз (уже находясь в режиме администратора), то попадете в пользовательский режим.
show privilege	Показывает привилегии для определенных пользователей
Расширенный пользовательский режим/ Режим администратора	
end	Выход из текущего режима и возвращение в режим администратора, только когда пользователь находится не в пользовательском/администраторском режимах.
Режим администратора	
clock set *<HH:MM:SS>* **[YYYY.MM.DD]**	Установка даты и времени.
show version	Отображение версии коммутатора.
set default	Возвращает заводские настройки.
write	Сохраняет текущую конфигурацию на Flash-память.
reload	Перезагрузка коммутатора.

show cpu usage	Показывает степень использования CPU.
show cpu utilization	Показывает текущую скорость загрузки процессора.
show memory usage	Показывает степень использования памяти.
Режим глобального конфигурирования	
banner motd <LINE> **no banner motd**	Настройка отображаемой информации при успешной авторизаци пользователя через Telnet или консольное соединение.

2.2 Управление Telnet

2.2.1 Telnet

2.2.1.1 Введение в Telnet

Telnet это простой протокол удаленного доступа для дистанционного входа. Используя Telnet, пользователь может дистанционно войти на хост используя его IP адрес или имя. Telnet может посылать нажатия клавиш удаленному хосту и выводить данные на экран пользователя используя протокол TCP. Это прозрачная процедура, так как кажется то, что пользовательские клавиатура и монитор подключены к удаленному узлу напрямую.

Telnet использует клиент-серверный режим, локальная система выступает в роли Telnet клиента, а удаленный хост - Telnet сервера. Коммутатор может быть как Telnet сервером, так и Telnet клиентом.

Когда коммутатор используется как Telnet сервер, пользователь может использовать Telnet клиентские программы, включенные в ОС Windows или другие операционные системы для входа в коммутатор, как описано ранее в разделе «управление по независимым каналам связи». Как Telnet сервер коммутатор позволяет до 5 клиентам Telnet подключение используя протокол TCP.

Также коммутатор работая как Telnet клиент, позволяет пользователю войти в другие удаленные хосты. Коммутатор может установить TCP-подключение только к одному удаленному хосту. Если появится необходимость соединения с другим удаленным хостом, текущие соединения TCP должны быть разорваны.

2.2.1.2 Команды конфигурирования Telnet

1. Настройка Telnet сервера;
2. Использование Telnet для удаленного доступа к коммутатору.

1. Настройка Telnet сервера

Команда	Описание
Режим глобального конфигурирования	
telnet-server enable **no telnet-server enable**	Активирует функцию Telnet сервера на коммутаторе, команда «**no**»деактивирует эту функцию.

username *<user-name>* [privilege *<privilege>*] [password [0 | 7] *<password>*] **no username *<username>***	Настраивает имя пользователя и пароль для доступа по Telnet. Команда «no» удаляет данные авторизации выбранного пользователя.
authentication securityip *<ip-addr>* **no authentication securityip *<ip-addr>***	Настраивает безопасность IP адресов для входа на коммутатор по Telnet: команда «**no**» отменяет предыдущую команду.
authentication securityipv6 *<ipv6-addr>* **no authentication securityipv6 *<ipv6-addr>***	Настраивает безопасность IPv6 адресов для входа на коммутатор по Telnet: команда «**no**» отменяет предыдущую команду.
authentication ip access-class {<num-std>|<name>} **no authentication ip access-class**	Связывает стандартный IP ACL с Telnet / SSH /Web; команда «**no**» отменяет предыдущую команду.
authentication ipv6 access-class {<num-std>|<name>} **no authentication ipv6 access-class**	Связывает IPv6 ACL с Telnet / SSH /Web; команда «**no**» отменяет предыдущую команду.
authentication line {console | vty | web} login {local | radius | tacacs} **no authentication line {console | vty | web} login**	Настройка режима аутентификации Telnet.
authentication enable method1 [method2 …] **no authentication enable**	Настройка включения списков методов аутентификации.
authorization line {console | vty | web} exec {local | radius | tacacs} **no authorization line {console | vty | web} exec**	Настройка режима авторизации Telnet.
accounting line {console | vty} command *<1-15>* {start-stop | stop-only | none} method1 [method2…] **no accounting line {console | vty} command *<1-15>***	Настройка списка методов учета.
Режим администратора	
terminal monitor **terminal no monitor**	Отображение отладочной информации для входа на коммутатор через Telnet клиент; Команда «**no**» отключает отображение данной информации.

2. Использование Telnet для удаленного доступа к коммутатору

Команда	Описание
Режим администратора	
telnet [vrf *<vrf-name>*] {*<ip-addr>* | *<ipv6-addr>* / host *<hostname>*} [*<port>*]	Вход на хост коммутатора через Telnet клиент, входящий в комплектацию коммутатора.

2.2.2. SSH

2.2.2.1 Введение в SSH

SSH (англ. ***S**ecure **SH**ell* — «безопасная оболочка») является протоколом, который обеспечивает безопасный удаленный доступ к сетевым устройствам. Он основан на надежном TCP/IP протоколе. Он поддерживает такие механизмы как распределение ключей, проверка подлинности и шифрования между SSH сервером и SSH-клиентом, установка безопасного соединения. Информация, передаваемая через это соединение защищена от перехвата и расшифровки. Для доступа к коммутатору, соответствующему требованиям SSH2.0, необходимо SSH2.0 клиентское программное обеспечение, такое, как SSH Secure Client и Putty. Пользователи могут запускать вышеперечисленное программное обеспечение для управления коммутатором удаленно. Коммутатор в настоящее время поддерживает аутентификацию RSA, 3DES и SSH шифрование протокола, пароль пользователя аутентификации и т.д.

2.2.2.2 Список команд для конфигурирования SSH сервера

Команда	Описание
Режим глобального конфигурирования	
ssh-server enable **no ssh-server enable**	Активация функции на коммутаторе; команда «**no**» отменяет предыдущую команду.
username *<username>* [privilege *<privilege>*] [password [0 | 7] *<password>*] **no username *<username>***	Настраивает имя пользователя и пароль для доступа к коммутатору через SSH клиент. Команда «**no**» удаляет данные авторизации выбранного пользователя.
ssh-server timeout *<timeout>* **no ssh-server timeout**	Настройка таймаута для аутентификации SSH; Команда «**no**» восстанавливает значения по умолчанию таймаута для аутентификации SSH.
ssh-server authentication-retires *<authentication-retires>* **no ssh-server authentication-retries**	Настройка число повторных попыток SSH аутентификации; Команда «no» восстанавливает значения по умолчанию.

ssh-server host-key create rsa modulus *<moduls>*	Создание нового RSA ключа хоста на SSH сервере.
Режим администратора	
terminal monitor **terminal no monitor**	Показ отладочной информации SSH на стороне клиента; команда «no» отменяет предыдущую команду.

2.2.2.3 Пример настройки SSH сервера

Пример 1:

Задачи:

- Включить SSH сервер на коммутаторе и запустить SSH2.0 программное обеспечение клиента, такое как SSH Secure Client или Putty на терминале. Войти на коммутатор, используя имя пользователя и пароль от клиента.
- Настроить IP-адрес, добавить SSH пользователей и активировать SSH сервис на коммутаторе. SSH2.0 клиент может войти в коммутатор, используя имя пользователя и пароль для настройки коммутатора.

```
Switch(config)#ssh-server enable
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 100.100.100.200 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#username test privilege 15 password 0 test
```

В IPv6 сетях, терминал должен запустить SSH-клиент и программное обеспечение, которое поддерживает IPv6, такие как putty6. Пользователи не должны изменять настройки коммутатора, за исключением распределения IPv6-адреса для локального хоста.

2.3 Настройка IP адресов коммутатора

Все Ethernet-порты коммутатора по умолчанию являются портами доступа для канального уровня и выполняются на втором уровне. VLAN интерфейс представляет собой интерфейс третьего уровня с функциями, для которых может быть назначен IP-адрес, который будет также IP-адресом коммутатора. Все сети VLAN, связанные с интерфейсом, и их конфигурация могут быть настроены в подрежиме конфигурирования VLAN. Коммутатор предоставляет три метода конфигурации IP адреса:

- Ручная
- BOOTP
- DHCP

Ручная настройка IP-адреса позволяет присваивать IP-адрес вручную.

В BOOTP / DHCP режиме, коммутатор работает как BOOTP/DHCP клиент, отправляет широковещательные пакеты BOOTP запроса на BOOTP/DHCP-сервера и BOOTP/DHCP сервер назначает адрес отправителю запроса, кроме того, коммутатор может работать в качестве сервера DHCP и динамически назначать параметры сети, такие, как IP-адреса, шлюз и адреса DNS-серверов DHCP клиентам, что подробно описано в последующих главах.

2.3.1 Список команд для настройки IP адресов

1. Включение VLAN режима;
2. Ручная настройка;
3. BOOTP конфигурация;
4. DHCP конфигурация.

1. Включение VLAN режима

Команда	Описание
Режим глобального конфигурирования	
interface vlan *<vlan-id>* **no interface vlan *<vlan-id>***	Создание VLAN интерфейса (интерфейса третьего уровня); команда «no» удаляет VLAN интерфейс.

2. Ручная настройка

Команда	Описание
VLAN режим	
ip address *<ip_address>* *<mask>* [secondary] **no ip address *<ip_address>* *<mask>* [secondary]**	Настройка IP адреса VLAN интерфейса; команда «no» удаляет IP адреса VLANинтерфейса.
ipv6 address *<ipv6-address / prefix-length>* [eui-64] **no ipv6 address *<ipv6-address / prefix-length>***	Настройка IPv6 адресов. Команда «no» удаляет IPv6 адреса.

3. BOOTP конфигурация

Команда	Описание
VLAN режим	
ip bootp-client enable **no ip bootp-client enable**	Включение коммутатора как BOOTP клиента для получения IP-адреса и адреса шлюза путем переговоров BOOTP. Команда «no» выключает BOOTP клиент.

4. DHCP конфигурация

Команда	Описание
VLAN режим	

ip dhcp-client enable **no ip dhcp-client enable**	Включение коммутатора как DHCP клиента для получения IP-адреса и адреса шлюза путем запросов DHCP. Команда «no» выключает DHCP клиент.

2.4 Настройка SNMP

2.4.1 Введение в SNMP

SNMP (Simple Network Management Protocol) является стандартным протоколом сетевого управления, который широко используется в управлении компьютерными сетями. SNMP является развивающимся протоколом. SNMP v1 [RFC1157] является первой версией протокола SNMP, которая адаптирована к огромному числу производителей своей простотой и легкостью внедрения; SNMP v2c является улучшенной версией SNMP v1; в SNMP v3 усилена безопасность, добавлены USM и VACM (View-Based Access Control Model).

SNMP-протокол обеспечивает простой способ обмена информацией управления сетью между двумя точками в сети. SNMP использует механизм запросов и передает сообщения через UDP (протокол без установления соединения транспортного уровня), поэтому он хорошо поддерживается существующим компьютерными сетями.

SNMP-протокол использует режим станции-агента. В этой структуре есть две составляющие: NMS (Network Management Station) и агент. NMS является рабочей станцией, на которой стоит клиентская программа SNMP. Это ядро SNMP-управления сетью. Агент серверного программного обеспечения работает на устройствах, которые нуждаются в управлении. NMS управляет всеми объектами через агентов. Коммутатор поддерживает функции агента.

Связь между NMS и агентом происходит в режиме Клиент-Сервер, обмениваясь стандартными сообщениями. NMS посылает запрос, и агент отвечает. Есть семь типов SNMP сообщений:

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

NMS связывается с агентом с помощью запросов: Get-Request, Get-Next-Request, Get-Bulk-Request and Set-Request, агент, при получении запросов, отвечает сообщением Get-Response. О некоторых специальных ситуациях, таких, как изменения статусов сетевых портов устройства или изменения топологии сети, агенты могут отправлять специальные сообщения об аномальных событиях. Кроме того, NMS может быть также установлен для предупреждения некоторых аномальных событий, активируя RMON функцию. Когда срабатывает определенное правило, агенты отправляют сообщения в журналы событий в соответствии с настройками.

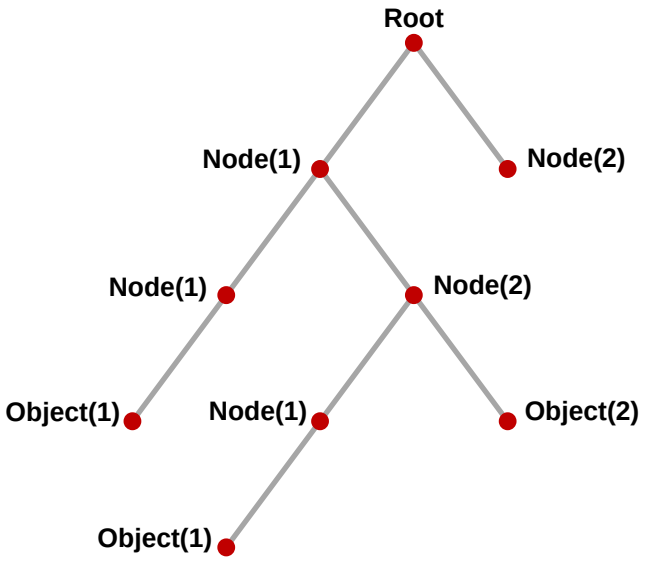
USM обеспечивает безопасную передачу, хорошо продуманное шифрование и аутентификацию. USM шифрует сообщения в зависимости от ввода пароля пользователя.

Этот механизм гарантирует, что сообщения не могут быть просмотрены во время передачи. Также USM Аутентификация гарантирует, что сообщение не может быть изменено при передаче. USM использует DES-CBC криптографию. И HMAC-MD5, и HMAC-SHA используются для аутентификации.

VACM используется для классификации прав и доступа пользователей. Это ставит пользователей с одним и тем же разрешением доступа в одну группу. Неавторизованные пользователи не могут проводить операции.

2.4.2 Введение в MIB

Информация управления сетью доступа в NMS корректно определена и организована в информационной базе управления (MIB). MIB это предопределенная информация, которая может быть доступна через протоколы управления сетью, во всей своей многослойности и структурированном виде. Предопределенная информация управления может быть получена путем мониторинга сетевых устройств. ISO ASN.1 определяет древовидную структуру для MIB, соответственно каждый MIB организует всю доступную информацию в виде такой структуры. Каждый узел этого дерева содержит OID (идентификатор объекта) и краткое описание узла. OID представляет собой набор целых чисел, разделенных точками, и может быть использован для определения местоположения узла в древовидной структуре MIB, как показано на рисунке ниже:



Пример дерева ASN.1

На этом рисунке OID объекта A является 1.2.1.1. NMS может найти этот объект через этот уникальный OID и получить стандартные переменные объекта. MIB определяет набор стандартных переменных для мониторинга сетевых устройств, следуя этой структуре.

Если информация о переменных MIB агента должна быть просмотрена, необходим запуск программного обеспечения просмотра MIB на NMS. MIB в агенте обычно состоит из публичного MIB и частного MIB. Публичный MIB содержит открытую информацию управления сетью, которая может быть доступна для всех NMS, частный MIB содержит

конкретную информацию, которая может быть просмотрена и контролируется поддержкой производителя.

MIB-I [RFC1156] была первой реализацией публичных MIB SNMP, и была заменена MIB-II [RFC1213]. MIB-II расширяет MIB-I и сохраняет OID для MIB деревьев в MIB-I. MIB-II, содержит вложенные деревья, которые также называются группами. Объекты в этих группах охватывают все функциональные области в управлении сетью. NMS получает информацию об управлении сетью просматривая MIB на SNMP агенте.

Коммутатор может работать в качестве SNMP агента, а также поддерживает SNMP v1/0/v2c и SNMP v3. Также коммутатор поддерживает базовые MIB-II, RMON публичные MIB и другие публичные MIB, такие как Bridge MIB. Кроме того, коммутатор поддерживает самостоятельно определенные частные MIB.

2.4.3 Введение в RMON

RMON является наиболее важным расширением стандартного SNMP протокола. RMON является набором определений MIB и используется для определения стандартных средств и интерфейсов для наблюдения за сетью, позволяет осуществлять связь между терминалами управления SNMP и удаленными управляемыми коммутаторами. RMON обеспечивает высокоэффективный метод контроля действий внутри подсети.

MIB RMON состоит из 10 групп. Коммутатор поддерживает наиболее часто используемые группы 1, 2, 3 и 9:

- **Statistics**: контролирует основное использование и ведет статистику ошибок для каждой подсети контролируемого агента.
- **History**: позволяет периодически записывать образцы статистики, которые доступны в Статистике.
- **Alarm**: позволяет пользователям консоли управления устанавливать количество или число для интервалов обновления и пороговых значений оповещения для записей RMON агента.
- **Event**: список всех событий, произошедших в RMON агенте.

Alarm зависят от реализации Event. Statistics и History отображают текущую статистику или историю подсети. Alarm и Event обеспечивают метод контроля любого изменения данных в сети и предоставляют возможность подавать сигналы при нештатных событиях (отправка Trap или запись в журналы).

2.4.4 Настройка SNMP

2.4.4.1 Список команд для настройки SNMP

1. Включение и отключение функции SNMP агента;
2. Настройка строки сообщества в SNMP;
3. Настройка IP-адреса станции управления SNMP;
4. Настройка engine ID;
5. Настройка пользователя;
6. Настройка группы;
7. Настройка вида;
8. Настройка TRAP;
9. Включение / выключение RMON.

1. Включение и отключение функции SNMP агента

Команда	Описание
Режим глобального конфигурирования	
snmp-server enable **no snmp-server enable**	Включение функции SNMP агента на коммутаторе. Команда «no» выключает эту функцию.

2. Настройка строки сообщества в SNMP

Команда	Описание
Режим глобального конфигурирования	
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>*] **no snmp-server community *<string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**	Настройка строки сообщества в SNMP для коммутатора. Команда «no» удаляет эту строку.

3. Настройка IP-адреса станции управления SNMP

Команда	Описание
Режим глобального конфигурирования	
snmp-server securityip {*<ipv4-address>* | *<ipv6-address>*} **no snmp-server securityip {*<ipv4-address>* | *<ipv6-address>*}**	Настройка безопасных IPv4/IPv6 адресов, которые имеют право доступа к коммутатору. Команда «no» удаляет эти настройки
snmp-server securityip enable **snmp-server securityip disable**	Включение и отключение функции проверки безопасных IP.

4. Настройка engine ID

Команда	Описание
Режим глобального конфигурирования	
snmp-server engineid *<engine-string>* **no snmp-server engineid**	Настройка локального engine ID на коммутаторе. Эта команда используется для SNMP v3.

5. Настройка пользователя

Команда	Описание
Режим глобального конфигурирования	
snmp-server user *<use-string>* *<group-string>* [{authPriv | authNoPriv} auth {md5 | sha} *<word>*] [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>*}]**	Добавление пользователя в SNMP группу. Эта команда используется для настройки USM для SNMP v3.

6. Настройка группы

Команда	Описание
Режим глобального конфигурирования	
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>*}]**	Установка информации о группе на коммутаторе. Эта команда используется для настройки VACM для SNMP v3.

7. Настройка вида

Команда	Описание
Режим глобального конфигурирования	
snmp-server view *<view-string>* *<oid-string>* {include|exclude} **no snmp-server view *<view-string>* [*<oid-string>*]**	Настройка вида на коммутаторе. Эта команда используется для SNMP v3.

8. Настройка TRAP

Команда	Описание
Режим глобального конфигурирования	
snmp-server enable traps **no snmp-server enable traps**	Включить отправку Trap сообщений. Эта команда используется для SNMP v1/0/v2/v3.
snmp-server host {<host-ipv4-address> | <host-ipv6-address>} {v1 | v2c | {v3 {noauthnopriv | authnopriv | authpriv}}} *<user-string>* **no snmp-server host {<host-ipv4-address> | <host-ipv6-address>} {v1 | v2c | {v3 {noauthnopriv / authnopriv | authpriv}}} *<user-string>***	Установка IPv4/IPv6 адреса хоста, который используется для получения информации SNMP Trap. Для SNMP v1/0/v2, эта команда также настраивает строку сообщества для Trap; для SNMP v3 , эта команда также настраивает имя пользователя и уровень безопасности Trap. Команда "no", отменяет этот IPv4 или IPv6 адрес.
snmp-server trap-source {<ipv4-address> | <ipv6-address>} **no snmp-server trap-source {<ipv4-address> | <ipv6-address>}**	Установка IPv4 или IPv6 адреса источника, который используется для отправки trap пакетов, команда "no»удаляет конфигурацию.

9. Включение / выключение RMON

Команда	Описание
Режим глобального конфигурирования	
rmon enable **no rmon enable**	Включение / выключение RMON

2.4.5 Типичные примеры настройки SNMP

IP-адрес NMS 1.1.1.5, IP-адрес коммутатора (агента) 1.1.1.9 .

Сценарий 1: Программное обеспечение NMS использует протокол SNMP для получения данных от коммутатора.

Конфигурация коммутатора, записана ниже:

```
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 может использовать частную строку сообщества для доступа к коммутатору для чтения и записи разрешений или использовать публичную строку сообщества для доступа к коммутатору только для чтения разрешений.

Сценарий 2: NMS будет получать Trap сообщения от коммутатора (Примечание: NMS, возможно, проверит значение строки сообщества для Trap сообщений. В этом случае NMS использует подтверждение строки сообщества usertrap).

Конфигурация коммутатора, изложена ниже:

```
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 SNMP v3, чтобы получить информацию от коммутатора.

Конфигурация коммутатора, изложена ниже:

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

Сценарий 4: NMS хочет получить v3Trap сообщение, отправленное коммутатором.

Конфигурация коммутатора, изложена ниже:

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server host 10.1.1.2 v3 authpriv tester
Switch(config)#snmp-server enable traps
```

Сценарий 5: IPv6 адреса NMS 2004:1:2:3::2; IPv6 адреса коммутатора (агента) 2004:1:2:3::1. Пользователи NMS используют протокол SNMP для получения данных от коммутатора.

Конфигурация коммутатора, изложена ниже:

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server community rw private
Switch(config)#snmp-server community ro public
Switch(config)#snmp-server securityip 2004:1:2:3::2
```

NMS может использовать частную строку сообщества для доступа к коммутатору для чтения и записи разрешений или использовать публичную строку сообщества для доступа к коммутатору только для чтения разрешений.

Сценарий 6: NMS будет получать Trap сообщения от коммутатора (Примечание: NMS, возможно, проверит значение строки сообщества для Trap сообщений. В этом случае NMS использует подтверждение строки сообщества usertrap).

Конфигурация коммутатора, изложена ниже:

```
Switch(config)#snmp-server host 2004:1:2:3::2 v1 usertrap
Switch(config)#snmp-server enable traps
```

2.4.6 Поиск неисправностей SNMP

Когда пользователи настраивают SNMP, SNMP сервер может не работать должным образом из-за отказа физического соединения и неправильной конфигурации и т.д. Пользователи могут устранить проблемы, выполнив требования, указанные ниже:

- ❖ Убедиться в надежности физического соединения.
- ❖ Убедиться, что интерфейс и протокол передачи данных находятся в состоянии «up» (используйте команду "Show interface"), а также связь между коммутатором и хостом может быть проверена путем pinga (используйте команду "ping").
- ❖ Убедиться, что включена функция SNMP агента. (Использовать команду "snmp-server ")
- ❖ Убедиться, что безопасность IP для NMS (использовать команду "snmp-server securityip") и строка сообщества (использовать команду "snmp-server community") правильно настроены. Если что-то из этого не настроено, SNMP не сможет общаться с NMS должным образом.
- ❖ Если необходима Trap функция, не забудьте включить Trap (использовать команду "snmp-server enable traps"). И не забудьте правильно настроить IP-адрес хоста и строку сообщества для Trap (использовать команду "snmp-server host"), чтобы обеспечить отправку Trap сообщений на указанный хост.
- ❖ Если необходима RMON функция, она должна быть включена (использовать команду "rmon enable").
- ❖ Используйте команду "show snmp», чтобы проверить отправленные и полученные сообщения SNMP; Используйте команду "show snmp status", чтобы проверить информацию о конфигурации SNMP; Используйте команду "debug snmp packet", чтобы включить функции отладки и проверки SNMP.
- ❖ Если пользователь по-прежнему не может решить проблемы с SNMP, обращайтесь в технический центр.

2.5 Модернизация коммутатора

Коммутатор предоставляет два способа обновления: обновление BootROM и TFTP/FTP обновление под Shell.

2.5.1 Системные файлы коммутатора

Системные файлы включают в себя файлы образа системы (image) и загрузочные (boot) файлы. Обновление системных файлов коммутатора подразумевает собой перезапись старых файлов новыми.

Файл образа системы включает в себя сжатые файлы аппаратных драйверов, файлы программного обеспечения и т. д., это то, что мы обычно называем «IMG file».

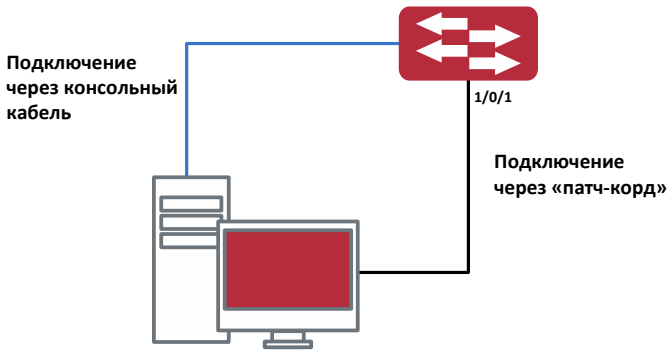
Загрузочные (boot) файлы необходимы для загрузки и запуска коммутатора, это то, что мы обычно называем «ROM file» (могут быть сжаты в IMG файлы, если они слишком больших размеров). В коммутаторе загрузочные файлы разрешено сохранять в только в ROM.

Коммутатор определяет путь и имена для файлов загрузки как flash:/boot.rom и flash:/config.rom.

Коммутатор предоставляет пользователю два режима обновления: 1. BootROM режим; 2. TFTP и FTP обновление в режиме Shell. Эти два способа обновления будут описаны подробно в следующих двух разделах.

2.5.2 BootROM обновление

Есть два метода для BootROM обновления: TFTP и FTP, которые могут быть выбраны в командах настройки BootROM.



Типичная топология для обновления коммутатора в режиме BootROM

Процедура обновления перечислена ниже:

Шаг 1:

Как показано на рисунке, используется консольный кабель для подключения ПК к порту управления на коммутаторе. ПК должен иметь программное обеспечение FTP / TFTP сервера, а также файл image необходимый для обновления.

Шаг 2:

Нажмите "Ctrl + B" во время загрузки коммутатора для переключения в режим BootROM монитора. Результат операции показан ниже:

Boot#

Шаг 3:

В BootROM режиме, запустите "setconfig", чтобы установить IP-адрес и маску коммутатора для режима BootROM, IP-адрес и маску сервера, а также выберите TFTP или FTP обновления. Предположим, что адрес коммутатора 192.168.1.2, а адрес компьютера 192.168.1.66 и выберите TFTP обновление конфигурации. Это будет выглядеть так:

```
Boot# config
Host IP Address: [10.1.1.1] 192.168.1.1
Server IP Address: [10.1.1.2] 192.168.1.2
Boot#
```

Шаг 4:

Включить FTP / TFTP сервер на ПК. Для TFTP запустите программу сервера TFTP, для FTP запустите программу FTP-сервер. Прежде, чем начать загрузку файла обновления на коммутатор, проверьте соединение между сервером и коммутатором с помощью ping’а с

сервера. Если ping успешен, запустите команду "run" в BootROM режиме. После чего начнётся запуск файла ПО непосредственно с tftp-сервера.

```
Boot# run tftp:nos.img
Loading nos.img ...
Using rtl8390#0 device
TFTP from server 192.168.1.2; our IP address is 192.168.1.1
Filename 'nos.img'.
Load address: 0x81000000
```

Шаг 5:

После удачной загрузки, произведите обновление коммутатора из Shell режима. См. пункт 2.5.2.1 «Примеры настройки FTP/TFTP».

2.5.3 Обновление FTP/TFTP

2.5.3.1 Введение в FTP/TFTP

FTP (File Transfer Protocol) / TFTP (Trivial File Transfer Protocol) являются протоколами передачи файлов, они оба принадлежат к четвертому уровню (уровню приложений) в TCP / IP стеке протоколов, используемому для передачи файлов между компьютерами, узлами и коммутаторами. Оба они передают файлы в клиент-серверной модели. Разница между ними описана ниже.

FTP основан на протоколе TCP для обеспечения надежной связи и транспортировки потока данных. Тем не менее, он не предусматривает процедуру авторизации для доступа к файлам и использует простой механизм аутентификации (передает имя пользователя и пароль для аутентификации в виде открытого текста). При использовании FTP для передачи файлов, должны быть установлены два соединения между клиентом и сервером: управляющее соединение и соединение передачи данных. Далее должен быть послан запрос на передачу от FTP-клиента на порт 21 сервера для установления управляющего соединения и согласования передачи данных через управляющее соединение.

Существует два типа таких соединений: активные и пассивные соединения.

При активном подключении клиент передает его адрес и номер порта для передачи данных серверу, управляющее соединение поддерживается до завершения передачи этих данных. Затем, используя адрес и номер порта, предоставленных клиентом, сервер устанавливает соединение на порт 20 (если не занят) для передачи данных, если порт 20 занят, сервер автоматически генерирует другой номер порта для установки соединения.

При пассивном подключении, клиент через управляющее соединение просит сервер установить подключение. Затем сервер создает свой порт для прослушивания данных и уведомляет клиента о номере этого порта, далее клиент устанавливает соединение с указанным портом.

TFTP основан на протоколе UDP, обеспечивающим службу передачи данных без подтверждения доставки и без аутентификации и авторизации. Он обеспечивает правильную передачу данных путем механизма отправки подтверждения и повторной передачи тайм-аут пакетов. Преимущество TFTP перед FTP в том, что первый гораздо проще и имеет низкие накладные расходы передачи данных.

Коммутатор может работать как FTP / TFTP клиент или сервер. Когда коммутатор работает как FTP / TFTP клиент, файлы конфигурации и системные файлы можно загрузить

с удаленного FTP / TFTP сервера (это могут быть как хосты, так и другие коммутаторы) без ущерба для его нормальной работы. И также может быть получен список файлов с сервера в режиме FTP клиента. Конечно, коммутатор может также загрузить текущие конфигурационные файлы и системные файлы на удаленный FTP / TFTP сервер (это могут быть как хосты, так и другие коммутаторы). Когда коммутатор работает как FTP / TFTP сервер, он может обеспечить загрузку и выгрузку файлов для авторизованных FTP / TFTP клиентов.

Вот некоторые термины часто используемые в FTP/TFTP.

ROM: Сокращенно от EPROM, СПЗУ. EPROM заменяет FLASH память в коммутаторе.

SDRAM: ОЗУ в коммутаторе, которая используется для работы системы и программного обеспечения, а также хранилища последовательности конфигурации.

FLASH: Флэш память используется для хранения файлов системы и файла конфигурации.

System file: включает в себя образ системы и загрузочный файл.

System image file: файл образа системы включает в себя сжатые файлы аппаратных драйверов, файлы программного обеспечения, это то, что мы обычно называем «IMG file». IMG файл может быть сохранен только в FLASH.

Boot file: необходимы для загрузки и запуска коммутатора, это то, что мы обычно называем «ROM file» (могут быть сжаты в IMG файлы, если они слишком больших размеров). В коммутаторе загрузочные файлы разрешено сохранять в только в ROM.

Коммутатор определяет путь и имена для файлов загрузки как flash:/boot.rom и flash:/config.rom.

Configuration file: включает в себя файл начальной конфигурации и файл текущей конфигурации. Разница в свойствах между этими файлами позволяет облегчить резервное копирование и обновление конфигураций

Start up configuration file: это последовательность команд конфигурации, используемая при запуске коммутатора. Файл начальной конфигурации хранится в энергонезависимой памяти. Если устройство не поддерживает CF, файл конфигурации хранится только во FLASH. Если устройство поддерживает CF, файл конфигурации хранится во FLASH-памяти или CF. Если устройство поддерживает мультиконфигурационный файл, они должны иметь расширение .cfg, имя по-умолчанию startup.cfg. Если устройство не поддерживает мультиконфигурационный файл, имя файла начальной конфигурации должно быть startup-config.

Running configuration file: это текущая(running) последовательность команд конфигурации, используемая коммутатором. Текущий конфигурационный файл хранится в оперативной памяти. В процессе работы текущая конфигурация running-config может быть сохранена из RAM во FLASH память командой «write» или «copy running-config startup-config».

Factory configuration file: файл конфигурации, поставляемый с коммутатором, так называемый factory-config. Для того, чтобы загрузить заводской файл конфигурации и перезаписать файл начальной конфигурации необходимо ввести команды «set default» и «write», а затем перезагрузить коммутатор.

2.5.3.2 Настройка FTP/TFTP

Конфигурации коммутатора как FTP и TFTP клиента почти одинаковы, поэтому процедуры настройки для FTP и TFTP в этом руководстве описаны вместе.

1. Настройка FTP/TFTP клиента

(1) Загрузка файлов FTP/TFTP клиентом

Команда	Пояснение
Режим администратора	
copy *<source-url>* *<destination-url>* [ascii | binary]	Загрузка файлов FTP/TFTP клиентом

(2) Просмотр доступных файлов на FTP сервере

Команда	Пояснение
Режим администратора	
ftp-dir *<ftpServerUrl>*	Просмотр доступных файлов на FTP сервере. Формат адреса в данном случае выглядит так: ftp://пользователь:пароль @IPv4|IPv6 адрес.

2. Настройка FTP сервера

(1) Запуск FTP сервера

Команда	Пояснение
Глобальный режим	
ftp-server enable **no ftp-server enable**	Запуск сервера, команда «no» выключает сервер

(2) Настройка имени пользователя и пароля для входа на FTP сервер.

Команда	Пояснение
Глобальный режим	
ip ftp username *<username>* password [0 | 7] *<password>* **no ip ftp username*<username>***	Настройка имени пользователя и пароля для входа на FTP сервер. Команда «no»удалит имя пользователя и пароль

(3) Изменение времени ожидания FTP сервера

Команда	Пояснение
Глобальный режим	
ftp-server timeout *<seconds>*	Выставляет время ожидания до разрыва связи

3. Настройка TFTP сервера

(1) Запуск TFTP сервера

Команда	Пояснение
Глобальный режим	
tftp-server enable **no tftp-server enable**	Запуск сервера, команда «no» выключает сервер

(2) Изменение времени ожидания TFTP сервера

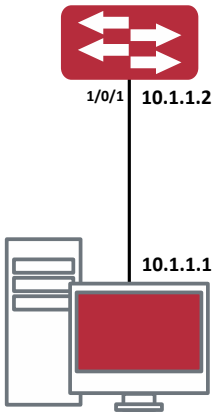
Команда	Пояснение
Глобальный режим	
tftp-server retransmission-timeout *<seconds>*	Выставляет таймаут до ретрансляции пакета

(3) Настройка количества раз ретрансляции до таймаута для неповрежденных пакетов

Команда	Пояснение
Глобальный режим	
tftp-server retransmission-number *<number>*	Устанавливает число ретрансляций

2.5.3.3 Примеры настройки FTP/TFTP

Настройки одинаковы для IPv4 и IPv6 адресов. Пример показан только для IPv4 адреса.



Загрузка nos.img файла FTP/TFTP клиентом

Сценарий 1: Использование коммутатора в качестве FTP/TFTP клиента. Коммутатор соединяется одним из своих портов с компьютером, который является FTP/TFTP сервером с IP-адресом 10.1.1.1, коммутатор действует как FTP/TFTP клиент, IP-адрес интерфейса VLAN1 коммутатора 10.1.1.2. Требуется загрузить файл "nos.img" с компьютера в коммутатор.

Настройка FTP

Настройка компьютера:

Запустите программное обеспечение FTP сервера на компьютере и установите имя пользователя "PC" и пароль "superuser". Поместите файл "12_30_nos.img" в соответствующий каталог FTP сервера на компьютере.

Далее описана процедура настройки коммутатора:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#exit
Switch#copy ftp://PC:superuser@10.1.1.1/0/12_30_nos.img nos.img
```

Сценарий 2: Использование коммутатора в качестве FTP сервера. Коммутатор работает как сервер и подключается одним из своих портов к компьютеру, который является клиентом. Требуется передать файл «nos.img» с коммутатора на компьютер и сохранить его как «12_25_nos.img».

Далее описана процедура настройки коммутатора:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#ftp-server enable
Switch(config)# username admin password 0 superuser
```

Настройка компьютера:

Зайдите на коммутатор с любого FTP клиента с именем пользователя «admin» и паролем «superuser», используйте команду «get nos.img 12_25_nos.img» для загрузки файла «nos.img» с коммутатора на компьютер.

Сценарий 3: Использование коммутатора в качестве TFTP сервера. Коммутатор работает как TFTP сервер и соединяется одним из своих портов с компьютером, который является TFTP клиентом. Требуется передать файл «nos.img» с коммутатора на компьютер

Далее описана процедура настройки коммутатора:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#tftp-server enable
```

Настройка компьютера:

Зайдите на коммутатор с любого TFTP клиента, используйте команду «tftp» для загрузки «nos.img» файла с коммутатора на компьютер.

Сценарий 4: Коммутатор выступает как FTP клиент для просмотра списка файлов на FTP сервере. Условия синхронизации: коммутатор соединен с компьютером через Ethernet порт, компьютер является FTP сервером с IP адресом 10.1.1.1; Коммутатор выступает как FTP клиент с IP адресом интерфейса VLAN1 10.1.1.2.

Настройка FTP:

Настройка компьютера:

Запустите FTP сервер на компьютере и установите имя пользователя «PC», и пароль «superuser»

Настройка коммутатора:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch#copy ftp: //PC:superuser@10.1.1.1
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.
150 Opening ASCII mode data connection for /bin/ls.
recv total = 480
nos.img
nos.rom
parsecommandline.cpp
position.doc
qmdict.zip
…(some display omitted here)
show.txt
```

```
snmp.TXT
226   ansfer complete.
```

2.5.3.4 Устранение неисправностей FTP/TFTP

Поиск неисправностей FTP

Перед началом процесса загрузки/скачивания системных файлов с помощью протокола FTP необходимо проверить наличие соединения между клиентом и сервером, это можно осуществить с помощью команды «ping». Если эхо-тестирование неудачно, следует устранить неполадки с соединением.

Следующее сообщение, отображается при успешной отправке файлов. Если оно не появилось, пожалуйста, проверьте подключение к сети и повторите команду «copy» еще раз.

```
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.
```

Если коммутатор обновляет файл прошивки или файл начальной конфигурации через FTP, он не должен перезапускаться пока не появится сообщение "close ftp client» или "226 Transfer complete» указывающие на успешное обновление, в противном случае коммутатор может быть поврежден и его запуск будет невозможен. Если обновление через FTP не удается, попробуйте еще раз или используйте режим BootROM для обновления.

Поиск неисправностей TFTP

Перед началом процесса загрузки/скачивания системных файлов с помощью протокола TFTP необходимо проверить наличие соединения между клиентом и сервером, это можно осуществить с помощью команды «ping». Если на отправленный echo-request не было получено ответа, следует устранить неполадки с соединением.

Следующее сообщение, отображается при успешной отправке файлов. Если оно не появилось, пожалуйста, проверьте подключение к сети и повторите команду «copy» еще раз.

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

Следующее сообщение, отображается при успешном получении файлов. Если оно не появилось, пожалуйста, проверьте подключение к сети и повторите команду «copy» еще раз.

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

```
close tftp client.
```

Если коммутатор обновляет файл прошивки или файл начальной конфигурации через TFTP, он не должен перезапускаться пока не появится сообщение "close tftp client» или "226 Transfer complete» указывающие на успешное обновление, в противном случае коммутатор может быть поврежден и его запуск будет невозможен. Если обновление через TFTP не удается, попробуйте еще раз или используйте режим BootROM для обновления.

3 КОНФИГУРИРОВАНИЕ ПОРТОВ

3.1 Введение

В коммутаторе существуют кабельные и комбо порты. Комбо порт может быть сконфигурирован как 1000G-TX порт, так и как оптический SFP Gigabit порт.

Если пользователь хочет сконфигурировать сетевой порт, он может ввести команду «interface ethernet <interface-list>» для входа в соответствующий режим конфигурации порта, где <interface-list> содержит один или несколько портов. Если <interface-list> содержит несколько портов, номера портов разделяются специальными символами «,» и «-», где «,» используется для перечисления портов, а «-» для указания диапазона номеров портов. Положим, операция должна быть выполнена над портами 2,3,4,5. Тогда команда будет выглядеть так «interface ethernet 1/0//2-5». В режиме конфигурации порта можно изменять скорость, режим дуплекса и настраивать управление траффиком, при этом данные изменения требуют соответствующих изменений на ответных сетевых портах.

3.2 Список команд для конфигурирования портов

1. Вход в режим конфигурации порта
2. Конфигурация параметров сетевого порта
(1) Конфигурация режима combo для combo портов
(2) Включить/выключить порты
(3) Конфигурация имени порта
(4) Конфигурация типа кабеля на порту
(5) Конфигурация скорости и дуплекса на порту
(6) Конфигурация контроля полосы пропускания
(7) Конфигурация управления траффиком
(8) Включение/выключение функции распознавания петли
(9) Конфигурация контроля широковещательных штормов на коммутаторе
(10) Конфигурация режима сканирования порта
(11) Конфигурация контроля нарушения скорости на порту
(12) Конфигурация интервала сбора статистики по скорости порта
3. Виртуальный тест кабеля

1. Вход в режим конфигурации Ethernet порта

Команда	Описание
Режим глобального конфигурирования	
interface ethernet *<interface-list>*	Вход в режим конфигурации Ethernet порта.

2. Конфигурация параметров сетевого порта

Команда	Описание
Режим порта	

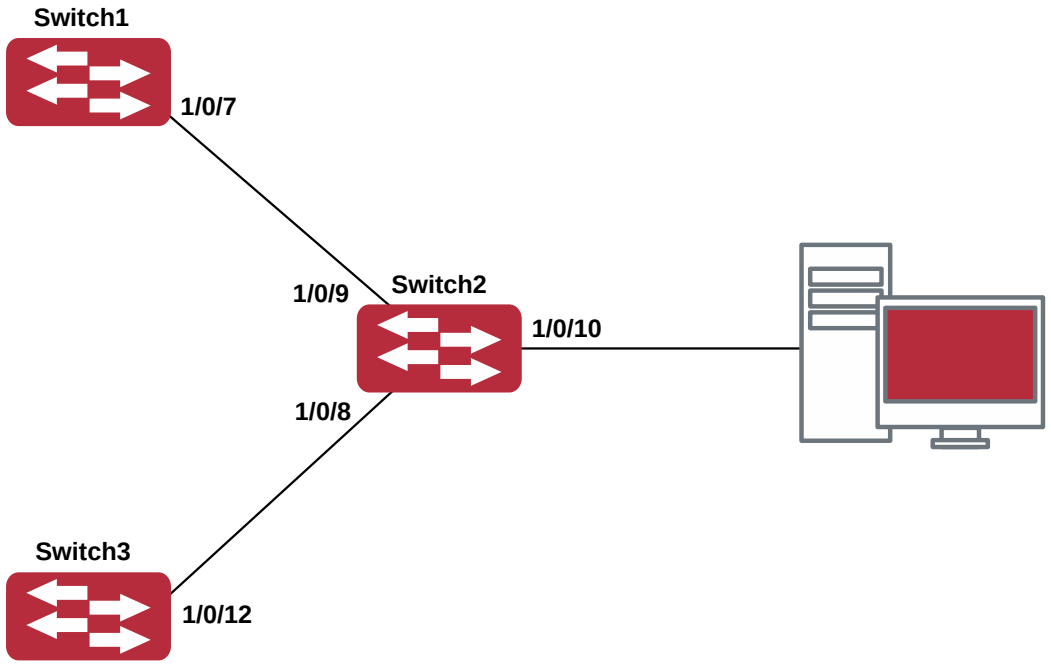
media-type {copper | fiber}	Установка режима combo порта (только для combo).
shutdown **no shutdown**	Включение/выключение указанного порта.
description *<string>* **no description**	Назначение или отмена имени порта.
speed-duplex {auto [10 [100 [1000]] | force10-half | force10-full | force100-half | force100-full | force100-fx [module-type {auto-detected | no-phy-integrated | phy-integrated}] | {{force1g-half | force1g-full} [nonegotiate [master | slave]]}| force10g-full} **no speed-duplex**	Установка скорости и дуплекса на порту для 100/1000Base-TX или 100Base-FX ports. С оператором NO данная команда восстанавливает параметры порта по умолчанию, то есть договорную скорость и автоматическое определение дуплекса.
negotiation {on|off}	Включение/выключение функции автоматического определения параметров для 1000Base-FX.
bandwidth control *<bandwidth>* [both | receive | transmit] **no bandwidth control**	Установка или отмена значения полосы пропускания, используемой для входящего/исходящего трафика для указанных портов.
flow control **no flow control**	Включение/выключение функции контроля траффика для указанных портов.
loopback **no loopback**	Включение/выключение функции петли для указанных портов.
storm-control {unicast | broadcast | multicast} *<Kbits>*	Включение функции контроля штормов для широковещательных, многопользовательских и персональных пакетов с неизвестным адресом назначения (коротких для широковещательного) и установка допустимого числа широковещательных пакетов; формат NO данной команды отключает функцию контроля широковещательных штормов.
Switchport flood-control {bcast|mcast|ucast}	Конфигурирование коммутатора не передавать широковещательные, многопользовательские и персональные

no switchport flood-control {bcast|mcast|ucast}	пакеты в указанный порт, команда no отключает данную функцию.
rate-violation <200-2000000> [recovery <0-86400>|] **no rate-violation**	Устанавливает максимальную скорость приема пакетов на порту. Если скорость принятия пакетов превышает разрешенную, команда выключает этот порт и конфигурирует время восстановления порта (по умолчанию 300с). Команда NO отключает установку.
Общий режим	
port-rate-statistics interval [<interval - value>]	Конфигурация интервала сбора статистики по скорости.

3. Виртуальный тест кабеля

Команда	Описание
Режим конфигурации порта	
virtual-cable-test interface ethernet	Тест виртуального кабеля на порте.

3.3 Примеры конфигурации порта



Пример конфигурации порта

VLAN не сконфигурированы на коммутаторе. По умолчанию используется VLAN1.

Коммутатор	Порт	Свойства
Switch1	1/0/7	Лимит входящей полосы: 50 Mb
Switch2	1/0/8	Зеркалированный порт источника
	1/0/9	100Mbps full, зеркалированный порт источника
	1/0/10	1000Mbps full, зеркалированный порт назначения
Switch3	1/0/12	100Mbps full

Конфигурация приведена ниже:

```
Switch1:
Switch1(config)#interface ethernet 1/0/7
Switch1(Config-If-Ethernet1/0/7)#bandwidth control 50000 receive

Switch2:
Switch2(config)#interface ethernet 1/0/9
Switch2(Config-If-Ethernet1/0/9)#speed-duplex force100-full
Switch2(Config-If-Ethernet1/0/9)#exit
Switch2(config)#interface ethernet 1/0/10
Switch2(Config-If-Ethernet1/0/10)#speed-duplex force1g-full
Switch2(Config-If-Ethernet1/0/10)#exit
Switch2(config)#monitor session 1 source interface ethernet1/0/8;1/0/9
Switch2(config)#monitor session 1 destination interface ethernet 1/0/10

Switch3:
Switch3(config)#interface ethernet 1/0/12
Switch3(Config-If-Ethernet1/0/12)#speed-duplex force100-full
Switch3(Config-If-Ethernet1/0/12)#exit
```

3.4 Устранение неисправностей на порту

Здесь приводится несколько ситуаций, часто встречающихся при конфигурации порта, и предлагаются их решения:

❖ Два соединенных оптических интерфейса не поднимаются если один интерфейс настроен на автоопределение, а на втором жестко установлены скорость и дуплекс. Это определяется стандартом IEEE 802.3.

❖ Не рекомендуется следующая конфигурация: включение контроля трафика и одновременно установление лимита для многопользовательских пакетов на том же порту; установка одновременно контроля за широковещательными, многопользовательскими и персональными пакетами с неизвестным назначением и ограничения полосы на порту. Если такие комбинации установлены, пропускная способность порта может оказаться меньше ожидаемой.

4 КОНФИГУРАЦИЯ ФУНКЦИИ ИЗОЛЯЦИИ ПОРТОВ

4.1 Введение в функцию изоляции портов

Изоляция портов — это независимая порто-ориентированная функция, работающая между портами, которая изолирует потоки различных портов друг от друга. С помощью этой функции пользователь может изолировать порты в пределах VLAN для сохранения ресурсов VLAN и усиления секретности сети. После того, как эта функция будет сконфигурирована, порты в группе изолированных портов будут изолированы друг от друга, в то время как порты из различных групп изоляции или неизолированных могут пересылать данные друг другу совершенно нормально. На коммутаторе может быть сконфигурировано не более 16 групп изоляции портов.

4.2 Список команд для конфигурации изоляции портов

1. Создать группу изолированных портов
2. Добавить Ethernet порты в группу
3. Отобразить конфигурацию группы изоляции портов

1. Создать группу изолированных портов

Команда	Описание
Режим глобального конфигурирования	
isolate-port group <*WORD*> **no isolate-port group <*WORD*>**	Создает группу изолированных портов. С оператором NO эта команда удаляет группу изолированных портов.

2. Добавить Ethernet порты в группу

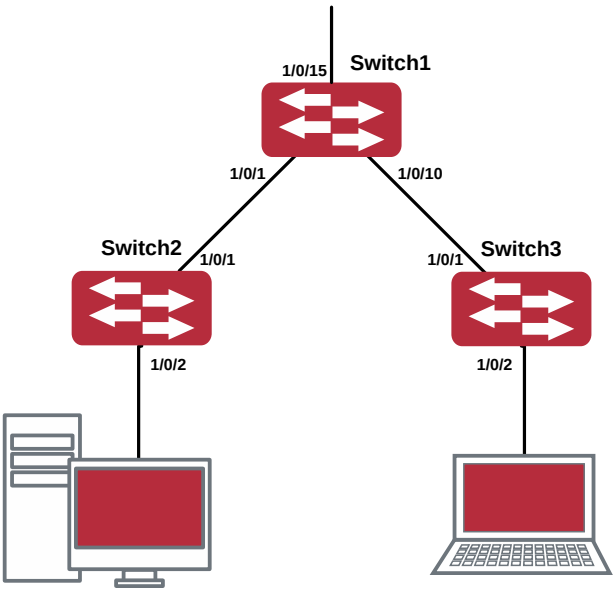
Команда	Описание
Режим глобального конфигурирования	
isolate-port group <*WORD*> switchport interface [ethernet | port-channel] <*IFNAME*> **no isolate-port group <*WORD*> switchport interface [ethernet | port-channel] <*IFNAME*>**	Добавляет один порт или группу портов в группу изолированных портов, которые будут изолированы от других портов в группе. Оператор NO удаляет один порт или группу портов из группы изолированных портов.

3. Отобразить конфигурацию группы изоляции портов

Команда	Описание
Режим администратора, Режим глобального конфигурирования	

show isolate-port group [*<WORD>*]	Показывает конфигурацию групп изолированных портов, включая все сконфигурированные группы изолированных портов и Ethernet порты в каждой группе.

4.3 Типовые примеры функции изоляции портов



Типовые примеры функции изоляции портов

Топология и конфигурация коммутаторов показана на рисунке выше. Порты e1/0/1, e1/0/10 и e1/0/15 все принадлежат к VLAN 100. Требование заключается в том, чтобы после включения функции изоляции портов на коммутаторе Switch1 порты e1/0/1 и e1/0/10 на этом коммутаторе не могли связываться друг с другом и оба могли связываться с портом e1/0/15, смотрящим в сеть. То есть связи между любыми парами downlink портов - нет, и в то же время связь между любым downlink портом и uplink - работает. Вышестоящий порт может работать с любым портом нормально.

Конфигурация коммутатора SWITCHA:

```
Switch(config)#isolate-port group test
Switch(config)#isolate-port group test switchport interface ethernet 1/0/1;1/0/10
```

5 КОНФИГУРАЦИЯ ФУНКЦИИ РАСПОЗНАВАНИЯ ПЕТЛИ НА ПОРТУ

5.1 Введение в функцию распознавания петли

С развитием сетевых устройств все больше и больше пользователей подключаются к сети через Ethernet-коммутаторы. В промышленных сетях пользователи получают доступ через коммутаторы 2-го уровня, что предъявляет строгие требования к взаимодействию между устройствами как внешней, так и внутренней сети. Когда требуется взаимодействие на 2-м уровне, сообщение должно отправляться точно в соответствии с MAC адресом для корректной работы между пользователями. Устройства второго уровня запоминают MAC адреса, изучая входящие MAC адреса источников пакетов и при поступлении пакета с неизвестным адресом источника они записывают его MAC адрес в таблицу, закрепляя его за портом, откуда пришел этот пакет. Таким образом следующий пакет с данным MAC адресом в качестве порта назначения будет отправлен сразу на этот порт. То есть адрес сразу фиксируется на порту для отправки всех пакетов.

Когда пакет с MAC адресом источника, уже изученным коммутатором, приходит через другой порт, запись в таблице MAC адресов изменяется таким образом, чтобы пакеты с данным MAC адресом направлялись через новый порт. В результате, если на участке между двумя адресатами существует какая-либо петля, все MAC адреса из сети второго уровня будут пересылаться на тот порт, где существует петля (обычно MAC адреса в этом случае с высокой частотой переключаются с одного порта на другой), что вызывает перегрузку и потерю работоспособности сети 2-го уровня. Вот почему необходимо проверять наличие петли на сетевых портах. Когда на порту определяется петля, обнаружившее ее устройство должно послать предупреждение в систему управления сетью, позволяя сетевому администратору обнаружить, локализовать и решить проблему в сети.

Поскольку система обнаружения петель может автоматически принимать решения о наличии петли в соединении и ее исчезновении, устройства с функциями контроля на портах (таких как изоляция портов и контроль за запоминанием MAC адресов) могут значительно снизить нагрузку с сетевого администратора, а также уменьшить время реакции на проблему, минимизируя воздействие петли на сеть.

5.2 Список команд для конфигурирования функции распознавания петли на порту

1. Конфигурирование временного интервала распознавания петли;
2. Включение функции распознавания петли;
3. Конфигурирование режима порта при распознавании петли;
4. Вывод отладочной информации по распознаванию петли;
5. Конфигурирование режима восстановления при распознавании петли

1. Конфигурирование временного интервала распознавания петли

Команда	Описание
Режим глобального конфигурирования	
loopback-detection interval-time *<loopback> <no-loopback>* **no loopback-detection interval-time**	Конфигурирование временного интервала распознавания петли

2. Включение функции распознавания петли

Команда	Описание
Режим конфигурирования порта	
loopback-detection specified-vlan <vlan-*list*> no loopback-detection specified-vlan <vlan-*list*>	Включение и выключение функции распознавания петли

3. Конфигурирование режима порта при распознавании петли

Команда	Описание
Режим конфигурирования порта	
loopback-detection control {shutdown |block} **no loopback-detection control**	Включение и выключение определенного режима порта при распознавании петли.

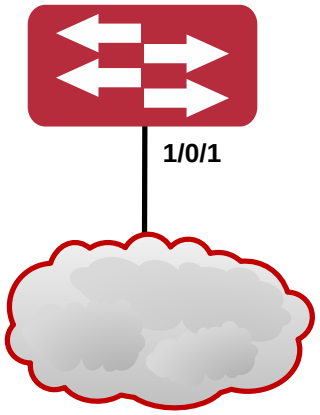
4. Вывод отладочной информации по распознаванию петли

Команда	Описание
Режим администратора	
debug loopback-detection **no debug loopback-detection**	Вывод отладочной информации по распознаванию петли. С оператором NO данная команда прекращает вывод отладочной информации.
show loopback-detection [interface *<interface-list>*]	Показывает статус и результаты распознавания петли на всех портах, если других параметров не вводится; в противном случае показывается статус и результат распознавания петли для конкретных портов

5. Конфигурирование режима восстановления при распознавании петли

Команда	Описание
Общий режим	
loopback-detection control-recovery timeout <0-3600>	Конфигурирование режима восстановления при распознавании петли (автоматическое восстановление или нет) или времени восстановления.

5.3 Примеры функции распознавания петли на порту



Типичный пример подключения

В приведенной ниже конфигурации, коммутатор определяет существование петли в топологии сети. После включения функции распознавания петли на порту, смотрящем во внешнюю сеть, коммутатор будет уведомлять подсоединенную сеть о существовании петли и контролировать порт коммутатора для обеспечения нормальной работы данной сети.

Последовательность конфигурации коммутатора:

```
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
```

Если выбран метод блокировки при определении петли, должен быть глобально включен протокол MSTP на всей сети, а также должны быть сконфигурированы соответствующие связи между протоколом связующего дерева и VLAN.

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

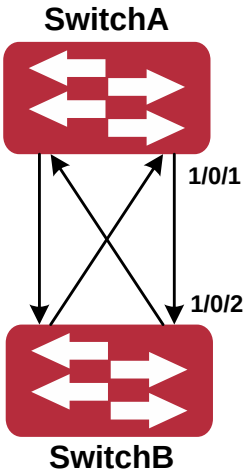
5.4 Решение проблем с функцией распознавания петли на порту

Функция распознавания петли на порту выключена по умолчанию и должна быть включена при необходимости.

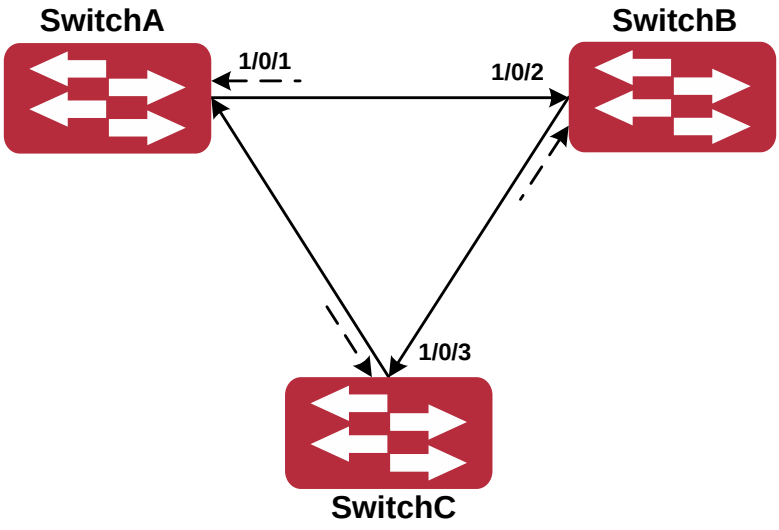
6 КОНФИГУРАЦИЯ ФУНКЦИИ ULDP

6.1 Общая информация о ULDP

Однонаправленный линк — это распространенная проблема в сети, особенно для оптических соединений. Под однонаправленным соединением понимается ситуация, когда один порт соединения может принимать сообщения от другого порта, а тот не может получать их от первого. Если физический уровень соединения есть и работает нормально, проблема связи между устройствами не может быть обнаружена. Как показано на рисунке, проблема оптического соединения не может быть обнаружена посредством механизмов физического уровня, таких как автоматическое согласование параметров.



Перекрестное подключение двунаправленного оптического соединения



Один из концов каждого двухнаправленного оптического соединения не подключен

Такой вид проблем часто возникает в ситуации, когда или интерфейс, или GBIC (Giga Bitrate interface Converter – конвертер интерфейса со скоростью 1Gb) имеют программные проблемы, в этом случае оборудование становится недоступным или работает неправильно. Однонаправленное соединение может вызывать целую серию проблем,

таких как зацикливание связующего дерева или широковещательным штормам (broadcast black hole).

ULDP (Unidirectional Link Detection Protocol – протокол обнаружения однонаправленных соединений) может помочь обнаружить неисправность, которая возникает в ситуациях, перечисленных выше. В коммутаторе, подключенном через оптическую или медную Ethernet линию (такую как витая пара пятой категории), ULDP может мониторить статус физических соединений. В случае, если обнаружено однонаправленное соединение, он посылает предупреждение пользователям и может выключить порт автоматически, или вручную, в зависимости от конфигурации пользователя.

Функция ULDP в коммутаторе распознает удаленные устройства и проверяет корректность соединений, используя интерактивную систему собственных сообщений. Когда ULDP включен на порту, механизм определения статуса порта запускается, что подразумевает посылку сообщений различного вида, которые посылаются различными подпрограммами этого механизма для проверки статуса соединений путем обмена информацией с удаленными устройствами. ULDP может динамически определять интервал, с которым удаленное устройство посылает свои уведомления и подстраивает в соответствии с ним свой локальный интервал. Кроме того, ULDP обеспечивает механизм рестарта, если порт был заблокирован ULDP, также соединение может быть проверено еще раз после рестарта. Временной интервал посылки уведомлений и рестарта порта в ULDP может конфигурироваться пользователями, таким образом ULDP может быстрее реагировать на проблемы соединений в различном сетевом окружении. Показателем правильной работы ULDP является работа соединения в дуплексном режиме, это значит, что ULDP включен на обоих концах соединения и использует одинаковый метод авторизации и пароль.

6.2 Список команд для конфигурирования ULDP

1. Включение функции ULDP на коммутаторе;
2. Включение функции ULDP на порту;
3. Конфигурация агрессивного режима на коммутаторе;
4. Конфигурация агрессивного режима на порту;
5. Конфигурация метода выключения однонаправленного соединения;
6. Конфигурация интервала уведомлений (Hello messages);
7. Конфигурация интервала восстановления;
8. Рестарт порта, выключенного функцией ULDP;
9. Демонстрационная и отладочная информация функции ULDP;

1. Включение функции ULDP на коммутаторе

Команда	Описание
Режим глобального конфигурирования	
uldp enable **uldp disable**	Включение или выключение функции ULDP на коммутаторе.

2. Включение функции ULDP на порту

Команда	Описание
Режим конфигурирования порта	
uldp enable **uldp disable**	Включение или выключение функции ULDP на порт.

3. Конфигурация агрессивного режима на коммутаторе

Команда	Описание
Режим глобального конфигурирования	
uldp aggressive-mode **no uldp aggressive-mode**	Устанавливает режим работы функции на коммутаторе.

4. Конфигурация агрессивного режима на порту

Команда	Описание
Режим конфигурирования порта	
uldp aggressive-mode **no uldp aggressive-mode**	Устанавливает режим работы функции на порту.

5. Конфигурация метода выключения однонаправленного соединения

Команда	Описание
Режим глобального конфигурирования	
uldp manual-shutdown **no uldp manual-shutdown**	Конфигурирует метод выключения однонаправленного соединения.

6. Конфигурация интервала уведомлений (Hello messages)

Команда	Описание
Режим глобального конфигурирования	
uldp hello-interval *<integer>* **no uldp hello-interval**	Конфигурация интервала уведомлений (Hello messages), диапазон от 5 до 100 секунд. Значение по умолчанию - 10 сек.

7. Конфигурация интервала восстановления

Команда	Описание
Режим глобального конфигурирования	
uldp recovery-time *<integer>* **no uldp recovery-time *<integer>***	Конфигурирует интервал восстановительного рестарта. Диапазон от 30 до 86400 секунд. Значение по умолчанию — 0 секунд.

8. Рестарт порта, выключенного функцией ULDP

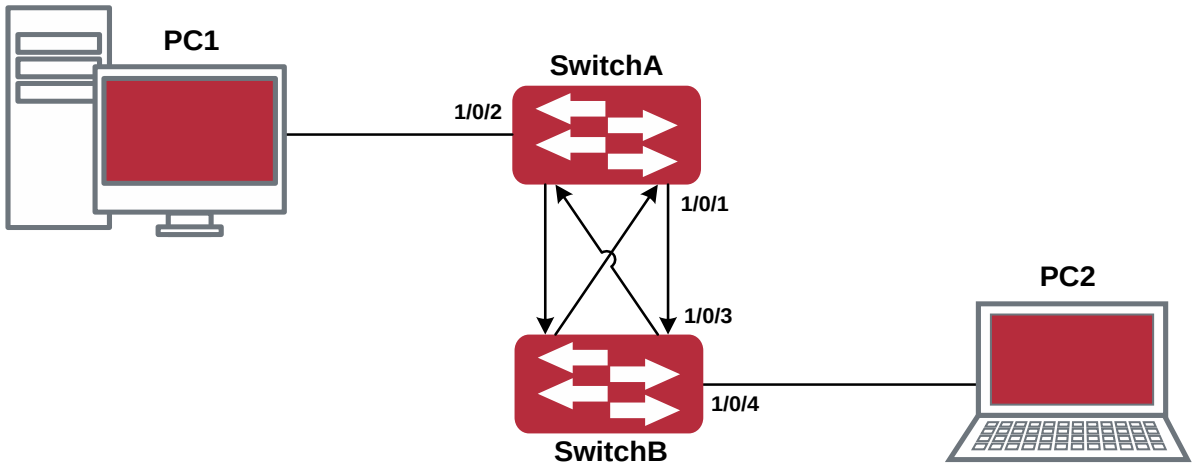
Команда	Описание
Режим глобального конфигурирования или режим конфигурирования порта	
uldp reset	Рестартует все порты в режиме глобального конфигурирования. Рестартует конкретный порт в режиме конфигурирования порта.

9. Демонстрационная и отладочная информация функции ULDP

Команда	Описание
Режим администратора	
show uldp [interface ethernet IFNAME]	Показывает информацию по ULDP. Для отображения общей ULDP информации параметров нет. При задании конкретного порта выводится общая информация и информация о соседях по данному порту.
debug uldp fsm interface ethernet *<IFname>* **no debug uldp fsm interface ethernet *<IFname>***	Включение или выключение вывода отладочной информации по определенному порту.
debug uldp error **no debug uldp error**	Включение или выключение отладочной информации об ошибках
debug uldp event **no debug uldp event**	Включение или выключение отладочной информации о событиях
debug uldp packet {receive|send} **no debug uldp packet {receive|send}**	Включение или выключение вывода отладочной информации по типу сообщений

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*>**	Включение или выключение вывода детальной информации об определенном типе сообщений, которые могут посылаться или приниматься на определенном порту.

6.3 Типовые примеры функции ULDP



Перекрестное подключение двунаправленного оптического соединения

В сетевой топологии на рисунке порт 1/0/1 на коммутаторе A, а также порт 1/0/3 на коммутаторе B – оптические. И соединение имеет перекрестный тип. Физический уровень включен и работает нормально, но соединение на уровне данных неработоспособно. ULDP может определить и заблокировать такой тип ошибки на соединении. Конечным результатом будет то, что порт 1/0/1 на коммутаторе A, а также порт 1/0/3 на коммутаторе B будут заблокированы функцией ULDP. Порты смогут работать (не будут заблокированы) только если соединение будет корректным.

Последовательность конфигурации коммутатора A:

```
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
```

Последовательность конфигурации коммутатора B:

```
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
```

В результате порт 1/0/1 на коммутаторе A будет заблокирован функцией ULDP и на дисплее терминала PC1 появится следующая информация.

```
%Oct 29 11:09:50 2007 A unidirectional link is detected! Port
Ethernet1/0/1 need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/1 shut down!
```

Порт 1/0/3 на коммутаторе B будет заблокирован функцией ULDP и на дисплее терминала PC2 появится следующая информация.

```
%Oct 29 11:09:50 2007 A unidirectional link is detected! Port
Ethernet1/0/3 need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/3 shutted down!
```

6.4 Устранение неполадок функции ULDP

Замечания по конфигурации:

- Для уверенности, что ULDP сможет определить, что один из оптических портов не подключен или порты некорректно соединены, порты должны работать в дуплексном режиме и иметь одинаковую скорость.
- Если механизм автоматического определения параметров оптических портов, один из которых включен некорректно, определит рабочий режим и скорость, ULDP не сможет отработать корректно, вне зависимости от того, включен он или нет. В данной ситуации порт помечается как выключенный.
- Для уверенности в том, что ответный порт корректно сконфигурирован и
- однонаправленное соединение сможет быть корректно определено, необходимо, чтобы на обоих концах соединения ULDP был включен и использовался одинаковый метод авторизации и пароль. В нашем примере пароль с обеих сторон не установлен.
- Интервал отправки hello сообщений может быть изменен (это 10 секунд по умолчанию и колеблется от 5 до 100 секунд), так что ULDP могут быстрее реагировать на ошибки подключения линий в различных условиях работы сети. Но этот интервал должен быть меньше 1/0/3 от времени конвергенции STP. Если интервал слишком длинный, петля STP будет сформирована до того, как ULDP обнаружит и отключит порт однонаправленного соединения. Если интервал слишком короткий, сетевая нагрузка на порт будет увеличена, что означает снижение пропускной способности.

ULDP не обрабатывает события LACP. Он обрабатывает каждое соединение группы TRUNK (например, port-channal, TRUNK порты) независимо друг от друга.
ULDP не работает с похожими протоколами других производителей. Это означает, что пользователи не могут использовать ULDP на одном конце и использовать другие подобные протоколы на другом конце соединения.
ULDP функция отключена по умолчанию. После включения функции ULDP в режиме глобального конфигурирования можно включить вывод отладочных сообщений. Существует несколько команд отладки (DEBUG) для вывода отладочной информации. Например, информацию о событиях, состоянии, ошибках и сообщениях. Различные типы отладочных сообщений также могут быть выведены в соответствии с различными значениями параметров.

- Таймер восстановления по умолчанию выключен и может быть включен только в случае, когда пользователь задал время восстановления (30-86400 секунд)

Команда рестарта и механизм перезагрузки порта воздействуют только на порт, который был выключен функцией ULDP.

7 НАСТРОЙКА ФУНКЦИИ LLDP

7.1 Общие сведения о функции LLDP

Протокол исследования соединительного уровня (Link Layer Discovery Protocol – LLDP) — это новый протокол, описанный в спецификации 802.1ab. Он позволяет соседним устройствам посылать уведомления о своем статусе другим устройствам и на всех портах любого устройства сохранять информацию об этом. Если необходимо, порты так же могут посылать информацию об изменении статуса устройствам, непосредственно подключенным к ним. Эта информация будет сохранена в стандартных MIB SNMP.Система управления сетью может проверять состояние соединений второго уровня по информации из MIB. LLDP не конфигурирует или контролирует элементы сети или потоки, он только описывает конфигурацию второго уровня. В спецификации 802.1ab также описывается, как используется информация, предоставляемая LLDP для обнаружения конфликтов на втором уровне. Институт стандартизации (IEEE) в настоящее время использует существующую физическую топологию, интерфейсы и наборы MIB IETF.

Упрощенно, LLDP – протокол обнаружения соседних устройств. Он определяет стандартный метод, позволяющий Ethernet устройствам, таким, как коммутаторы, маршрутизаторы и точки доступа уведомлять о своем существовании другие узлы сети и сохранять информацию обо всех соседних устройствах. Как следсвие, детальная информация о конфигурации устройства и о найденных соседях может объявляться посредством данного протокола.

В частности, LLDP определяет состав основного информационного объявления, передачу объявления и метод сохранения данной информации. Для объявления собственной информации устройство может посылать несколько частей информационного объявления в одном LAN пакете данных. Тип передачи определяется значением поля TLV (Type Length value – значение длины типа). Все устройства, поддерживающие LLDP, должны поддерживать оповещения о идентификаторе (ID) устройства и идентификаторе порта, но предполагается, что большинство устройств поддерживают оповещения об имени системы, ее описании и производительности системы. Оповещения с описанием системы и о производительности системы могут также содержать полезную информацию, необходимую для сбора информации о потоках в сети. Описание системы может включать такие данные как полное имя объявляемого устройства, тип устройства, версия его операционной системы и так далее.

Протокол LLDP позволяет упростить поиск проблем в корпоративной сети, расширить возможности инструментов управления сетью путем определения и хранения точной сетевой структуры.

Многие типы программ управления сетью используют функцию автоматического обнаружения («Automated Discovery») для отслеживания изменений и текущего состояния топологии, но большинство из них работает только на третьем уровне и в лучшем случае классифицирует устройства по их подсетям. Эти данные слишком примитивны, позволяют отслеживать только базовые события, такие как добавление или удаление устройств вместо детальной информации о них и о том, как устройства взаимодействуют с сетью.

Информация, собранная на 2 уровне, содержит сведения об устройствах, их портах и о том какие коммутаторы с какими соединены и т. п. Она так же может показывать

маршруты между клиентами, коммутаторами, маршрутизаторами и сетевыми серверами. Такие данные очень важны для определения и исследования источника проблем на сети.

LLDP является полезным инструментом управления, предоставляющим точную информацию о зеркалировании сети, отображении потоков данных и поиске сетевых проблем.

7.2 Список команд для конфигурирования LLDP

1. Включение LLDP на устройстве;
2. Включение функции LLDP на порту;
3. Конфигурация статуса LLDP на порту;
4. Конфигурация интервала обновления сообщений LLDP;
5. Конфигурация множителя времени поддержки сообщений LLDP;
6. Конфигурация задержки отправки обновляющих сообщений;
7. Конфигурация интервалов посылки TRAP пакетов;
8. Включение функции TRAP на порту;
9. Конфигурация дополнительных параметров информации для отправки на порту;
10. Конфигурация размера памяти, используемой для хранения таблиц на порту;
11. Конфигурация действий при переполнении памяти для таблицы на порту;
12. Отображение отладочной информации по функции LLDP;

1. Включение LLDP на устройстве

Команда	Описание
Режим глобального конфигурирования	
lldp enable **lldp disable**	Общее включение/выключение

2. Включение функции LLDP на порту

Команда	Описание
Режим конфигурирования порта	
lldp enable **lldp disable**	Включение/выключение функции LLDP на порту.

3. Конфигурация статуса LLDP на порту

Команда	Описание
Режим конфигурирования порта	
lldp mode (send|receive|both|disable)	Конфигурация режима работы функции LLDP

4. Конфигурация интервала обновления сообщений LLDP

Команда	Описание
Режим глобального конфигурирования	
lldp tx-interval *<integer>* **no lldp tx-interval**	Конфигурация интервала обновления сообщений LLDP как определенной величины или значения по умолчанию.

5. Конфигурация множителя времени поддержки сообщений LLDP

Команда	Описание
Режим глобального конфигурирования	
lldp msgTxHold *<value>* **no lldp msgTxHold**	Конфигурация множителя времени поддержки сообщений LLDP как определенной величины или значения по умолчанию.

6. Конфигурация задержки отправки обновляющих сообщений

Команда	Описание
Режим глобального конфигурирования	
lldp transmit delay *<seconds>* **no lldp transmit delay**	Конфигурация задержки отправки обновляющих сообщений как определенной величины или значения по умолчанию.

7. Конфигурация интервалов посылки TRAP пакетов

Команда	Описание
Режим глобального конфигурирования	
lldp notification interval *<seconds>* **no lldp notification interval**	Конфигурация интервалов посылки TRAP пакетов как определенной величины или значения по умолчанию.

8. Включение функции TRAP на порту

Команда	Описание
Режим конфигурирования порта	
lldp trap <enable|disable>	Включение/выключение функции TRAP на порту

9. Конфигурация дополнительных параметров информации для отправки на порту

Команда	Описание
Режим конфигурирования порта	
lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap] **no lldp transmit optional tlv**	Конфигурация дополнительных параметров информации для отправки на порту как определенной величины или значения по умолчанию.

10. Конфигурация размера памяти, используемой для хранения таблиц на порту

Команда	Описание
Режим конфигурирования порта	
lldp neighbors max-num *<value>* **no lldp neighbors max-num**	Конфигурация размера памяти, используемой для хранения таблиц на порту как определенной величины или значения по умолчанию.

11. Конфигурация действий при переполнении памяти для таблицы на порту

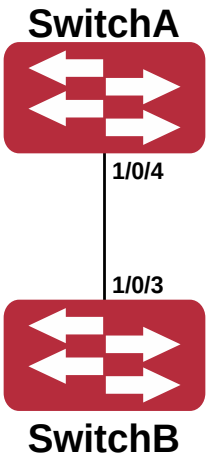
Команда	Описание
Режим конфигурирования порта	
lldp tooManyNeighbors {discard | delete}	Конфигурация действий при переполнении памяти для таблицы на порту

12. Отображение отладочной информации по функции LLDP

Команда	Описание
Admin, Режим глобального конфигурирования	
show lldp	Отображение текущей конфигурации функции LLDP.
show lldp interface ethernet *<IFNAME>*	Отображение информации о конфигурации LLDP на конкретном порту
show lldp traffic	Отображение информации обо всех счетчиках.
show lldp neighbors interface ethernet *<IFNAME>*	Отображение информации о LLDP соседях на данном порту.

show debugging lldp	Отображение всех портов с включенной функцией отладки LLDP
Режим администратора	
debug lldp **no debug lldp**	Включение/выключение вывода отладочной иинформации LLDP.
debug lldp packets interface ethernet *<IFNAME>* **no debug lldp packets interface ethernet *<IFNAME>***	Включение/выключение вывода отладочной информации о отправке или приеме пакетов LLDP на порту или на коммутаторе.
Режим конфигурирования порта	
clear lldp remote-table	Очистка таблицы соседей на порту

7.3 Типовой пример функции LLDP



Типовой пример конфигурации функции LLDP

На схеме сетевой топологии, приведенной выше, порт 1,3 на коммутаторе B подключен к порту 2,4 коммутатора A. Порт 1 коммутатора B сконфигурирован в режиме приема пакетов. Опция TLV на порту 4 коммутатора A сконфигурирована как portDes и SysCap.

Коммутатор A. Последовательность команд конфигурации:

```
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
```

Коммутатор B. Последовательность команд конфигурации:

```
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
```

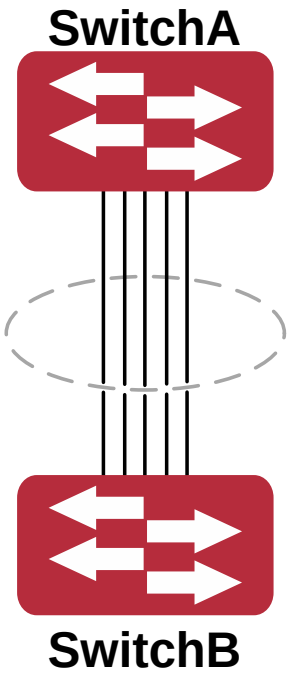
7.4 Устранение неисправностей функции LLDP

Функция LLDP по умолчанию выключена. После ее включения в режиме глобального конфигурирования, пользователи могут включить режим отладки «debug lldp» для проверки отладочной информации. Используя команду «show» функции LLDP можно вывести информацию о конфигурировании в глобальном режиме конфигурирования, либо в режиме настройки интерфейсов.

8 НАСТРОЙКА PORT CHANNEL

8.1 Общие сведения о Port channel

Для понимания термина порт-канала (Port channel) надо ввести понятие группы портов. Группа портов – это группа физических портов на конфигурационном уровне. Только физические порты в группе портов могут быть частью объединенного канала и стать участниками Port channel. Логически группа портов является не портом, а набором портов. При определенных условиях физические порты в группе портов позволяют посредством объединения портов сформировать Port channel, который обладает всеми свойствами логического порта и таким образом становится независимым логическим портом. Агрегация портов — это абстрактное понятие, подразумевающее по собой объединение набора портов с одинаковыми свойствами в логический порт. Port channel — это набор физических портов, который логически используется как один физический порт. Он может использоваться пользователем как обычный порт. Он не может не только добавить пропускной способности на сеть, но и способен обеспечить резервирование соединений. Обычно объединение портов используется, когда коммутатор подключен к маршрутизатору, клиентской станции или другим коммутаторам.



Агрегирование портов

Как показано выше, коммутатор SwitchA объединил порты в Port channel. Пропускная полоса Port channel равна сумме пропускных способностей четырех портов. Когда необходимо передать трафик с коммутатора SwitchA на SwitchB, распределение трафика будет определяться на основе MAC адреса источника и младшего бита MAC адреса приемника. В результате вычислений определяется, какой порт будет передавать трафик. Если один порт в Port channel неисправен, трафик будет перераспределяться на

другие порты посредством алгоритма распределения. Данный алгоритм поддерживается аппаратно.

Коммутатор предлагает два метода конфигурации объединения портов: ручное создание Port channel и динамическое посредством протокола контроля объединения соединений (Link Aggregation Control Protocol – LACP). Объединение возможно только для портов, работающих в режиме полного дуплекса.

Для правильной работы Port channel необходимо соблюдать следующие условия:

- ❖ Все порты работают в режиме полного дуплекса;
- ❖ Все порты имеют одинаковую скорость;
- ❖ Все порты являются портами доступа и принадлежат одному VLAN, или все они являются транковыми портами или они все гибридные порты.
- ❖ Если все порты являются транковыми или гибридными, тогда сконфигурированные на них допустимые VLAN и основной VLAN должны быть у всех одинаковыми.

Если Port channel сконфигурирован на коммутаторе вручную иди динамически, система автоматически назначает порт с наименьшим номером мастер-портом Port channel'a. Если на коммутаторе активирован протокол spanning tree, протокол построения дерева воспринимает Port channel как логический порт и посылает BPDU пакеты через мастер-порт.

Объединение портов жестко связано с аппаратной частью коммутатора. Коммутатор позволяет агрегировать соединения между любыми двумя коммутаторами. Максимально возможно создать 128 групп по 8 портов к каждой.

После того, как порты агрегированы, их можно использовать, как обычный порт. Коммутатор имеет встроенный режим конфигурирования интерфейса агрегации, пользователь может создавать соответствующую конфигурацию в этом режиме точно также, как при конфигурировании VLAN или физического интерфейса.

8.2 Общие сведения о LACP

LACP – протокол, базирующийся на стандарте IEEE 802.3ad, и реализующий механизм динамического объединения каналов. Протокол LACP использует пакеты LACPDU (Link Aggregation Control Protocol Data Unit) для обмена информацией с ответными портами.

После того, как протокол LACP включен на порту, данный порт посылает пакеты LACPDU на ответный порт соединения, уведомляя о приоритете системы, MAC адресе системы, приоритете порта, идентификаторе порта и ключе операции. Когда ответный порт получает эту информацию, она сравнивается с информацией о других портах, которые могут быть объединены. Соответственно, обе стороны соединения могут достичь соглашения о включении или исключении порта из динамической объединенной группы.

Ключ операции создается протоколом в соответствии с комбинацией параметров конфигурации (скорость, дуплекс, базовая конфигурация, ключ управления) портов, которые будут объединяться.

После включения протокола динамического объединения портов (LACP), ключ управления по умолчанию равен 0. После статического объединения портов посредством LACP, ключ управления порта такой же, как ID объединенной группы.

При динамическом объединении портов все члены одной группы имеют одинаковый ключ операции. При статическом объединении только активные порты имеют одинаковый ключ операции.

8.2.1 Статическое объединение LACP

Статическое объединение выполняется путем конфигурирования пользователем и не требует протокола LACP. При конфигурировании статического LACP объединения, используется режим «on» для включения порта в группу агрегации.

8.2.2 Динамическое объединение LACP

1. Общие положения динамического объединения LACP

Динамическое объединение — это объединение, создаваемое/удаляемое системой автоматически. Оно не позволяет пользователям самостоятельно добавлять или удалять порты из динамического объединения LACP. Порты, которые имеют одинаковые параметры скорости и дуплекса, подключенные к одним и тем же устройствам, имеющие одинаковую конфигурацию могут быть динамически объединены в группу. В случае, если только один порт может создавать динамическое объединение, это называется однопортовым объединением. При динамическом объединении LACP протокол на порту должен быть включен.

2. Режимы портов в динамической группе объединения

В динамической группе объединения порты имеют два статуса — выбранный (selected) или «в ожидании» (standby). Оба типа портов могут посылать и принимать пакеты протокола LACP, но порты в статусе «ожидания» не могут пересылать данные.

Поскольку существует ограничение на максимальное количество портов в группе агрегации, если текущий номер порта превышает предел в группе, тогда устройство на одном конце соединения договаривается с устройством на другом конце для определения статуса порта в соответствии с идентификатором порта.

Этапы согласования, следующие:

Сравнение идентификаторов (ID) устройств (приоритет системы и MAC адрес системы). Сначала сравниваются приоритеты систем. Если они одинаковые, тогда сравниваются MAC адреса устройств. Устройство с меньшим идентификатором имеет высший приоритет.

Затем идет сравнение идентификаторов портов (приоритет порта и идентификатор порта). Для каждого порта на стороне устройства с наивысшим приоритетом системы сначала сравниваются приоритеты портов. Если приоритеты одинаковые, тогда сравниваются идентификаторы портов. Порт с наименьшим идентификатором порта становится выбранным (selected), а остальные становятся в режим «ожидание» (standby).

В группе объединения порт с наименьшим идентификатором и статусом «выбранный» становится мастер-портом. Другие порты со статусом «выбранный» становятся участниками группы.

8.3 Настройка Port channel

1. Создание группы портов в режиме глобального конфигурирования;
2. Добавление портов в определенную группу из режима конфигурирования порта;
3. Вход в режим конфигурирования port-channel;

4. Задание метода балансировки для группы портов
5. Задание приоритета системы в LACP протоколе
6. Задание приоритета для конкретного порта в LACP протоколе
7. Задание режима таймаута на порту в LACP протоколе

1. Создание группы портов

Команда	Описание
Режим глобального конфигурирования	
port-group <port-group-number> **no port-group <port-group-number>**	Создание или удаление группы портов.

2. Добавление портов в определенную группу

Команда	Описание
Режим конфигурирования порта	
port-group *<port-group-number>* mode {active | passive | on} **no port-group**	Добавляет порты в группу и устанавливает их режим.

3. Вход в режим конфигурирования port-channel

Команда	Описание
Режим глобального конфигурирования	
interface port-channel *<port-channel-number>*	Вход в режим конфигурирования port-channel.

4. Задание метода балансировки для устройства

Команда	Описание
Режим глобального конфигурирования	
load-balance {dst-src-mac | dst-src-ip | dst-src-mac-ip}	Задание метода балансировки для устройства, изменения начинают действовать на группе портов и ECMP функции сразу.

5. Задание приоритета системы в LACP протоколе

Команда	Описание
Режим глобального конфигурирования	
lacp system-priority <*system-priority*> **no lacp system-priority**	Задание приоритета системы в LACP протоколе, команда no возвращает значение по умолчанию.

6. Задание приоритета для конкретного порта в LACP протоколе

Команда	Описание
Режим конфигурирования порта	
lacp port-priority <*port-priority*> **no lacp port-priority**	Задание приоритета для конкретного порта в LACP протоколе. команда no возвращает значение по умолчанию.

7. Задание режима таймаута на порту в LACP протоколе

Команда	Описание
Режим конфигурирования порта	
lacp timeout {short | long} **no lacp timeout**	Задание режима таймаута на порту в LACP протоколе. команда no возвращает значение по умолчанию.

8.4 Примеры использования Port channel

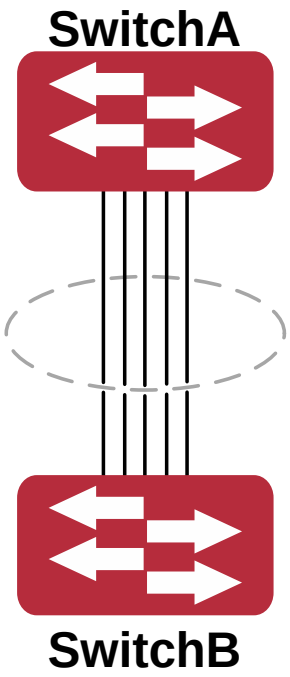
Вариант 1 Настройка Port channel для протокола LACP.

Имеется два коммутатора SWITCHA и SWITCHB. Порты 1,2,3,4 на коммутаторе SWITCHA - порты доступа и добавлены в группу1 в активном режиме. Порты 6,8,9,10 на коммутаторе SWITCHB – тоже порты доступа и добавлены в группу 2 в пассивном режиме. Все порты соединены кабелями.

Этапы конфигурации показаны ниже:

```
Switch1#config
Switch1(config)#interface ethernet 1/0/1-4
Switch1(Config-If-Port-Range)#port-group 1 mode active
Switch1(Config-If-Port-Range)#exit
Switch1(config)#interface port-channel 1
Switch1(Config-If-Port-Channel1)#
```

```
Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/0/6
Switch2(Config-If-Ethernet1/0/6)#port-group 2 mode passive
Switch2(Config-If-Ethernet1/0/6)#exit
Switch2(config)#interface ethernet 1/0/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode passive
Switch2(Config-If-Port-Range)#exit
Switch2(config)#interface port-channel 2
Switch2(Config-If-Port-Channel2)#
```



Конфигурация Port-Channel

Результат конфигурации:

Коммутатор сообщит, что агрегирование прошло успешно. Порты 1,2,3,4 коммутатора SwitchA входят в группу Port-Channel1, а порты 6,8,9,10 коммутатора SwitchB входят в группу Port-Channel2.

Вариант 2 Конфигурация Port channel в режиме ON.

Как показано на рисунке, порты 1,2,3,4 коммутатора SwitchA – порты доступа и будут добавлены в группу1 с режимом ON. Порты 6,8,9,10 коммутатора SwitchB – тоже порты доступа и будут добавлены в группу2 с режимом ON.

Этапы конфигурации показаны ниже:

```
Switch1#config
Switch1(config)#interface ethernet 1/0/1
Switch1(Config-If-Ethernet1/0/1)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/1)#exit
```

```
Switch1(config)#interface ethernet 1/0/2
Switch1(Config-If-Ethernet1/0/2)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/2)#exit
Switch1(config)#interface ethernet 1/0/3
Switch1(Config-If-Ethernet1/0/3)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/3)#exit
Switch1(config)#interface ethernet 1/0/4
Switch1(Config-If-Ethernet1/0/4)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/4)#exit

Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/0/6
Switch2(Config-If-Ethernet1/0/6)#port-group 2 mode on
Switch2(Config-If-Ethernet1/0/6)#exit
Switch2(config)#interface ethernet 1/0/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode on
Switch2(Config-If-Port-Range)#exit
```

Результат конфигурации:

Порты 1,2,3,4 на коммутаторе SwitchA добавлены по порядку в группу портов 1 в режиме ON. Коммутатору на удаленном конце не требуется обмен пакетами LACP для завершения объединения. Агрегация завершается сразу, когда выполняется команда добавления порта 2 в группу 1. Порты 1 и 2 объединяются в port channel 1. Когда порт 3 вступает в группу 1, port channel 1 из портов 1 и 2 разбирается и пересобирается с портом 3 опять в port channel 1. Когда порт 4 вступает в группу 1, port channel 1 из портов 1, 2 и 3 разбирается и пересобирается с портом 4 опять в port channel 1 (надо отметить, что каждый раз, когда новый порт вступает в группу объединения портов, группа разбирается и собирается заново). Теперь все 4 порта на обоих коммутаторах объединены в режиме «ON».

8.5 Устранение неисправностей Port channel

Если во время конфигурации объединения портов возникли проблемы, в первую очередь проверьте следующее:

- ❖ Убедитесь, что все порты в группе имеют одинаковые настройки, например, они все в режиме полного дуплекса, имеют одинаковую скорость и настройки VLAN. Если обнаружены несоответствия, исправьте это.
- ❖ Некоторые команды не могут быть использованы на портах в port channel. Такие как arp, bandwigth, ip, ip-forward и т.д.

9 КОНФИГУРИРОВАНИЕ MTU

9.1 Общие сведения об MTU

В настоящий момент Jumbo фрейм не имеет определяющего стандарта в сетевых технологиях (в частности, не были стандартизированы формат пакета и длина). Обычно пакет имеющий размер от 1519 до 9000 называется JUMBO фрейм. При использовании таких пакетов, скорость передачи данных в сети увеличивается на 2%-5%. Технически JUMBO – это удлиненный фрейм, посылаемый и принимаемый коммутатором. Однако, учитывая длину, такие фреймы не могут быть посланы на процессор устройства. Мы исключаем посылку больших фреймов процессору во время приема пакетов.

9.2 Конфигурирование MTU

1. Включение функции MTU

Команда	Описание
Общий режим	
mtu [<mtu-value>] **no mtu enable**	Включает функцию приема/посылки JUMBO фреймов. Команда NO выключает функцию приема/посылки JUMBO фреймов.

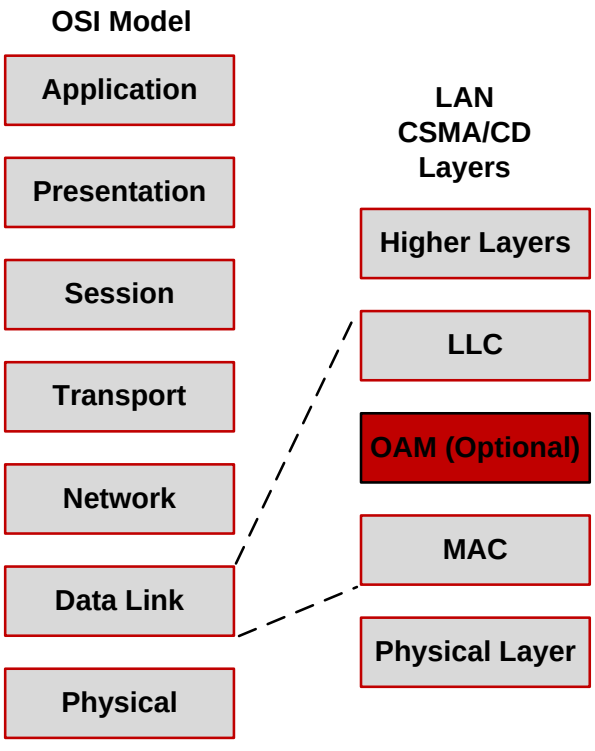
10 КОНФИГУРАЦИЯ EFM OAM

10.1 Общие сведения о EFM OAM

Первоначально технология Ethernet разрабатывалась для локальных сетей, но длина каналов и размеры сетей стремительно увеличивались, и теперь эта технология применяется так же и на Metro и на глобальных сетях. Из-за отсутствия эффективного механизма управления, что влияло на работу тенологии Ethernet в Метро и глобальных сетях, стало жизненно необходимым применение OAM на Ethernet.

Существует четыре стандарта протоколов для Ethernet OAM: 802.3ah (EFM OAM), 802.3ag (CFM), E-LMI и Y.1731. EFM OAM и CFM определены международным комитетом по стандартам (IEEE). EFM OAM работает на канальном уровне для корректного обнаружения и управления каналом данных. Использование EFM OAM позволяет повысить управляемость и упростить обслуживание Ethernet уровня для повышения устойчивости работы сети. CFM используется для мониторинга общей сетевой связности и локализации проблем на сетевом уровне. По сравнению с CFM стандарт Y.1731, принятый международным телекоммуникационным союзом (ITU), более мощный. Стандарт E-LMI, принятый MEF, применяется только к UNI (User Network Interface). Так как вышеуказанные протоколы могут использоваться для различных сетевых топологий и управления, между ними существуют дополнительные соглашения.

EFM OAM (Ethernet in the First Mile Operation, Administration and Maintenance – использование, администрирование и управление Ethernet на первой миле (имеется в виду от клиента) работает на канальном уровне сетевой модели OSI, реализуя дополнительные функции через подуровень OAM, как показано на рисунке ниже:



Положение OAM в OSI модели сети

Пакеты данных OAM (OAMPDU) используют в качестве MAC адреса назначения 01-80-c2-00-00-02 по протоколу. Скорость передачи не выше 10 пакетов в секунду.

EFM OAM устанавливается на базе OAM соединения. Эта функция обеспечивает механизмы управления каналами, такие, как мониторинг каналов, удаленное обнаружение проблем и удаленное тестирование портов. Говоря проще, основные понятия EFM OAM следующие:

1. Установление соединения ethernet OAM

Модуль Ethernet OAM ищет удаленные OAM модули и устанавливает с ними сессии путем обмена пакетами OAMPDU. EFM OAM может работать в двух режимах: активном и пассивном. Сессия устанавливается только OAM модулем, работающим в активном режиме, а модуль, работающий в пассивном режиме, вынужден ждать, пока не получит запрос на соединение. После того как Ethernet OAM соединение установлено, модули OAM с обоих концов канала постоянно обмениваются пакетами OAMPDU для поддержания соединения. Если модуль Ethernet OAM не получает пакетов OAMPDU в течении 5 секунд, Ethernet OAM соединение разрывается.

2. Мониторинг канала

Определение неисправности в среде Ethernet затруднено, особенно когда физическое соединение не разрывается, но работоспособность сети нарушена. Мониторинг канала используется для определения и исследования неисправностей каналов в различных средах. EFM OAM обеспечивает мониторинг канала посредством обмена уведомлениями о событиях OAMPDUs. При определении неисправности канала, локальный модуль OAM посылает уведомление OAMPDU об этом событии удаленному модулю. В то же время он записывает это событие в логи и посылает SNMP Trap системе управления сетью. Когда удаленный модуль получает уведомление о проблеме, он так же записывает информацию в логи и сообщает системе управления. Анализируя информацию в логах, сетевой администратор может отследить состояние канала в определенный период времени.

Мониторинг канала средствами EFM OAM отслеживает следующие аварийные события — Errored symbol period event, Errored frame event, Errored frame period event и Errored frame seconds event.

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-прием ошибочного фрейма определяется по контрольной сумме).

Errored frame period event: количество определенных ошибочных фреймов за M секунд не должно быть меньше нижнего порога ошибок.

Время принятия ошибочных фреймов: количество секунд приема ошибочных фреймов зафиксированных за M секунд не может быть ниже порога ошибок (количество

секунд ошибочных фреймов — когда в течении секунды принимаются ошибочные фреймы).

3. Удаленное определение неисправностей

Когда в сети прерывается передача данных из-за сбоя устройства или его недоступности, Ethernet OAM модуль устанавливает соответствующий флаг в OAMPDU пакетах, сообщая информацию о проблеме удаленному концу. Так как модули обмениваются пакетами OAMPDU постоянно при установившемся соединении, Ethernet OAM модуль может информировать ответные модули о неисправности канала через пакет OAMPDU. Поэтому системный администратор может проследить состояние канала по логам и вовремя устранять неисправности.

Существует три типа проблем на канале, которые отмечаются в пакетах OAMPDU. Это Critical, Dying Gasp и Link Fault. Их определение зависит от реализации различными производителями. В данном оборудовании определение следующее:

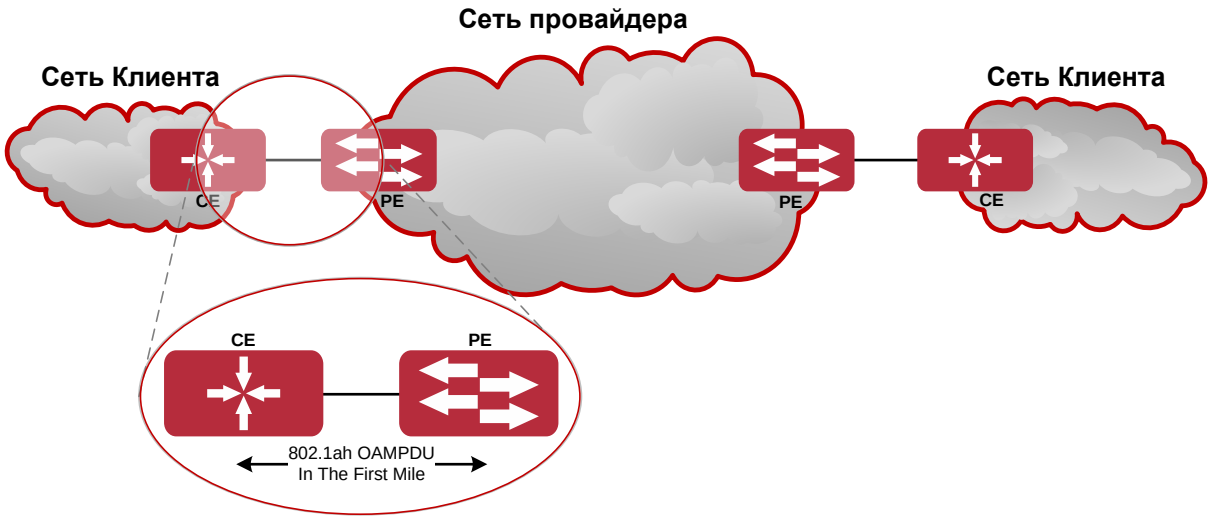
Critical event: неопределенное критическое событие

Link Fault: на приемнике локального интерфейса виден сбой

Dying Gasp: непоправимое событие (в случае перезагрузки, отключения линка, удаления конфигурации)

4. Удаленное тестирование петель соединения.

Если режим удаленной петли (loopback) включен, работающий в активном режиме OAM модуль посылает запрос удаленной петли 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 проблему. Замечание: нормальная работа канала в режиме удаленного тестирования невозможна.



Типовое применение OAM топологии

Типовое применение EFM OAM происходит в следующих топологиях: точка-точка и эмулированных IEEE802.3 соединений типа точка-точка. Устройства получают возможность контролировать канальные ошибки на Первой миле доступа через Ethernet

посредством EFM OAM. Для пользователя соединение между ним и сетью является «первой милей». Для провайдера оно является «последней милей».

10.2 Конфигурирование EFM OAM

1. Включение EFM OAM на порту;
2. Конфигурирование мониторинга соединения;
3. Конфигурирование обнаружения удаленных неисправностей;

Примечание: для этого нужно сперва включить OAM при глобально.

1. Включение EFM OAM на порту

Команда	Описание
Режим конфигурирования порта	
ethernet-oam mode {active | passive}	Конфигурация режима работы EFM OAM. По умолчанию режим - активный.
ethernet-oam **no ethernet-oam**	Включение EFM OAM на порту. Команда NO выключает EFM OAM на порту.
ethernet-oam period <seconds> **no ethernet-oam period**	Конфигурация интервала передачи пакетов OAMPDU. Команда NO возвращает значение по умолчанию
ethernet-oam timeout <seconds> **no ethernet-oam timeout**	Конфигурация таймаута для EFM OAM соединения. Команда NO возвращает значение по умолчанию

2. Конфигурирование мониторинга соединения

Команда	Описание
Режим конфигурирования порта	
ethernet-oam link-monitor **no ethernet-oam link-monitor**	Включение мониторинга соединения EFM OAM, Команда NO выключает мониторинг.
ethernet-oam errored-symbol-period {threshold low <low-symbols> | window <seconds>} **no ethernet-oam errored-symbol-period {threshold low | window}**	Конфигурирование нижнего порога ошибок и окна фиксации ошибочных символов. Команда NO возвращает значение по умолчанию.
ethernet-oam errored-frame-period {threshold low <low-frames> | window <seconds>}	Конфигурирование нижнего порога ошибок и окна фиксации периода

no ethernet-oam errored-frame-period {threshold low | window}	ошибочных фреймов. Команда NO возвращает значение по умолчанию.
ethernet-oam errored-frame {threshold low <low-frames> | window <seconds>} **no ethernet-oam errored-frame {threshold low | window}**	Конфигурирование нижнего порога ошибок и окна фиксации ошибочных фреймов. Команда NO возвращает значение по умолчанию.
ethernet-oam errored-frame-seconds {threshold low <low-frame-seconds> | window <seconds>} **no ethernet-oam errored-frame-seconds {threshold low | window}**	Конфигурирование нижнего порога ошибок и окна фиксации секунд ошибочных фреймов. Команда NO возвращает значение по умолчанию.

3. Конфигурирование обнаружения удаленных неисправностей

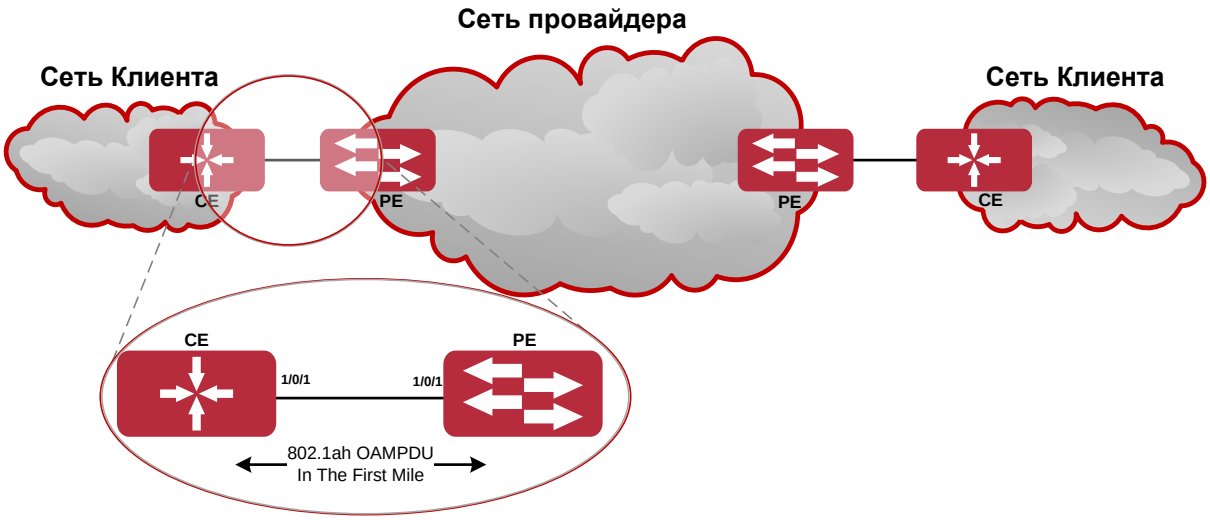
Команда	Описание
Режим конфигурирования порта	
ethernet-oam remote-failure **no ethernet-oam remote-failure**	Включает режим удаленной диагностики EFM OAM (под неисправностью понимается критическое событие или неисправность соединения на ближнем конце), Команда NO отключает функцию
ethernet-oam errored-symbol-period threshold high {high-symbols | none} **no ethernet-oam errored-symbol-period threshold high**	Конфигурирование верхнего предела ошибок приема символов. Команда NO восстанавливает значение по умолчанию.
ethernet-oam errored-frame-period threshold high {high-frames | none} **no ethernet-oam errored-frame-period threshold high**	Конфигурирование верхнего предела ошибок приема ошибочных фреймов за период. Команда NO восстанавливает значение по умолчанию.
ethernet-oam errored-frame threshold high {high-frames | none} **no ethernet-oam errored-frame threshold high**	Конфигурирование верхнего предела ошибок приема фреймов. Команда NO восстанавливает значение по умолчанию.
ethernet-oam errored-frame-seconds threshold high {high-frame-seconds | none}	Конфигурирование верхнего предела ошибочных секунд приема фреймов. Команда NO

no ethernet-oam errored-frame-seconds threshold high	восстанавливает значение по умолчанию.

10.3 Примеры EFM OAM

Сценарий 1:

Клиентское и сетевое устройства, соединенные напрямую, имеют включенную функцию EFM OAM для мониторинга состояния линии. Информация о линии передается в систему управления сетью при возникновении аварийных событий. Так же используется функция тестирования петель для проверки линии по необходимости.



Типовая топология применения OAM

Процедура конфигурации: (опуская конфигурацию SNMP и логгирования)

Конфигурация клиентского устройства (CE):

```
CE(config)#interface ethernet 1/0/1
CE (config-if-ethernet1/0/1)#ethernet-oam mode passive
CE (config-if-ethernet1/0/1)#ethernet-oam
CE (config-if-ethernet1/0/1)#ethernet-oam remote-loopback supported
```

Другие параметры используются по умолчанию.

Конфигурация на PE:

```
PE(config)#interface ethernet 1/0/1
PE (config-if-ethernet1/0/1)#ethernet-oam
```

Другие параметры используются по умолчанию.

При необходимости использования удаленной петли используется следующая команда.

```
PE(config-if-ethernet1/0/1)#ethernet-oam remote-loopback
```

Выполнение следующей команды вызывает прекращение режима удаленной петли после завершении тестирования.

```
PE(config-if-ethernet1/0/1)# no ethernet-oam remote-loopback
```

Выполнение следующей команды отключает поддержку удаленной петли.

```
CE(config-if-ethernet1/0/1)#no ethernet-oam remote-loopback supported
```

10.4 Устранение неисправностей EFM OAM

Если при использовании EFM OAM возникают проблемы, проверьте, не являются ли они следствием следующих причин:

- ❖ Проверьте, не находятся ли оба OAM модуля соединения в пассивном режиме. Если так, то EFM OAM соединение не будет установлено между OAM модулями.
- ❖ Убедитесь, что SNMP сконфигурирован корректно. В противном случае аварийные сообщения не будут отправляться в систему управления сетью.
- ❖ Соединение в режиме OAM петли не работает. Необходимо выключить режим тестирования после проверки состояния линии.
- ❖ Убедитесь, что оба устройства поддерживают режим удаленной петли
- ❖ На порту не должны быть сконфигурированы STP, MRPP, ULPP, управление потоком и функция определения удаленной петли при включении функции удаленной петли OAM, поскольку эти функции не могут использоваться одновременно.

11 БЕЗОПАСНОСТЬ ПОРТОВ

11.1 Введение

Безопасность порта — это механизм, основывающийся на MAC-адресе для управления доступом к сети. Это расширение существующих аутентификаций 802.1x и MAC. Он контролирует доступ неавторизированных устройств сети, проверяя MAC-адрес источника полученного кадра и доступ к неавторизированным устройствам, проверяя MAC-адрес устройства назначения в кадре. С безопасностью портов, пользователь может настраивать различные режимы безопасности порта для того, чтобы устройство обучалось только легальным MAC-адресам источника. После включения безопасности портов устройство обнаруживает нелегальный фрейм, что вызывает соответствующую функцию безопасности порта и выполняет предопределенные действия автоматически. Это снижает нагрузку пользовательского обслуживания и значительно повышает безопасность системы.

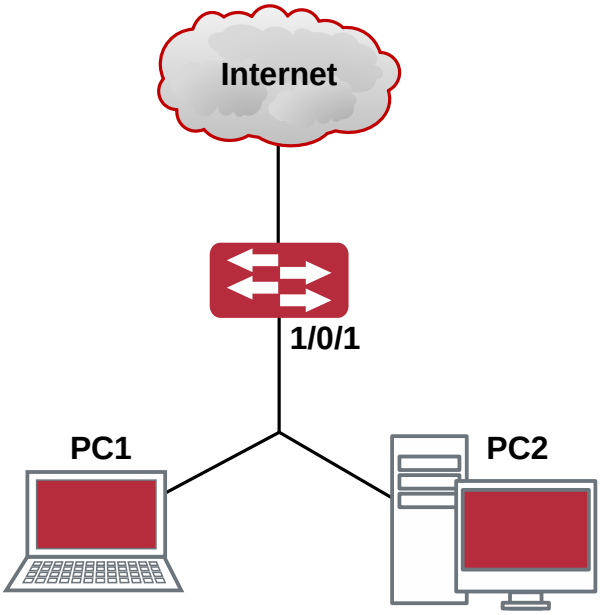
11.2 Настройка безопасности портов

1. Базовые настройки безопасности портов

Команда	Описание
Режим конфигурирования порта	
switchport port-security **no switchport port-security**	Настройка безопасности портов на интерфейсе.
switchport port-security mac-address <*mac-address*> [vlan <*vlan-id*>] **no switchport port-security mac-address <*mac-address*> [vlan <*vlan-id*>]**	Насройка статического безопасного MAC-адреса на интерфейсе
switchport port-security maximum <*value*> [vlan <*vlan-list*>] **no switchport port-security maximum <*value*> [vlan <*vlan-list*>]**	Настройка максимального числа безопасных MAC-адресов, разрешенных на интерфейсе
switchport port-security violation {protect | restrict | shutdown} **no switchport port-security violation**	Когда превышено максимальное число настроенных MAC-адресов, MAC-адрес доступа к интерфейсу не принадлежит этому интерфейсу в таблице MAC-адресов или MAC-адрес настроен на несколько интерфейсов в одном VLAN, они оба будут нарушать безопасность MAC-адресов.
switchport port-security aging {static | time <*value*> | type {absolute | inactivity}}	Включает время или тип старения port-security на интерфейсе.

no switchport port-security violation aging {static | time | type}	
Режим администратора	
clear port-security {all | configured | dynamic | sticky} [[address <*mac-addr*> | interface <*interface-id*>] [vlan <*vlan-id*>]]	Стирает введенные безопасные MAC-адреса на интерфейсе.
show port-security [interface <*interface-id*>] [address | vlan]	Показывает конфигурацию.

11.3 Приметы настройки PORT SECURITY



Типичная схема топологии для безопасности порта.

На интерфейсе включена функция безопасности порта, настроено максимальное число разрешенных источников MAC-адресов на интерфейсе равное 10, и интерфейс разрешает доступ 10 пользователям в интернет. Если превышено максимальное количество, то новый пользователь не получит доступ в интернет, так что это не только отграничит число пользователей, но и сделает доступ в интернет безопасным. Если сделать настройку максимального числа безопасных MAC-адресов равной 1, то только PC1 или PC2 получат доступ в сеть.

Процесс настройки:

```
#Configure the switch.
Switch(config)#interface Ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport port-security
Switch(config-if- ethernet1/0/1)#switchport port-security maximum 10
Switch(config-if- ethernet1/0/1)#exit
Switch(config)#
```

11.4 Устранение неисправностей PORT SECURITY

Если возникают проблемы с настройкой безопасности, проверьте не являются ли они следствием следущих причин:

- ❖ Проверьте включен ли PORT SECURITY
- ❖ Убедитесь в настройке максимального количества MAC-адресов

12 НАСТРОЙКА DDM

12.1 Введение

12.1.1 Краткое введение в DDM

DDM (Digital Diagnostic Monitor) реализует функцию подробной цифровой диагностики по стандарту SFF-8472 MSA. DDM контролирует параметры сигнала и оцифровывает его на печатной плате внутреннего модуля. После этого предоставляет разграниченный результат и параметры, которые сохраняются в стандартных рамках памяти таким образом, чтобы целесообразно было читать последовательный интерфейс с двойного кабеля.

Обычно интеллектуальные цифровые модули поддерживают функцию цифровой диагностики. Единицы сетевого управления имеют возможность контролировать параметры (температура, напряжение, ток смещения, tx мощность и rx мощность) оптических модулей для получения их пороговых значений в режиме реального времени на текущем оптическом модуле. Это помогает единицам сетевого управления обнаруживать неисправности в оптической линии, сократить эксплуатационную нагрузку и повысить надежность системы.

Применение DDM показано далее:

1. Прогноз продолжительности жизни модуля.

Контролирование токов утечки позволяет сделать прогноз времени жизни лазера. Администратор может найти несколько потенциальных проблем по мониторингу напряжения и температуры модуля.

(1) Высокое напряжение Vcc приведет к поломке CMOS, низкое – к неправильной работе

(2) Высокая rx мощность приведёт к повреждению принимающего модуля, из-за низкой rx мощности модуль не сможет нормально работать.

(3) Высокая температура приведет к быстрому старению аппаратных средств.

(4) Контроль мощности, получаемой по волокну, помогает проверить возможности линии и удаленного коммутатора

2. Определение места повреждения.

В оптоволоконной линии определение неисправности имеет важное значение для быстрой перезагрузки сервиса, изолирование неисправности помогает администратору быстро найти местоположение неисправности в модуле (локальный или удаленный модули) или на линии, что также сокращает время восстановления системы после неисправности.

Анализируя статусы оповещения и сигнализации в режиме реального времени по параметрам (температура, напряжение, ток смещения, tx мощность и rx мощность) можно быстро обнаружить неисправность с помощью функции цифровой диагностики.

Кроме того, состояние Tx Fault и Rx LOS имеет важное значение для анализа неисправности.

3. Проверка совместимости.

Проверка совместимости используется для анализа, является ли окружающая среда модуля согласованной вручную или совместима с соответствующим стандартом, поскольку возможности модуля могут быть реализованы только с совместимой окружающей средой.

Иногда параметры окружающей среды превышают установленные вручную или стандарт соответствия, что приведет к уменьшению возможностей модуля и ошибке передачи.

Окружающая среда не совместима:

(1) Напряжение превышает установленный диапазон.

(2) Rx power приводит к перезагрузке или к меньшей чувствительности приемопередатчика.

(3) Температура превышает диапазон рабочей температуры.

12.1.2 Функции DDM

Описание DDM показано в следующем примере:

1. Просмотр информации мониторинга на приемопередатчике.

Администратор может узнать текущее состояние трансивера и найти потенциальные проблемы с помощью проверки следующих параметров (входящая TX мощность, RX мощность, температура, напряжение, токи утечки) и запросить информацию мониторинга (такую как оповещения, сигнализация, состояние в реальном масштабе времени и т.д.). Кроме того, проверка информации о неисправностях оптических модулей помогает администратору быстро обнаружить неисправную линию и сократить время восстановления.

2. Определение значения порога пользователем.

Для параметров в реальном масштабе времени (TX мощности, RX мощности, температуры, напряжения, токов утечки) есть фиксированные значения порогов. Потому, что пользовательское окружение различно, пользователь может определить значение порога (входящая сигнализация с высоким и низким приоритетом, оповещение с высоким и низким приоритетом), гибко контролировать рабочее состояние трансивера и немедленно обнаружить неисправность.

Настройка значения порогов производится пользователем и производителем и может быть показана в то же время. Когда порог определяется пользователем нерационально, он будет запрошен у пользователя и сигнал тревоги или оповещения автоматически установит порог по умолчанию (пользователь может восстановить все пороговые значения по умолчанию).

Рациональное пороговое значение: высокое/низкое значение сигнала оповещения должно быть между высоким и низким сигналом сигнализации и высокое значение порога должно быть выше, чем низкое и, а именно, высокое значение сигнализации >= высокое значение оповещения >= низкое значение оповещения >= низкое значение сигнализации.

Для оптического модуля режим проверки получаемого питания включает внутреннюю и внешнюю проверку, которые определили производители. Кроме того, режим проверки параметров в реальном масштабе времени и пороговых значений по умолчанию.

3. Контроль трансивера.

Кроме проверки состояния работы трансивера в реальном масштабе времени, пользователю нужно следить за подробной информацией о состоянии, такой как последнее время неисправности и ее тип. Контроль трансивера помогает пользователю найти последнее состояние неисправности через проверку логов и запросить последнее состояние неполадки через выполнение команд. Когда пользователь находит информацию о неполадке оптического модуля, то информация об оптическом модуле может быть перепроверена после обработки информации о неисправности, здесь пользователь может знать информацию о неисправности и возобновить мониторинг.

12.2 Список команд конфигурации DDM

Настройка DDM:

1. Просмотр информации контроля в реальном масштабе времени.
2. Настройка значений порога сигнализации или оповещения каждого параметра для трансивера.
3. Настройка состояния мониторинга трансивера.

(1) Настройка интервала мониторинга трансивера.
(2) Настройка состояния включения мониторинга трансивера.
(3) Просмотр информации мониторинга трансивера.
(4) Очистка информации мониторинга трансивера.

1. Просмотр информации контроля в реальном масштабе времени.

Команда	Описание
Режим конфигурирования порта, режим администратора или глобальный режим	
show transceiver [interface ethernet <interface-list>] [detail]	Просмотр мониторинга состояния трансивера.

2. Настройка значений порога сигнализации или оповещения каждого параметра для трансивера.

Команда	Описание
Режим конфигурирования порта	
transceiver threshold {default | {temperature | voltage | bias | rx-power | tx-power} {high-alarm | low-alarm | high-warn | low-warn} {<value> | default}}	Установка определенного порога пользователем.

3. Настройка состояния мониторинга трансивера.

(1) Настройка интервала мониторинга трансивера.

Команда	Описание
Режим конфигурирования порта	
transceiver-monitoring interval <minutes> **no transceiver-monitoring interval**	Установка интервала мониторинга трансивера. Команда no устанавливает интервал по умолчанию, равный 15 минут.

(2) Настройка состояния включения мониторинга трансивера.

Команда	Описание
Режим конфигурирования порта	
transceiver-monitoring {enable | disable}	Устанавливает, включен ли мониторинг трансивера. После включения на порте мониторинга трансивера, система записывает состоние неисправности. После отключения функции на порте, информация о неисправности будет стерта.

(3) Просмотр информации мониторинга трансивера.

Команда	Описание
Режим конфигурирования порта	
show transceiver threshold-violation [interface ethernet <interface-list>]	Показывает иформацию мониторинга трансивера, включающую последнюю информацию нарушения порогового значения, мониторинг протекающего тока через трансивер, включен ли мониторинг трансивера на порте.

(4) Очистка информации мониторинга трансивера.

Команда	Описание
Режим конфигурирования порта	
clear transceiver threshold-violation [interface ethernet <interface-list>]	Стирает значение порога нарушения мониторинга трансивера.

12.3 Примеры применения DDM

Пример 1:

В интерфейсы Ethernet 1/0/21 и Ethernet 1/0/23 включены оптические модули с DDM, в интерфейс Ethernet 1/0/24 включен оптический модуль без DDM, в Ethernet 1/0/22 не включен какой-либо оптический модуль. Просмотр информации о DDM для описанного сценария представлен ниже.

a) Просмотр информации о всех интерфейсах, которые могут читать параметры в режиме реального времени (при отсутствии оптического модуля или оптический модуль не поддерживается, информация не будет показана), для примера:

```
Switch #show transceiver
Interface   Temp(C)     Voltage(V)  Bias(mA)    RX Power(dBM)     TX Power(dBM)
---------   --------    ----------  --------    -------------     -------------
1/0/21         28          3.28       23.34         -3.75             -0.79
1/0/23         46          3.28       26.00         -2.10             -2.21
```

b) Просмотр информации об указанном интерфейсе (N/A означает, что оптический модуль не вставлен или не поддерживается), для примера:

```
Switch #show transceiver interface ethernet 1/0/21-22;23
Interface   Temp(C)     Voltage(V)  Bias(mA)    RX Power(dBM)     TX Power(dBM)
---------   --------    ----------  --------    -------------     -------------
1/0/21         28          3.28       23.34         -3.75             -0.79
1/0/22         N/A          N/A         N/A           N/A               N/A
1/0/23         46          3.28       26.00         -2.10             -2.21
```

c) Просмотр подробной информации, включающей основную информацию, значение параметров мониторинга в реальном масштабе времени, сигнал оповещения, сигнализацию, состояние неисправности и информацию порогового значения, для примера:

```
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, 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(°C)   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, 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
```

Пример 2:

В порт Ethernet 1/0/21 включен в оптический модуль с DDM. Настройка порогового значения на оптическом модуле после просмотра информации о DDM.

Шаг 1: Просмотр подробной информации 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 (°C)    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)      -13.0           19.00       -25.00     9.00       -25.00
```

Шаг 2: Настройка порогового значения tx-power на оптическом интерфейсе, нижнее значение порогового оповещения - 12, нижнее значение пороговой сигнализации – 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
```

Шаг 3: Просмотр подробной информации о DDM на оптическом модуле. Сигнализация использует пороговое значение, настраиваемое пользователем, пороговое значение, настроенное производителем обозначено скобками. Сигнализация с ‘A-’ как -13.01 меньше, чем -12.00.

```
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 (°C)     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 включен оптический модуль с DDM. Включение мониторинга трансивера на порте, после просмотра мониторинга на оптическом модуле.

Шаг 1: Просмотр мониторинга трансивера на опическом модуле. На Ethernet 21 and ethernet 22 не включен мониторинг трансивера, установленный интервал 30 минут.

```
Switch(config)#show transceiver threshold-violation interface ethernet 1/0/21-22
Ethernet 1/0/21 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn’t exist.

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.
```

Шаг 2: Включение мониторинга трансивера на ethernet 21.

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

Шаг 3: Просмотр мониторинга трансивера на оптическом модуле. В следующих настройках, на ethernet 21 включен мониторинг трансивера, последнее нарушение порогового значения Jan 02 11:00:50 2011, подробная информации о DDM, превышающая пороговое значение также показана:

```
Switch(config-if-ethernet1/0/21)#quit
Switch(config)#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 02 12:30:50 2011.
The last threshold-violation time is Jan 02 11:00:50 2011.
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 (°C)     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.
```

12.4 Устранние неисправностей DDM

Если возникают проблемы при настройке DDM, пожалуйста, проверьте является ли эта проблема следствием следующих причин:

- ❖ Убедитесь, что трансивер на оптическом модуле был включен на порте, иначе конфигурация DDM не пудет показана.
- ❖ Убедитесь, что конфигурация SNMP работает, иначе оповещение о событии не сможет оповестить систему сетевого управления.
- ❖ Не все коммутаторы поддерживают SFP с DDM или XFP с DDM, убедитесь в использовании коммутатора с поддержкой соответствующей функции.
- ❖ Использование команд **show transceiver** или **show transceiver detail** может занять много времени, так как коммутатор будет проверять все порты, поэтому рекомендуется запрашивать информацию о трансивере на определенный порт.
- ❖ Убедитесь, что установленный пользователем порог является действующим. При любой ошибке порогового значения трансивер будет позылать сигнализацию в соответствии со значением, установленным по умолчанию.

13 LLDP-MED

13.1 Введение в LLDP-MED

LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) основан на 802.1AB LLDP (Link Layer Discovery Protocol) of IEEE. LLDP предоставляет стандартный режим Link Layer Discovery, посылающего информацию о локальных устройствах (включающую основные возможности, управление IP-адресами, ID устройства и ID порта) такой как TLV (type/length/value) тройки в LLDPDU (Link Layer Discovery Protocol Data Unit), управляющих свзью с соседними устройствами. Полученная информация об устройстве будет храниться со стандартоной базой управления информацией (MIB). Это позволяет системе сетевого управления быстро обнаруживать и идентифицировать статус связи на линии.

В стандарте 802.1AB LLDP нет передачи и управления информацией о голосовом устройстве. Для применения и управления голосового устройства целесообразно с помощью LLDP-MED TLVs предоставлять множественную информацию, такую как PoE (Power over Ethernet), сетевую политику и локальную информацию об обслуживании нового телефона.

13.2 Конфигурация LLDP-MED

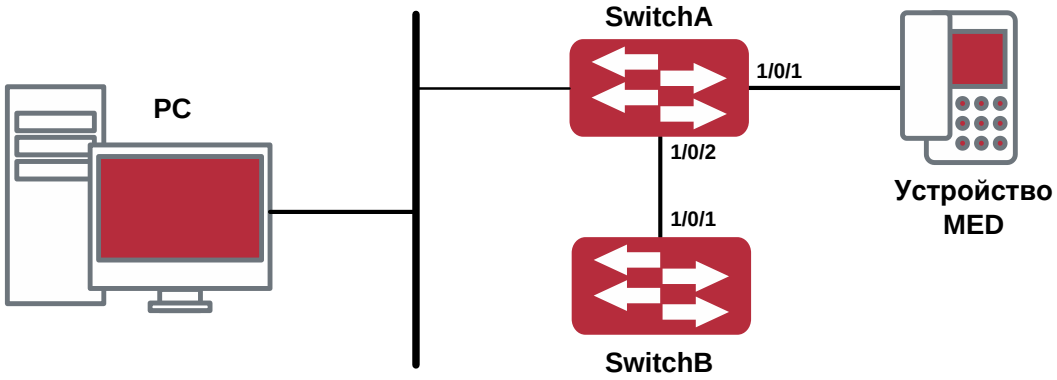
1. Базовая конфигурация

Команда	Описание
Режим конфигурирования порта	
lldp transmit med tlv all **no lldp transmit med tlv all**	Настройка указанного порта отправлять все LLDP-MED TLVs. Команда no отменяет функцию.
lldp transmit med tlv capability **no lldp transmit med tlv capability**	Настройка указанного порта отправлять LLDP-MED Capability TLV. Команда no отменяет функцию.
lldp transmit med tlv networkPolicy **no lldp transmit med tlv networkPolicy**	Настройка указанного порта отправлять LLDP-MED Network Policy TLV. Команда no отменяет данную функцию.
lldp transmit med tlv extendPoe **no lldp transmit med tlv extendPoe**	Настройка указанного порта отправлять LLDP-MED Extended Power-Via-MDI TLV. Команда no отменяет функцию.
lldp transmit med tlv inventory **no lldp transmit med tlv inventory**	Настройка указанного порта отправлятьLLDP-MED Inventory Management TLVs. Команда no отменяет функцию.

network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-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}**	Настройка сетевой политики порта, включающая VLAN ID, поддерживаемые приложения (такие как голос и видео), приоритет приложений и политика использования, и так далее.
civic location {dhcp server | switch | endpointDev} *<country-code>* **no civic location**	Настройка типа устройства и кода страны в соответствии с форматом Civic Address LCI и включение режима Civic Address LCI. Команда no отменяет все настройки в соответствии с форматом Civic Address LCI.
ecs location *<tel-number>* **no ecs location**	Настройка расположения с форматом ECS ELIN на порте. Команда no отменяет конфигурацию
lldp med trap {enable | disable}	Включение/отключение ловушки LLDP-MED на указанном порте.
Режим Civic Address LCI address	
{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}**	Настройка подробных адресов после ввода режима Civic Address LCI address на порте.
Режим глобального конфигурирования	
lldp med fast count *<value>* **no lldp med fast count**	Когда включен механизм быстрого запуска LLDP-MED, то должна производиться быстрая отправка пакетов LLDP с LLDP-MED TLV, эта команда используется для установки значения быстрой отправки пакетов, команда no восстанавливает значение по умолчанию.
Режим администратора	

show lldp	Показывает настройки глобального LLDP и LLDP-MED
show lldp [interface ethernet <*IFNAME*>]	Показывает настройки LLDP и LLDP-MED на текущем порте
show lldp neighbors [interface ethernet <*IFNAME*>]	Показывает настройки LLDP и LLDP-MED на соседних устройствах.

13.3 Пример настройки LLDP-MED



Топология базовой конфигурации LLDP-MED

1) Настройка Switch A

```
SwitchA(config)#interface ethernet1/0/1
SwitchA (Config-If-Ethernet1/0/1)# lldp enable
SwitchA (Config-If-Ethernet1/0/1)# lldp mode both (this configuration can be omitted, the default mode is RxTx)
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
SwitchA (config)#interface ethernet1/0/2
SwitchA (Config-If-Ethernet1/0/2)# lldp enable
SwitchA (Config-If-Ethernet1/0/2)# lldp mode both
```

2) Настройка Switch B

```
SwitchB (config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)# lldp enable
SwitchB (Config-If-Ethernet1/0/1)# lldp mode both
SwitchB (Config-If-Ethernet1/0/1)# lldp transmit med tlv capability
SwitchB (Config-If-Ethernet1/0/1)# lldp transmit med tlv network policy
SwitchB (Config-If-Ethernet1/0/1)# lldp transmit med tlv inventory
SwitchB (Config-If-Ethernet1/0/1)# network policy voice tag tagged vid 10 cos 4
```

3) Verify the configuration

Просмотр глобального статуса и статуса интерфейса на SwitchA

```
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
SwitchA# show lldp neighbors interface ethernet 1/0/2
Port name : interface ethernet 1/0/2
Port Remote Counter : 1
Neighbor Index: 1
Port name : Ethernet1/0/2
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :00-03-0f-00-00-02
PortIdSubtype :Local
PortId :1
PortDesc :Ethernet1/0/1
SysName :****
SysDesc :*****
SysCapSupported :4
SysCapEnabled :4
```

Пояснение:

1. Ethernet 1/0/2 коммутатора A и Ethernet 1/0/1 коммутатора B являются портами устройства сетевого соединения, они не пересылают пакеты с информацией MED TLV. Хотя Ethernet 1/0/2 коммутатора A настроен для посылки информации MED TLV, он не будет посылать информацию MED, что приведет к отсутствию в соответствующей удаленной таблице информации MED на Ethernet 1/0/2 коммутатора A.
2. Устройство LLDP-MED может посылать пакеты LLDP с MED TLV, поэтому в соответствующей удаленной таблице будет информация об Ethernet 1/0/1 коммутатора A.

13.4 Устранение неисправностей LLDP-MED

Если возникают проблемы при настройке LLDP-MED, пожалуйста, проверьте является ли эта проблема следствием следующих причин:

- ❖ Убедитесь, что LLDP включен глобально
- ❖ Только устройство сетевого соединения получает LLDP пакеты с LLDP-MED TLV от ближайшего устройства MED, он так же посылает LLDP-MED TLV. Если на устройстве сетевого соединения настроена команда для отправки LLDP-MED TLV, пакеты без LLDP-MED TLV посылаются на порт, что означает, что никакой информации порт не получает и на порте отключена функция посылки информации LLDP-MED TLV.
- ❖ Если соседние устройства посылают информацию LLDP-MED устройству сетевого соединения, но она не является информацией LLDP-MED, проверяемая командой **show lldp neighbors**, что означает, что отправляемая информация LLDP-MED к соседним устройствам является ошибочной.

14 НАСТРОЙКА BPDU-TUNNEL

14.1 Введение в bpdu-tunnel

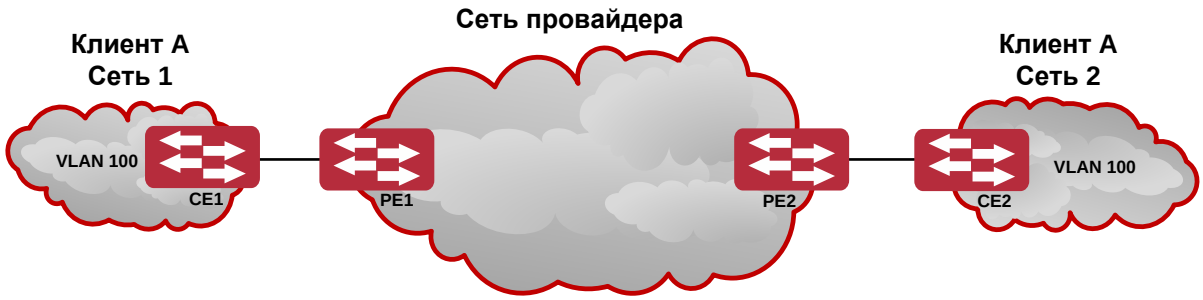
BPDU Tunnel является технологией второго уровня. Это позволяет пакетам протоколов второго уровня географически распределенных частных сетей прозрачно передаваться по специальным туннелям через сеть поставщика услуг.

14.1.1 Функции bpdu-tunnel

В приложении MAN, множественные ветви корпорации могут соединяться с друг с другом по сети оператора. VPN предоставляет возможность оператору включать географически распределенные сети в одну локальную сеть LAN, поэтому поставщику услуг нужно предоставить функцию туннелирования, а именно передачу информационных данных, поступающих от пользовательской сети, через сеть оператора. Для поддержания локальной концепции, необходима не только передача данных от пользовательских частных сетей через туннель, но также передача пакетов протоколов второго уровня от пользовательских сетей.

14.1.2 Создание bpdu-tunnel

Специальные линии используются оператором для создания пользовательских сетей второго уровня. В результате, пользовательская сеть разбивается на части по различные стороны сетевого провайдера. Как показано на рисунке, пользователь А имеет два устройства (CE1 и CE2) и оба этих устройства принадлежат к некоторому VLAN. Пользовательская сеть разделена на сеть 1 и сеть 2, которые соединяются через сеть провайдера. Когда пакеты протокола уровня 2 не могут быть реализованы через сеть поставщика услуг, то пользовательская сеть не может обработать вычисление независимого протокола второго уровня (для примера: вычисление spanning tree), таким образом сети влияют друг на друга.



Применение BPDU-туннеля

14.2 Конфигурация bpdu-tunnel

1. Настройка глобального MAC-адреса туннеля.
2. Настройка порта для поддержки туннеля.

1. Настройка глобального MAC-адреса туннеля.

Команда	Описание
Режим глобального конфигурирования	
bpdu-tunnel-protocol {dot1x | gvrp | stp | user-defined-protocol <name>} [protocol-mac <MAC address>] [encape-type { ethernetii | llc | snap}] {default-group-mac | group-mac <MAC address>} **no bpdu-tunnel-protocol {dot1x | gvrp | stp | user-defined-protocol <name>}**	Включение/отключение глобального MAC-адреса туннеля.

2. Настройка порта для поддержки туннеля.

Команда	Описание
Режим конфигурирования порта	
bpdu-tunnel-protocol {dot1x | gvrp | stp | user-defined-protocol <name>} **no bpdu-tunnel-protocol {dot1x | gvrp | stp | user-defined-protocol <name>}**	Включение/отключение на порте поддержки туннеля.

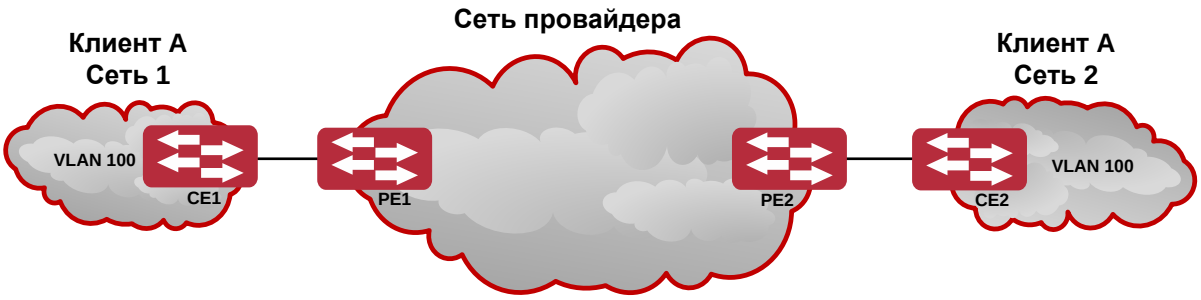
14.3 Пример bpdu-tunnel

Специальные линии используются оператором для построения пользовательских сетей второго уровня. В результате, пользовательская сеть разбивается на части по различные стороны сетевого провайдера. Как показано на рисунке, пользователь A имеет два устройства (CE1 и CE2) и оба этих устройства принадлежат к некоторому VLAN. Пользовательская сеть разделена на сеть 1 и сеть 2, которые соединяются через сеть провайдера. Когда пакеты протокола уровня 2 не могут быть реализованы через сеть поставщика услуг, то пользовательская сеть не может обработать вычисление независимого протокола второго уровня (для примера: вычисление spanning tree), таким образом сети влияют друг на друга.

Применение BPDU-туннеля

С BPDU Tunnel, пакеты протокола второго уровня от пользовательской сети могут быть переданы через сеть оператора в следующей последовательности:

1. После получения пакета протокола второго уровня от первой сети пользователя A, PE 1 в сети оператора пакет инкапсулируется, MAC-адрес назначения заменяется конкретным multicast MAC-адресом, и затем пакет пересылается в сети оператора.
2. Инкапсулированный пакет протокола второго уровня (называемый пакетом BPDU Tunnel) пересылается к PE 2 на другой конец сети, где пакет деинкапсулируется, возвращается оригинальный MAC-назначения пакета и затем пакет посылается сети 2 пользователя A.



Применение BPDU-туннеля

Настройка bpdu-tunnel на коммутаторах PE1 и PE2:

Настройка PE 1:

```
PE1(config)# bpdu-tunnel-protocol dot1x default-group-mac
PE1(config)# bpdu-tunnel-protocol stp default-group-mac
PE1(config)# bpdu-tunnel-protocol gvrp default-group-mac
PE1(config-if-ethernet1/0/1)# bpdu-tunnel-protocol dot1x
PE1(config-if-ethernet1/0/1)# bpdu-tunnel-protocol stp
PE1(config-if-ethernet1/0/1)# bpdu-tunnel-protocol gvrp
```

Настройка PE 2:

```
PE2(config)# bpdu-tunnel-protocol dot1x default-group-mac
PE2(config)# bpdu-tunnel-protocol stp default-group-mac
PE2(config)# bpdu-tunnel-protocol gvrp default-group-mac
PE2(config-if-ethernet1/0/1)# bpdu-tunnel-protocol dot1x
PE2(config-if-ethernet1/0/1)# bpdu-tunnel-protocol stp
PE2(config-if-ethernet1/0/1)# bpdu-tunnel-protocol gvrp
```

14.4 Устранение неисправностей bpdu-tunnel

После отключения функций stp, gvrp, dot1x на порте, можно настроить функцию bpdu-tunnel.

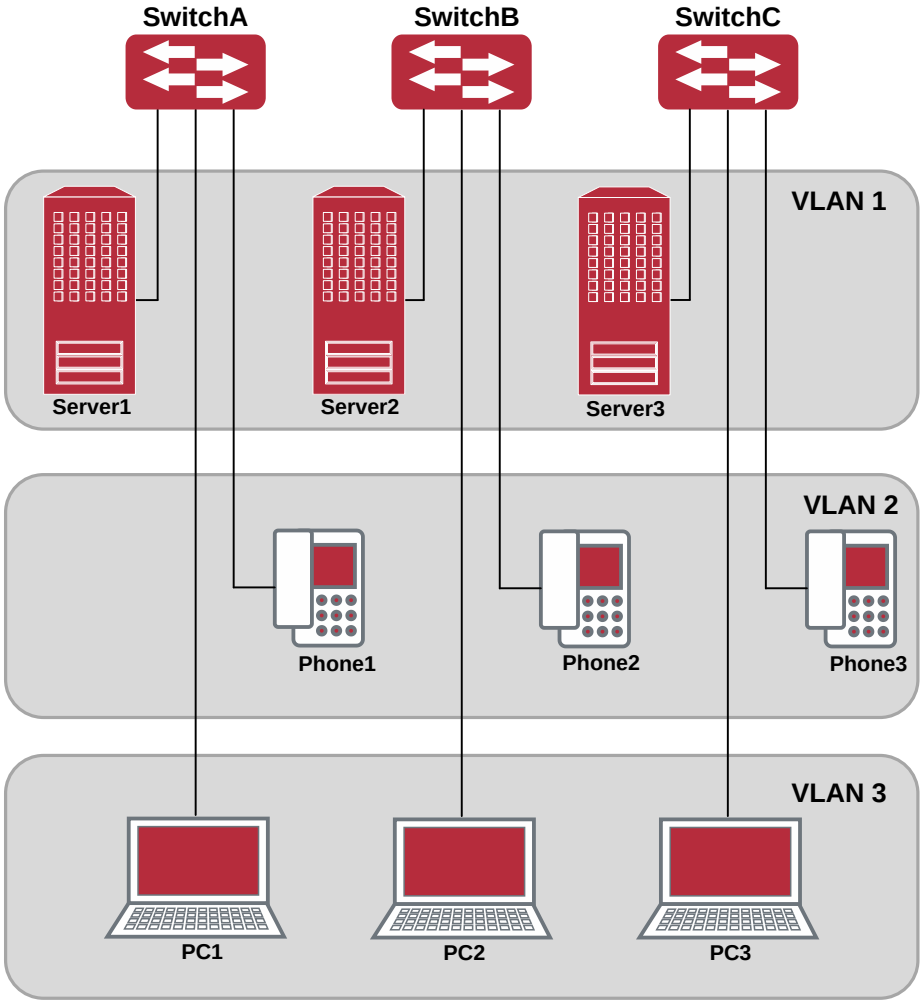
15 НАСТРОЙКА ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ – VLAN

15.1 Конфигурирование VLAN

15.1.1 Начальные сведения о VLAN

VLAN (Virtual Local Area Network – виртуальная локальная сеть) – технология, разделяющая логические адреса устройств в сети для отделения сегментов сети в зависимости от функций, выполняемых устройствами, приложений или требований управления. Таким образом, виртуальные локальные группы могут формироваться независимо от физического расположения устройств. IEEE опубликовал протокол IEEE 802.1Q для стандартизации применения VLAN. VLAN на коммутаторе работает в соответствии с этим протоколом.

Основная идея технологии VLAN в том, чтобы разделить динамически большую локальную сеть на несколько независимых широковещательных доменов в соответствии с требованиями, предъявляемыми к сети.



Логическое определение сети VLAN

Каждый широковещательный домен на рисунке является VLAN. VLAN’ы имеют те же свойства, что и физические сети, за исключением того, что VLAN – логическое объединение, а не физическое. Поэтому объединение VLAN’ов может создаваться вне зависимости от физического расположения устройств и широковещательный, многопользовательский и однопользовательский трафик внутри VLAN отделен от других VLAN’ов.

Благодаря вышеперечисленным особенностям, технология VLAN обеспечивает следующие преимущества:

- Улучшается производительность сети;
- Экономятся сетевые ресурсы;
- Упрощается управление сетью;
- Снижается стоимость сети;
- Улучшается безопасность сети;

Ethernet порты коммутатора могут работать в трех различных режимах: Access, Hybrid и Trunk. Каждый режим имеет свой способ пересылки пакетов, с меткой или без.

Порты типа Access принадлежат только одному VLAN. Обычно они используются для подключения к компьютеру.

Порты типа Trunk позволяют пересылать пакеты нескольких VLAN’ов. Они могут использоваться для соединения между коммутаторами или подключения пользовательских устройств.

Порты типа Hybrid также позволяют пересылать пакеты нескольких VLAN’ов. Они могут использоваться для соединения между коммутаторами или подключения пользовательских устройств.

Порты типов Hybrid и Trunk принимают данные по одному алгоритму, но методы отправки данных отличаются: порты типа Hybrid могут отправлять пакеты в различные VLAN’ы без метки VLAN’а, тогда как порты типа Trunk отправляют пакеты различных VLAN только с меткой VLAN’а, за исключением VLAN, прописанного на порту как native.

Применение VLAN и GVRP (GARP VLAN Registration Protocol – протокол регистрации GARP VLAN) на коммутаторе описывается в стандарте 802.1Q. Данная глава детально объясняет использование и конфигурацию VLAN’ов и GVRP.

15.1.2 Конфигурирование VLAN

1. Создание или удаление VLAN;
2. Установка или удаление имени VLAN’а;
3. Присоединение порта коммутатора к VLAN’у;
4. Установка типа порта коммутатора;
5. Настройка транкового порта;
6. Настройка порта доступа;
7. Настройка гибридного порта;
8. Включение/выключение правил обработки входных пакетов VLAN на портах;
9. Конфигурация приватного VLAN’а;
10. Настройка связей приватного VLAN’а;
11. Определение внутреннего идентификатора VLAN’а;

1. Создание или удаление VLAN

Команда	Описание
Режим глобального конфигурирования	
vlan WORD **no vlan WORD**	Создание/удаление VLAN'а или вход в режим VLAN'а

2. Установка или удаление имени VLAN'а

Команда	Описание
VLAN Mode	
name <vlan-name> **no name**	Установка или удаление имени VLAN'а

3. Присоединение порта коммутатора к VLAN'у

Команда	Описание
VLAN Mode	
switchport interface <*interface-list*> **no switchport interface <*interface-list*>**	Назначение порта коммутатора VLAN'у

4. Установка типа порта коммутатора

Команда	Описание
Режим конфигурирования **порта**	
switchport mode {trunk | access | hybrid}	Установка текущего порта как транкового, порта доступа или гибридного.

5. Настройка транкового порта

Команда	Описание
Режим конфигурирования порта	
switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD} **no switchport trunk allowed vlan**	Установка/удаление VLAN'ов, приписанных к этому транку. Команда «no» восстанавливает значение по умолчанию.

switchport trunk native vlan <*vlan-id*> **no switchport trunk native vlan**	Установка/удаление PVID для транкового порта.

6. Настройка порта доступа

Команда	Описание
Режим конфигурирования порта	
switchport access vlan <*vlan-id*> **no switchport access vlan**	Добавляет текущий порт к указанному VLAN'у. Команда NO восстанавливает значение по умолчанию.

7. Настройка гибридного порта

Команда	Описание
Режим конфигурирования порта	
switchport hybrid allowed vlan {WORD | all | add WORD | except WORD | remove WORD} {tag | untag} **no switchport hybrid allowed vlan**	Установка/удаление VLAN'а, приписанного к гибридному порту с режимом метки или без нее.
switchport hybrid native vlan <*vlan-id*> **no switchport hybrid native vlan**	Установка/удаление PVID на порту.

8. Включение/выключение правил обработки входных пакетов VLAN на портах

Команда	Описание
Режим конфигурирования порта	
vlan ingress enable **no vlan ingress enable**	Включение/выключение входящих правил на VLANe.

9. Конфигурация приватного VLAN'а

Команда	Описание
VLAN mode	
private-vlan {primary | isolated | community} **no private-vlan**	Конфигурация текущего VLAN'а как приватного. Команда NO удаляет приватный VLAN.

10. Настройка связей приватного VLAN’a

Команда	Описание
VLAN mode	
private-vlan association <secondary-vlan-list> **no private-vlan association**	Установка/удаление связей приватного VLAN’a.

11. Определение внутреннего идентификатора VLAN’a

Команда	Описание
Режим глобального конфигурирования	
vlan <2-4094> internal	Определяет идентификатор внутреннего VLAN’a.

15.1.3 Типичное применение VLAN’a

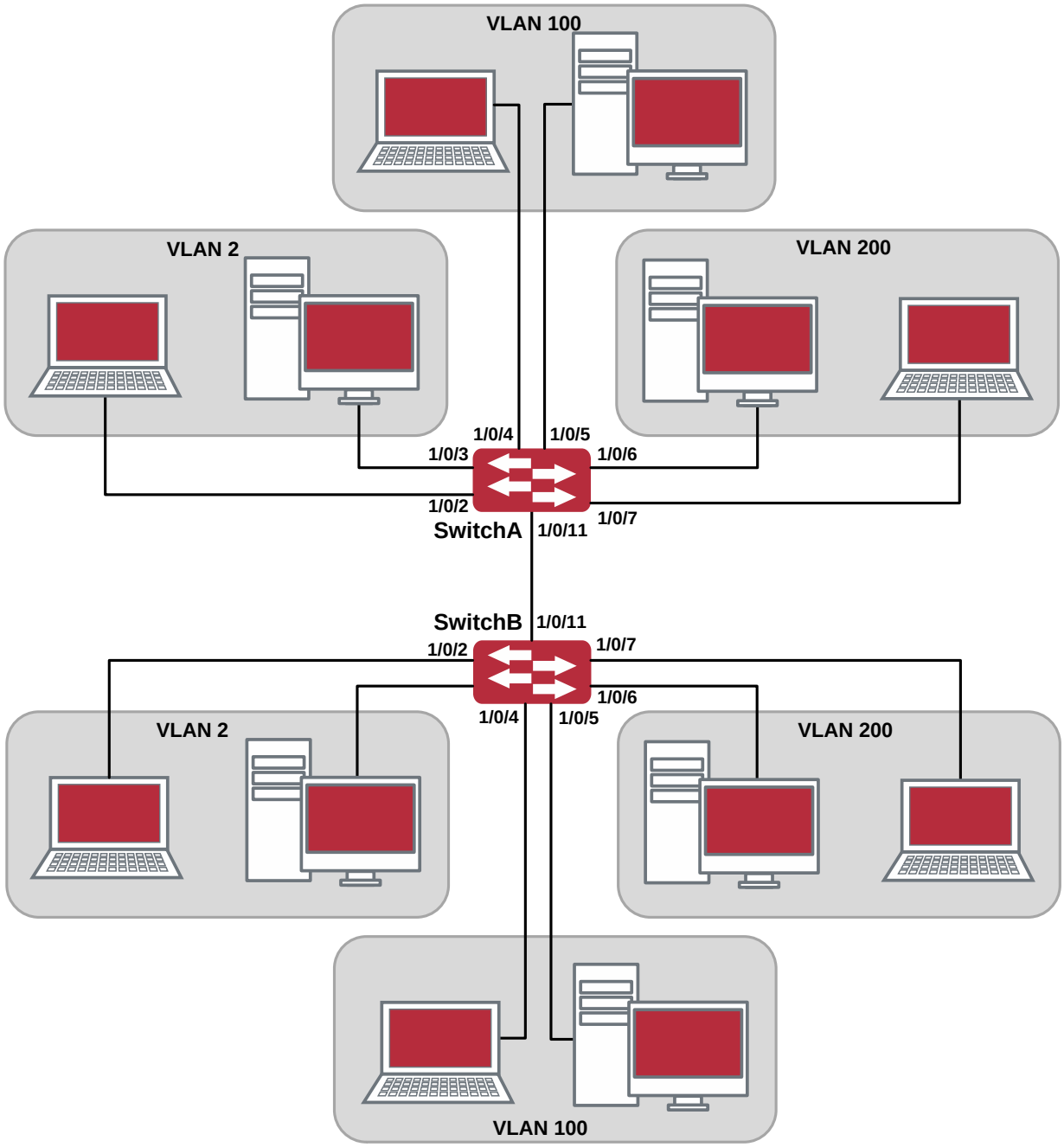
В соответствии с требованиями приложений и безопасности существующую локальную сеть необходимо разделить на три VLAN. Три VLAN имеют идентификаторы VLAN2, VLAN100 и VLAN200. Эти три VLAN охватывают два различных физических места размещения: площадки A и B.

На каждой площадке имеется коммутатор, требования к связи между площадками удовлетворяются, если коммутаторы могут выполнять обмен трафиком VLAN.

Объект конфигурации	Описание конфигурации
VLAN2	Site A and site B switch port 2-3
VLAN100	Site A and site B switch port 4-5.
VLAN200	Site A and site B switch port 6-7.
Trunk port	Site A and site B switch port 11.

Транковые порты с обеих сторон подключены к транковому каналу для передачи между узлами трафика VLAN’a. Остальные устройства подключены к другим портам VLAN’ов.

В данном примере порты 1 и 12 свободны и могут быть использованы для управляющих портов или других целей.



Типичная топология применения VLAN'а

Шаги конфигурации описаны ниже:

Коммутатор А:

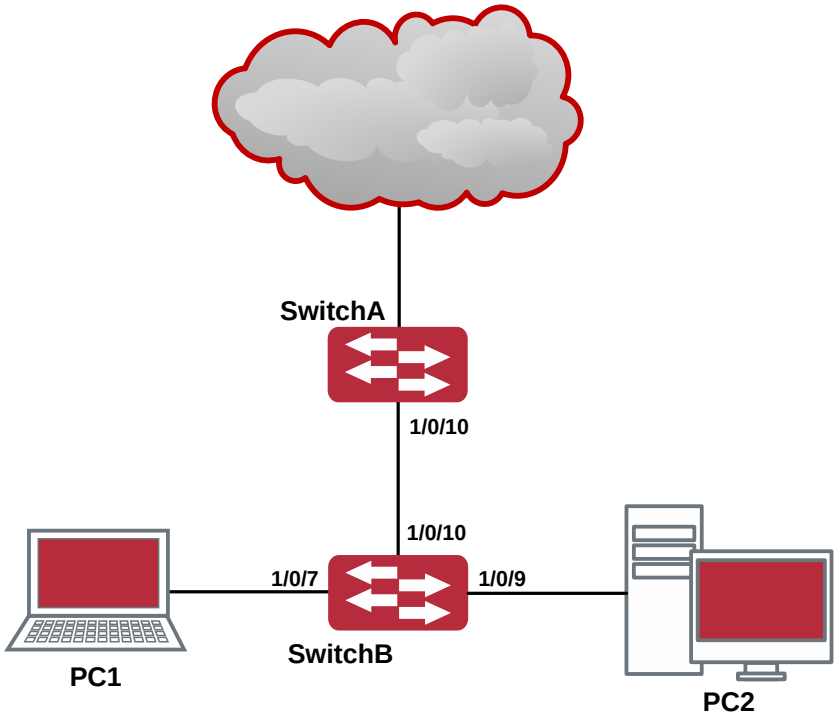
```
Switch(config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/0/2-3
Switch(Config-Vlan2)#exit
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/0/4-5
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
```

```
Switch(Config-Vlan200)#switchport interface ethernet 1/0/6-7
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
Switch(config)#
```

Коммутатор B:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/0/2-3
Switch(Config-Vlan2)#exit
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/0/4-5
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/0/6-7
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
```

15.1.4 Типичное применение гибридных портов



Типичное применение гибридного порта

PC1 подключен к интерфейсу Ethernet 1/0/7 коммутатора B, PC2 подключен к интерфейсу Ethernet 1/0/9 коммутатора B. Порт Ethernet 1/0/10 коммутатора A к порту Ethernet 1/0/10 коммутатора B.

Требуется, чтобы PC1 и PC2 не видели друг друга по соображениям секретности. Но PC1 и PC2 должны иметь доступ к другим сетевым ресурсам через шлюз коммутатора A. Мы можем реализовать эту схему через гибридный порт.

Конфигурация объектов как описано ниже:

Порт	Тип	PVID	Пропускаемые VLAN’ы
Port 1/0/10 of Switch A	Access	10	Пропускает пакеты VLAN’а 10 без меток.
Port 1/0/10 of Switch B	Hybrid	10	Пропускает пакеты VLAN’ов 7,9, 10 без меток.
Port 1/0/7 of Switch B	Hybrid	7	Пропускает пакеты VLAN’ов 7, 10 без меток
Port 1/0/9 of Switch B	Hybrid	9	Пропускает пакеты VLAN’ов 9, 10 без меток.

Шаги конфигурации описаны ниже:

Коммутатор A:

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

Коммутатор 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
```

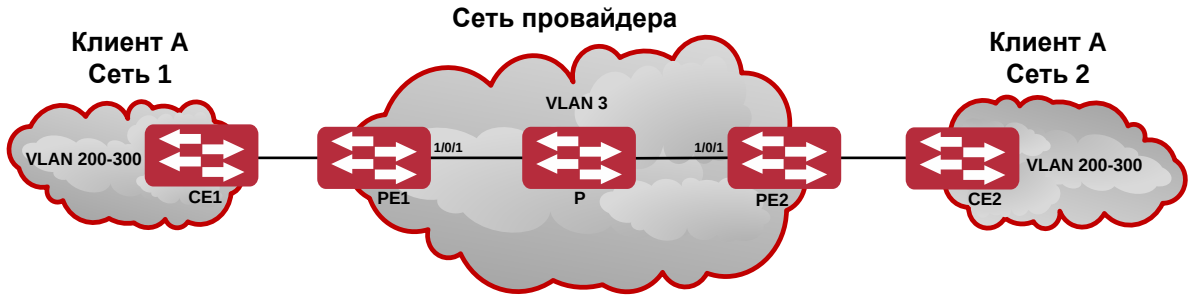
15.2 Конфигурирование туннеля Dot1Q

15.2.1 Общие сведения о туннелях Dot1q

Туннель Dot1q, также называемый QinQ (802.1q-in-802.1q), является расширением протокола 802.1q. Основная идея заключается в упаковке метки клиентского VLAN’а (CVLAN tag) в метку VLAN’а сервис-провайдера (SPVLAN tag). Пакет с двумя метками VLAN’а передается через магистральную сеть интернет-провайдера, таким образом обеспечивая простой туннель второго уровня для пользователя. Это просто и легко для управления, применимо только на статических конфигурациях и специально адаптировано для

небольших офисных или метро-сетей, использующих коммутаторы третьего уровня как магистральное оборудование.

Как показано выше, после включения на клиентском порту, туннель Dot1q присваивает каждому пользователю идентификатор SPVLAN (SPVID). Здесь идентификатор пользователя – 3. Такой же SPVID может быть присвоен таким же пользователям на других PE. Когда пакет приходит с CE1 на PE1, он несет метки VLAN'ов 200-300 внутренней сети пользователя. Когда туннель Dot1q включен, клиентский порт на PE1 добавляет в пакет дополнительные метки VLAN'ов, у которых идентификатором является назначенный пользователю SPVID. Потом пакет будет направлен только в VLAN3, который уходит в сеть интернет-провайдера, и будет нести две метки VLAN'ов (внутренняя метка добавлена, когда пакет пришел на PE1, и другая является SPVID), в то время как информация о клиентских VLAN открыта для провайдера сети. Когда пакет достигнет PE2 и перед отправкой на CE2 с клиентского порта на PE2, внешняя метка VLAN'а удаляется и пакет, пришедший на CE2, становится полностью идентичен пакету, отправленному с CE1. Для пользователя роль оператора сети между PE1 и PE2 заключается в обеспечении канала второго уровня.



Межсетевое взаимодействие на основе Dot1q туннеля

Технология туннеля Dot1q позволяет интернет-сервис-провайдеру поддерживать множество клиентских VLAN'ов с помощью одного своего VLAN'а. Провайдер и клиент могут конфигурировать свои VLAN'ы независимо друг от друга.

Технология туннеля Dot1q имеет следующие характеристики:

- Применима через простую статическую конфигурацию, не нужны сложная конфигурация и манипуляции;
- Оператор присваивает один SPVID каждому пользователю, что увеличивает количество одновременно поддерживаемых пользователей; в то же время пользователи имеют полную свободу при выборе и управлении идентификаторов VLAN (пользователь выбирает из диапазона от 1 до 4096);
- Клиентская сеть полностью независима. Когда интернет-сервис-провайдер модернизирует свою сеть, клиентские сети не требуют изменения конфигурации;

15.2.2 Конфигурирование туннеля Dot1q

1. Конфигурирование функции туннеля Dot1q на порту;
2. Конфигурирование типа протокола (TPID) на порту;

1. Конфигурирование функции туннеля Dot1q на порту

Команда	Описание
Режим конфигурирования порта	
dot1q-tunnel enable **no dot1q-tunnel enable**	Вход/выход из режима туннеля dot1q-на порту

2. Конфигурирование типа протокола (TPID) на порту

Команда	Описание
Режим конфигурирования порта	
dot1q-tunnel tpid {0x8100|0x9100|0x9200|<1-65535>}	Конфигурирование типа протокола на магистральном порту.

15.2.3 Типичное применение туннеля Dot1q

Сценарий:

Пограничные узлы PE1 и PE2 интернет-провайдера пересылают данные VLAN'ов 200-300. Между CE1 и CE2 клиентской сети через VLAN3. Порт PE1 подключен к CE1, порт 10 подключен к публичной сети, TPID подключенного оборудования – 9100; Порт 1 PE2 подключен к CE2, порт 10 подключен к публичной сети.

Объект конфигурации	Описание конфигурации
VLAN3	Порт 1/0/1 узлов PE1 и PE2.
dot1q-tunnel	Порт 1/0/1 узлов PE1 и PE2.
tpid	9100

Процедура конфигурации описана ниже:

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 1/0/1
Switch(Config-Ethernet1/0/1)#switchport mode trunk
Switch(Config-Ethernet1/0/1)#dot1q-tunnel tpid 0x9100
Switch(Config-Ethernet1/0/1)#exit
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 1/0/1
Switch(Config-Ethernet1/0/1)#switchport mode trunk
Switch(Config-Ethernet1/0/1)#dot1q-tunnel tpid 0x9100
Switch(Config-Ethernet1/0/1)#exit
Switch(Config)#
```

15.2.4 Устранение неисправностей туннеля Dot1q

❖ Включение туннеля Dot1q на транковом порту делает метку пакета данных непредсказуемой, что не подходит приложениям. Поэтому не рекомендуется использовать туннель Dot1q на транковом порту.

❖ Использование туннеля совместно с STP/MSTP не поддерживается

❖ Использование туннеля совместно с PVLAN не поддерживается.

15.3 Конфигурирование Selective QinQ

15.3.1 Общие сведени о Selective QinQ

Selective QinQ расширение функции туннелирования dot1q . Он тегирует пакеты (они получаюся по одному порту) с различными внешними тегами VLAN на основе различных внутренних тегов в соответствии с требованиями пользователя, поэтому пакеты различного типа относятся к различным VLAN на основе различных путей передачи.

15.3.2 Конфигурация Selective QinQ

1. Настройка глобально или на портах связи внутреннего и внешнего тегирования.
2. Настройка selective QinQ на порте

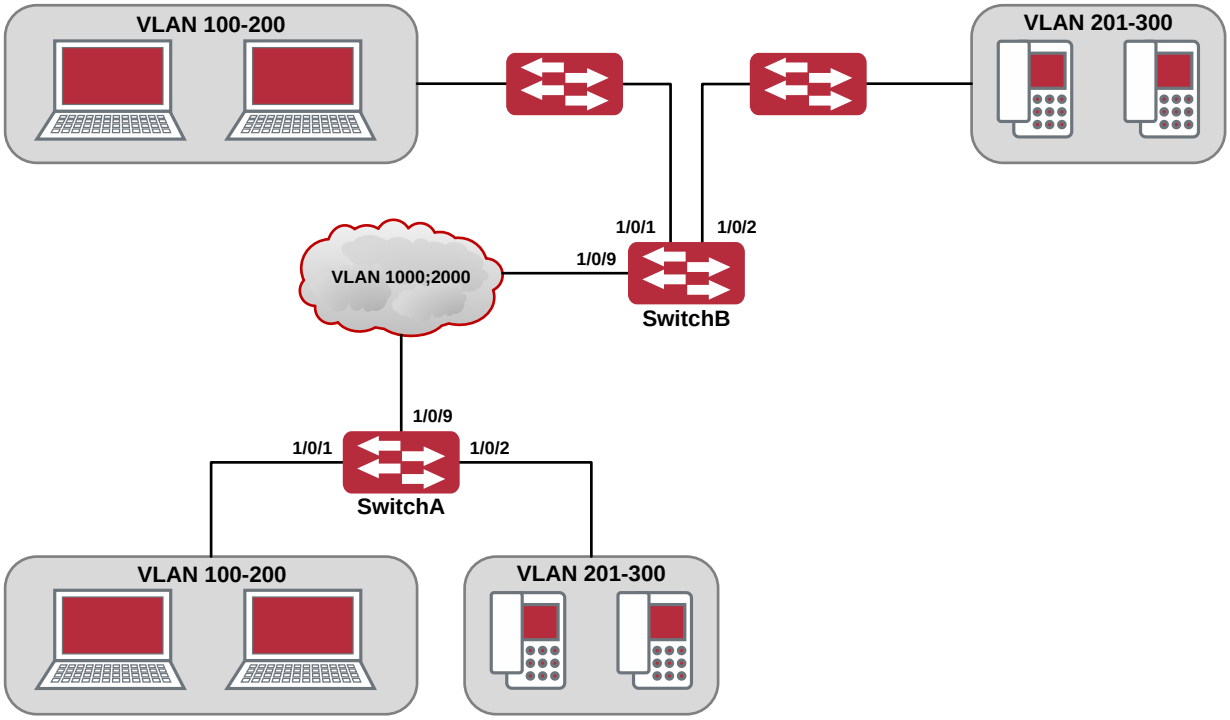
1. Настройка глобально или на портах связи внутреннего и внешнего тегирования.

Команда	Описание
Режим глобального конфигурирования или конфигурирования порта	
dot1q-tunnel selective s-vlan <*s-vid*> c-vlan <*c-vid-list*> **no dot1q-tunnel selective s-vlan <*s-vid*> c-vlan <*c-vid-list*>**	Включение/отключение глобально или на портах связи внутреннего и внешнего тегирования для selective QinQ.

2. Настройка selective QinQ на порте

Команда	Описание
Режим конфигурирования порта	
dot1q-tunnel selective enable **no dot1q-tunnel selective enable**	Включение/отключение selective QinQ на порте.

15.3.3 Типичное применение Selective QinQ



Применение Selective QinQ

1. Ethernet1/0/1 коммутатора A предоставляет доступ к сети общего пользования для пользователей PC и Ethernet1/0/2 коммутатора A предоставляет доступ к сети общего пользования для пользователей с IP телефоном, пользователи PC принадлежат к VLAN 100-VLAN 200, и пользователи с телефонами IP принадлежат к VLAN 201-VLAN 300. Ethernet 1/0/9 коммутатора A соединена с сетью общего пользования.

2. Ethernet1/0/1 и Ethernet1/0/2 коммутатора B предоставляет сетевой доступ для пользоваелей PC, принадлежащих VLAN 100- VLAN 200 и пользователей с IP телефонами, принадлежащих VLAN 201-VLAN 300 соответственно. Ethernet 1/0/9 соединена с сетью общего пользования.

3. Сеть общего пользования разрешает пересылать пакеты в VLAN 1000 и VLAN 2000.

4. Включен selective QinQ на портах Ethernet1/0/1 и Ethernet1/0/2 на коммутаторах A и B соответственно. Пакеты VLAN 100- VLAN 200 отмечены тегом VLAN 1000 как выходящий тег VLAN на Ethernet1/0/1, и пакеты VLAN 201- VLAN 300 отмечены тегом VLAN 2000 как выходящий тег VLAN на Ethernet1/0/2.

Конфигурирование:

Создание VLAN 1000 and VLAN 2000 on SwitchA.

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

Насройка Ethernet1/0/1 как гибридного порта и настройка удаления тега VLAN при пересылке пакетов в VLAN 1000.

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

Настройка правил отображения для selective QinQ на Ehernet1/0/1 для помещения тега VLAN 1000 как выходящего тега VLAN в пакеты с тегами VLAN 100-VLAN 200.

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

Включение selective QinQ на Ethernet1/0/1.

```
switch(config-if-ethernet1/0/1)#dot1q-tunnel selective enable
```

Настройка Ethernet 1/0/2 как гибридного порта и настройка удаления тега VLAN при пересылке пакетов в VLAN 2000.

```
switch(config-if-ethernet1/0/2)#switchport mode hybrid
switch(config-if-ethernet1/0/2)#switchport hybrid allowed vlan 2000 untag
```

Настройка правил отображения для selective QinQ на Ehernet1/0/2 для помещения тега VLAN 2000 как выходящего тега VLAN в пакеты с тегами VLAN 201- VLAN 300.

```
switch(config-if-ethernet1/0/2)#dot1q-tunnel selective s-vlan 2000 c-vlan 201-300
# Включение selective QinQ на Ethernet 1/0/2.
switch(config-if-ethernet1/0/2)#dot1q-tunnel selective enable
```

Настройка порта Ethernet 1/0/9 как гибридного порта и настройка сохранения тега VLAN при пересылке пакетов в 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 проведения конфигурации, пакеты VLAN 100-VLAN 200 от Ethernet1/0/1 автоматически отмечаются тегом с VLAN 1000 как выходящим тегом VLAN, и пакеты VLAN 201- VLAN 300 от Ethernet1/0/2 автоматически отмечаются тегом с VLAN 2000 как выходящим тегом VLAN на SwitchA.

Настройки на Switch B аналогичны настройкам на Switch A, конфигурация следующая:

```
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
```

15.3.4 Устранение неисправностей Selective QinQ

❖ Функции Selective QinQ и dot1q-tunnel не могут быть одновременно настроены на порте.

❖ Только связь глобального отображения или связь отображения порта можно настроить для selective QinQ.

15.4 Настройка трансляции VLAN’ов

15.4.1 Общие сведения о трансляции VLAN’ов

Трансляция VLAN’ов, как следует из названия, транслирует оригинальный идентификатор VLAN’а в новый в соответствии с требованиями пользователя или для обмена данными между различными VLAN’ами. Трансляция может применяться как для входящей, так и исходящей информации. Данное оборудование поддерживает изменение идентификатора VLAN’а только на входе.

Применение и конфигурирование трансляции VLAN’ов подробно объясняется далее.

15.4.2 Конфигурирование трансляции VLAN’а

1. Конфигурирование функции трансляции VLAN’а на порту;
2. Конфигурирование соответствий трансляции VLAN’а на порту;
3. Просмотр конфигурации соответствий трансляции VLAN’а;

1. Конфигурирование функции трансляции VLAN’а на порту

Команда	Описание
Режим конфигурирования порта	
vlan-translation enable **no vlan-translation enable**	Включает или выключает режим трансляции VLAN

2. Конфигурирование соответствий трансляции VLAN’а на порту

Команда	Описание
Режим конфигурирования порта	
vlan-translation *<old-vlan-id>* to *<new-vlan-id>* in **no vlan-translation old-vlan-id in**	Добавление/удаление соответствий трансляции VLAN’ов.

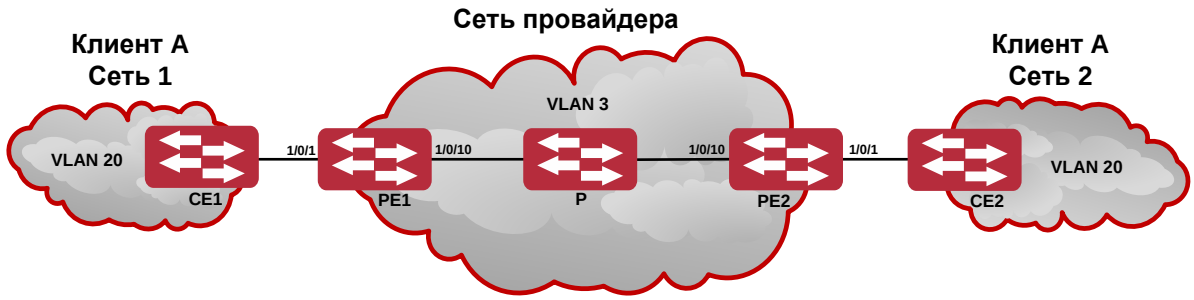
3. Просмотр конфигурации соответствий трансляции VLAN’а

Команда	Описание
Режим администратора	
show vlan-translation	Просмотр сконфигурированных соответствий трансляции VLAN’ов

15.4.3 Типовое применение трансляции VLAN’ов

Сценарий:

Пограничные узлы PE1 и PE2 интернет-провайдера поддерживают VLAN данных 20 между CE1 и CE2 из клиентской сети, через 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.



Топология сети с трансляцией VLAN’ов

Объект конфигурации	Описание конфигурации
VLAN-translation	Порт 1/0/1 узлов PE1 и PE2.
Trunk port	Порты 1/0/1 и 1/0/10 узлов PE1 и PE2.

Процедура конфигурирования указана ниже:

PE1, PE2:

```
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 1/0/1
switch(Config-Ethernet1/0/1)#switchport mode trunk
switch(Config-Ethernet1/0/1)#exit
switch(Config)#
```

15.4.4 Устранение неисправностей трансляции VLAN'ов

Обычно трансляция VLAN применяется на транковых портах.

Приоритеты между трансляцией VLAN'ов и входящей фильтрацией VLAN'ов распределяются так: Трансляция VLAN'ов выше входящей фильтрации VLAN'ов

15.5 Конфигурация Multi-to-One VLAN трансляции

15.5.1 Введение в Multi-to-One VLAN трансляцию

Трансляция Multi-to-One VLAN – это трансляция исходного VLAN ID в новом VLAN ID в соответствии с требованиями пользователей на восходящий траффик и возвращение исходного VLAN ID на нисходящий траффик.

Применение и конфигурация Multi-to-One VLAN передачи будут подробно описаны в этом разделе.

15.5.2 Настройка передачи Multi-to-One VLAN

1. Настройка Multi-to-One VLAN передачи на порте
2. Просмотр настроек и Multi-to-One VLAN передач

1. Настройка Multi-to-One VLAN передачи на порте

Команда	Описание
Режим конфигурирования порта	
vlan-translation n-to-1 <*WORD*> to <*new-vlan-id*> **no vlan-translation n-to-1 <*WORD*>**	Включение/отключение трансляции Multi-to-One VLAN

2. Просмотр настроек Multi-to-One VLAN передачи

Команда	Описание
Режим администратора	
show vlan-translation n-to-1	Показывает связанные настройки трансляции Multi-to-One VLAN

15.5.3 Типичное применение трансляции Multi-to-One VLAN

Сценарий:

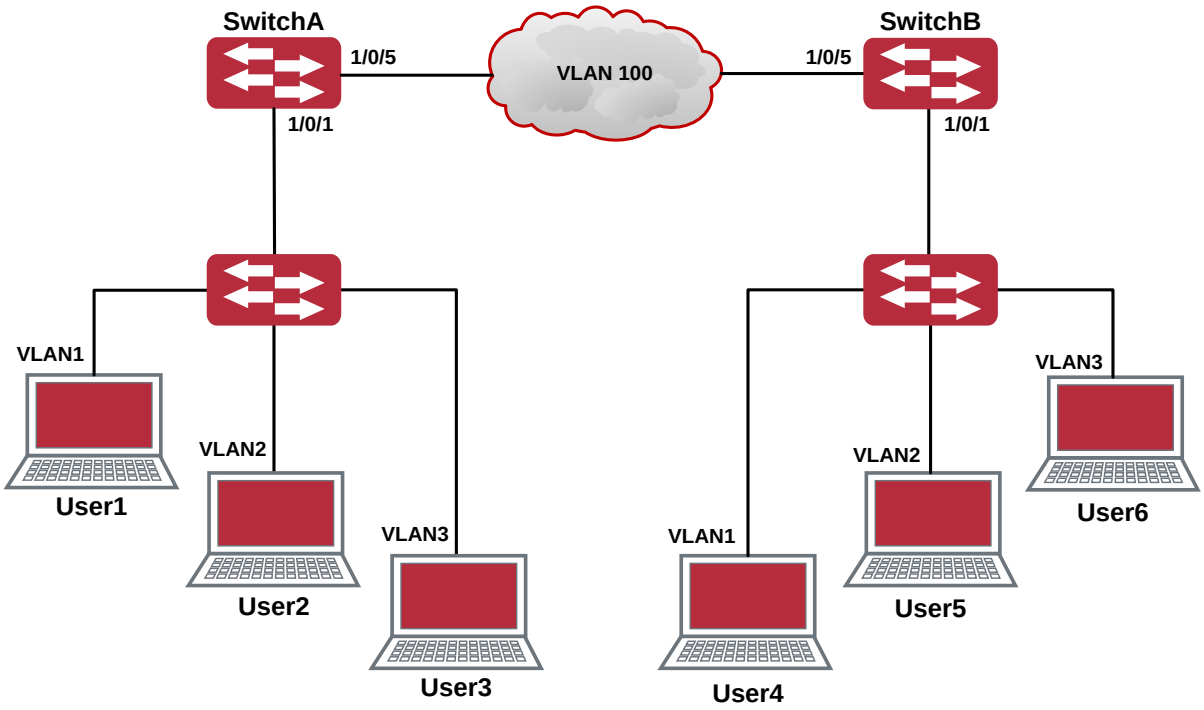
Пользователи 1, 2 и 3 принаддлежат VLAN 1, 2 и 3 соответственно. Входящий траффик данных, пользователей 1, 2 и 3 будет переведен в VLAN100 на интерфейсе Ethernet1/0/1 со стороны SwitchA. Таким же образом будет передан траффик данных пользователей 3, 4 и 5.

Элемент конфигурации	Описание
VLAN	SwitchA, SwitchB
Trunk Port	Нисходящий порт 1/0/1 и восходящий порт 1/0/5 на SwitchA и SwitchB
Multi-to-One VLAN-трансляция	Нисходящий порт 1/0/1 на SwitchA и SwitchB

Процедура настройки:

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
```



Типичное применение трансляции VLAN

15.5.4 Устранение неисправностей Multi-to-One VLAN трансляции

- ❖ Нельзя одновременно использовать с Dot1q-tunnel
- ❖ Нельзя одновременно использовать с VLAN-translation
- ❖ MAC-адрем не должен существовать в оригинальном и транслированном VLAN.
- ❖ Убедитесь, что аппаратный чип может поддерживать нормальную работу клиентов.
- ❖ Превышение предела обучения MAC-адресам может повлиять на Multi-to-One VLAN трансляцию
- ❖ Multi-to-One VLAN трансляция должна быть включена после MAC обучения.

15.6 Конфигурирование динамических VLAN

15.6.1 Общие сведения

Динамическим VLAN называется так в противовес статическому VLAN'у (называемому портом, приписанным к VLAN'у). Динамический VLAN, поддерживаемый коммутатором, включает в себя VLAN на MAC-адресах, VLAN подсетей и протокольный VLAN. Подробное описание далее:

VLAN, базирующийся на MAC адресах представляет собой технологию, когда каждый хост с определенным MAC адресом соответствует определенному VLAN'у. Это позволяет пользователю сети сохранить свое членство в VLANe при перемещении из одного места в другое. Как мы видим, главное преимущество этого метода в том, что нет необходимости переконфигурировать VLAN, когда пользователь меняет свое месторасположение, а именно переключается с одного коммутатора на другой. Это следствие того, что VLAN базируется на MAC адресе пользователя, а не на порту коммутатора.

VLAN, базирующийся на IP подсетях представляет собой технологию, где метка VLAN назначается в соответствии с IP адресом источника и его маской подсети. Преимущество этого метода то же, что и у предыдущего, пользователю не требуется изменять конфигурацию при изменении местонахождения.

Метод VLAN'а на базе протоколов сетевого уровня назначает различным протоколам различные номера VLAN'ов. Это очень удобно для тех сетевых администраторов, которые хотят упорядочивать пользователей по приложениям и сервисам. Более того, пользователи могут свободно перемещаться по сети, зарегистрировавшись в ней один раз. Преимуществом данного метода является то, что он позволяет пользователям менять свое местоположение без изменения конфигурации VLAN'ов, а то, что VLAN'ы различаются по типу протоколов – очень важно для сетевого администратора. К тому же, данный метод не требует добавления метки фрейма для идентификации VLAN'а, что снижает общий трафик в сети.

Замечание: Порты, которые необходимо приписать к динамическим VLAN должны быть сконфигурированы как гибридные.

15.6.2 Конфигурирование динамических VLAN

1. Конфигурирование функции VLAN'а по MAC адресам на порту;
2. Настройка VLAN как MAC VLAN;
3. Конфигурирование соответствия между MAC адресами и VLAN'ами;

4. Конфигурирование соответствия между протоколами и VLAN’ами;

1. Конфигурирование функции VLAN’а по MAC адресам на порту

Команда	Описание
Режим конфигурирования порта	
switchport mac-vlan enable **no switchport mac-vlan enable**	Включение/выключение функции VLAN’а по MAC адресам на порту

2. Настройка VLAN как MAC VLAN

Команда	Описание
Режим глобального конфигурирования	
mac-vlan vlan <*vlan-id*> **no mac-vlan**	Конфигурация определенного VLAN’а как MAC VLAN; команда «no mac-vlan»удаляет настройки MAC VLAN’а на данном VLANe.

3. Конфигурирование соответствия между MAC адресами и VLAN’ами

Команда	Описание
Режим глобального конфигурирования	
mac-vlan mac <mac-addrss> vlan <vlan-id> priority <priority-id> **no mac-vlan {mac <*mac-addrss*>|all}**	Добавление/удаление соответствий между MAC адресами и VLAN’ами, а именно – запись/исключение определенного MAC адреса из определенного VLAN’а

4. Конфигурирование соответствия между протоколами и VLAN’ами

Команда	Описание
Режим глобального конфигурирования	
protocol-vlan mode [etherII | llc | snap] etype <etype-id> vlan <vlan-id> **no protocol-vlan [all | mode] {etype <etype-id> vlan <vlan-id>|all}**	Добавление/удаление соответствий между протоколами и VLAN’ами, а именно – вхождение/исключение определенного протокола в/из определенного VLAN’а.

15.6.3 Типовое применение динамического VLAN’а

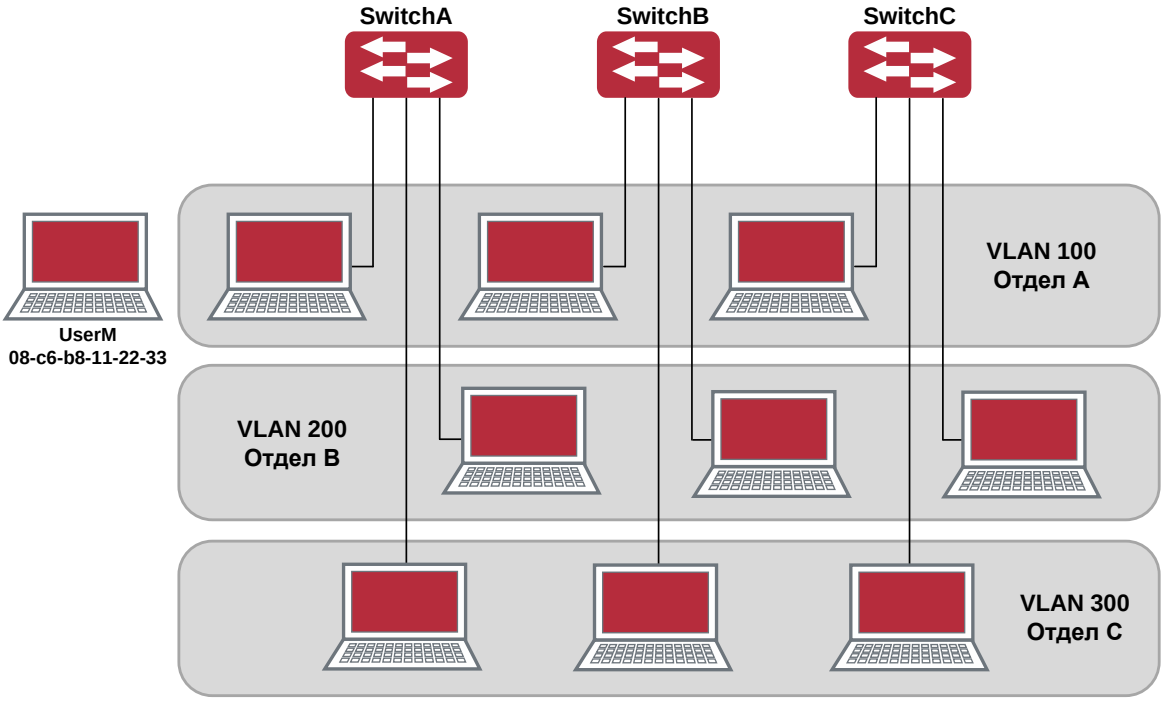
Сценарий:

В офисной сети отдел А принадлежит к VLAN100. Несколько сотрудников отдела часто вынуждены перемещаться внутри офисной сети. Так же требуется обеспечивать доступ других сотрудников отдела к VLAN100. Допустим, что один из сотрудников – UserM. MAC адрес его компьютера – 08-c6-b3-11-22-33, когда M переключается в, один из портов коммутатора A, B или C, интерфейс автоматически конфигурируется как гибридный и подключается к VLAN100 в режиме «без меток». В этом случае данные VLAN100 будут передаваться на порт, к которому подключен M, и обеспечивать требования связности в VLAN100.

Объект конфигурации	Описание конфигурации
MAC-based VLAN	Общая конфигурация коммутаторов A,B,C.

Пример конфигурации:

```
Switch A, Switch B, Switch C:
switch(Config)#mac-vlan mac 08-c6-b3-11-22-33 vlan 100 priority 0
switch(Config)#exit
```



Типовая топология применения динамического VLAN’а

15.6.4 Устранение неисправностей динамического VLAN’а

На коммутаторах со сконфигурированным динамическим VLANом, когда к ним подключено несколько устройств (например, два компьютера), бывает, что первая попытка соединения между ними не получается. Решение в данном случае такое – надо дать возможность обоим устройствам успешно послать какие-либо пакеты в сеть

(например ICMP, командой ping), это позволит коммутатору запомнить их MAC адреса, и тогда они смогут свободно связываться через динамический VLAN.

Приоритеты динамического VLAN'а и входного фильтра VLAN'ов для обработки пакетов следующие: приоритет динамического VLAN'а выше, чем у входящего фильтра.

15.7 Конфигурирование GVRP

15.7.1 Общая информация о GVRP

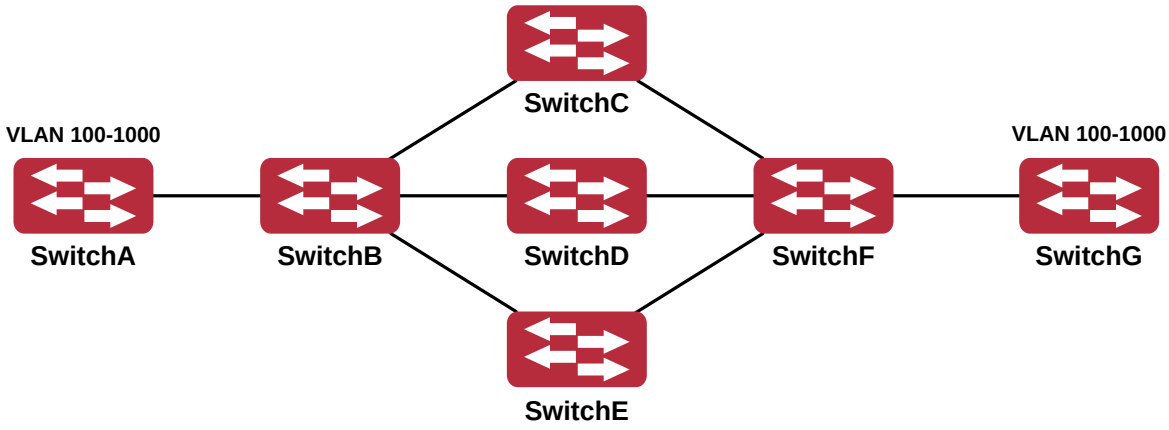
Протокол GARP (Generic Attribute Registration Protocol), используется для

динамического распределения, распространения и регистрации атрибутов информации между коммутаторами-участниками в сети коммутации.

Атрибутом может быть информация VLAN, групповой MAC-адрес и так далее. Очевидно, что протокол GARP может транспортировать множество атрибутов на коммутатор, на который их необходимо передать (*populate*). На основе GARP определены различные приложения (называемые приложениями-объектами GARP), одним из них является GVRP.

Протокол GVRP (GARP VLAN Registration Protocol) — это приложение, использующее для работы механизм GARP. Оно отвечает за обслуживание информации динамической регистрации *VLAN* и передачу регистрационной информации на другие коммутаторы. Коммутаторы, поддерживающие GVRP, могут принимать информацию динамической регистрации VLAN от других коммутаторов и обновлять локальную информацию регистрации VLAN в соответствии с принятой.

Коммутатор, на котором включен протокол GVRP может передавать свою собственную информацию регистрации VLAN на другие коммутаторы. Принятая информация содержит локальную статическую информацию, заданную вручную и динамическую информацию, полученную обучением от других коммутаторов. Поэтому, за счет передачи информации регистрации VLAN, состоятельная информация VLAN может быть распространена на все коммутаторы с включенным GVRP.



Типичная схема применения

Коммутаторы A и G не соединены между собой на сети второго уровня; B, C, D, E, F промежуточные коммутаторы, подключенные к A и G. На коммутаторах A и G сконфигурировали VLAN100-1000 вручную, тогда как на B, C, D, E, F их нет. Когда GVRP выключен, A и G не могут ни с кем соединиться, поскольку промежуточные узлы не имеют соответствующих VLAN'ов. Однако после включения GVRP на всех узлах, его механизм

передачи атрибутов VLAN позволяет промежуточным узлам регистрировать VLAN'ы динамически, и VLAN в VLAN100-1000 узлов A и G могут соединяться с любым другим. Все VLAN'ы, динамически зарегистрированные на промежуточных узлах, будут разрегистрированы, когда на узлах A и G вручную удалятся VLAN100-1000. Таким образом одинаковые VLAN'ы двух несоседних узлов могут соединяться посредством протокола GVRP вместо ручной конфигурации всех промежуточных узлов для получения простой конфигурации VLAN'ов.

15.7.2 Настройка GVRP

1. Конфигурирование таймера GARP;
2. Включение/выключение функции GVRP на порту;
3. Включение функции GVRP в коммутаторе;

1. Конфигурация таймера GARP

Команда	Описание
Режим глобального конфигурирования	
garp timer join <200-500> **garp timer leave <500-1200>** **garp timer leaveall <5000-60000>** **no garp timer (join | leave | leaveAll)**	Конфигурирование таймеров удержания, слияния и выхода для GARP.

2. Включение/выключение функции GVRP на порту

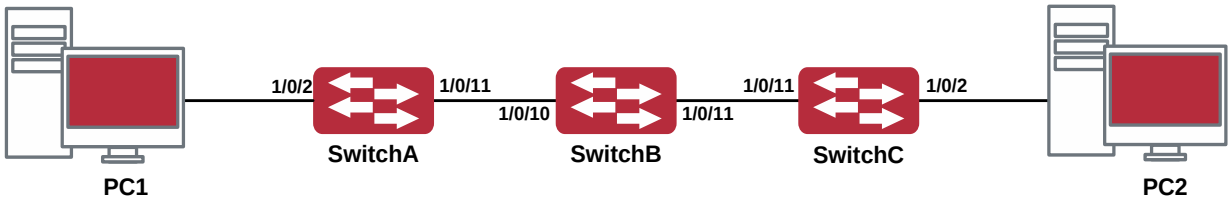
Команда	Описание
Режим конфигурирования порта	
gvrp **no gvrp**	Включение/выключение функции GVRP на порту.

3. Включение функции GVRP в коммутаторе

Команда	Описание
Режим глобального конфигурирования	
gvrp **no gvrp**	Включение/выключение функции GVRP в коммутаторе.

15.7.3 Примеры применения GVRP

Сценарий 1:



Типичная топология применения GVRP

Для получения информации динамической регистрации VLAN и ее обновления на коммутаторах должен быть сконфигурирован протокол GVRP.

Сконфигурированный на коммутаторах A, B и C протокол GVRP , позволяет динамически сконфигурировать VLAN 100 на коммутаторе B и двум рабочим станциям, подключенным к VLAN 100 на коммутаторах A и C связаться между собой без статического конфигурирования VLAN 100 на коммутаторе B.

Объект настройки	Описание объекта настройки
VLAN100	Порты 2-6 на коммутаторах A и C.
Trunk port	Порты 11 на коммутаторах A и C, порты 10, 11 на коммутаторе B.
GVRP в режиме глобального конфигурирования	Коммутаторы A, B, C.
GVRP в режиме конфигурирования портов	Порты 11 коммутаторов A и C, порты 10, 11 коммутатора B.

Подключим две рабочие станции к портам VLAN 100 на коммутаторах A и C, подключим порт 11 на коммутаторе A к порту 10 на коммутаторе B и порт 11 на коммутаторе B к порту 11 на коммутаторе C.

Шаги конфигурации описаны ниже:

Коммутатор 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
```

Коммутатор 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
```

Коммутатор 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
```

15.7.4 Устранение неисправностей GVRP

Счетчик GARP, установленный на транковых портах на обоих концах магистральной линии должен быть одинаковым, в противном случае GVRP не сможет работать нормально. Рекомендуется избегать одновременной работы протоколов GVRP и RSTP на узле. Если требуется включить протокол GVRP, необходимо сначала выключить функцию RSTP на портах.

16 НАСТРОЙКА ТАБЛИЦЫ MAC АДРЕСОВ

16.1 Общие сведения о таблице MAC адресов

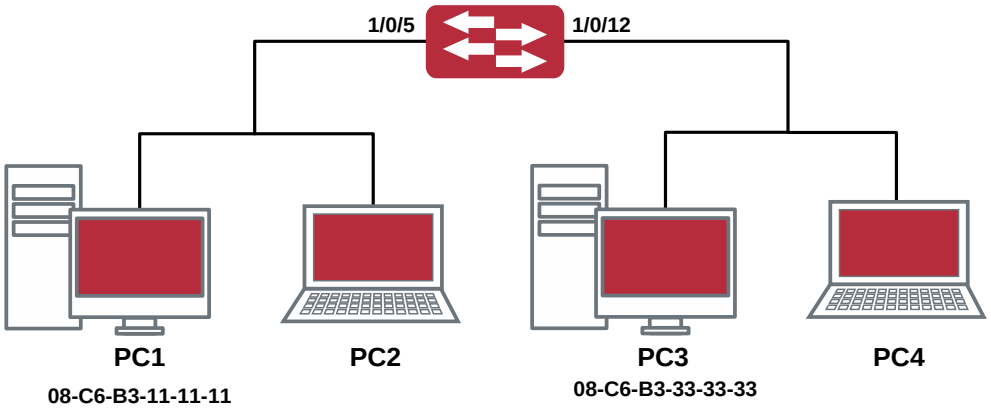
Таблица MAC-адресов — это таблица соответствий MAC-адресов устройств назначения портам коммутатора. MAC адреса делятся на статические и динамические. Статические MAC адреса вручную сконфигурированы пользователем, имеют наивысший приоритет и действуют постоянно (они не могут быть замещены динамическим MAC адресами). Динамические адреса запоминаются коммутатором при передаче пакетов данных, и они действуют ограниченное время. Когда коммутатор получает фрейм данных для пересылки, он сохраняет MAC адрес источника фрейма и соответствующий ему порт назначения. Когда таблица MAC адресов опрашивается на предмет MAC адреса приемника, при нахождении нужного адреса, пакет данных отправляется на соответствующий порт, в противном случае коммутатор пересылает пакет на свой широковещательный домен. Если динамический MAC адрес не встречается в пакетах для пересылки длительное время, запись о нем удаляется из таблицы MAC адресов коммутатора.

Для таблицы MAC адресов определены две операции:

1. Получение MAC адреса;
2. Отправка или фильтрация пакета данных в соответствии с таблицей MAC адресов.

16.1.1 Получение таблицы MAC адресов

Таблица MAC адресов может быть построена статически или динамически. Статическим конфигурированием настраивается соответствие между MAC адресами и портами. Динамическое обучение – это процесс, когда коммутатор изучает связи между MAC адресами и портами и регулярно обновляет таблицу MAC адресов. В этой секции мы остановимся на процессе динамического построения таблицы MAC адресов.



Динамическое построение таблицы MAC адресов

Топология на рисунке выше: 4 компьютера подключены к коммутатору, где PC1 и PC2 принадлежат одному физическому сегменту (домену коллизий), физический сегмент подключен к порту 1/0/5 коммутатора, PC3 и PC4 принадлежат к другому физическому сегменту, подключенному к порту 1/0/12 коммутатора.

Начальная таблица MAC адресов не содержит никаких значений. Возьмем для примера процесс связи между PC1 и PC3. Процесс обучения MAC адресам, следующий:

1. Когда PC1 посылает сообщение к PC3, MAC адрес источника 08-C6-B3-11-11-11-11 и порт 1/0/5 из этого сообщения заносятся в таблицу MAC адресов коммутатора.
2. В то же время коммутатору надо понять, как доставить сообщение на адрес 08-C6-B3-33-33-33. Так как таблица содержит запись только для адреса 08-C6-B3-11-11-11-11 и порта 1/0/5, а для адреса 08-C6-B3-33-33-33 никаких записей нет, коммутатор рассылает данное сообщение на все свои порты (предполагаем, что все порты принадлежат по умолчанию VLAN1).
3. PC3 и PC4 получают сообщение, посланное PC1, но PC4 не отвечает на это сообщение, так как адрес приемника 08-C6-B3-33-33-33, и отвечать на него будет только PC3. Когда порт 1/0/12 получает сообщение, отправленное PC3, в таблицу MAC адресов добавляется запись о MAC адресе 08-C6-B3-33-33-33 и соответствующем ему порте 1/0/12.
4. Теперь таблица MAC адресов имеет две динамические записи: MAC адрес 08-C6-B3-11-11-11-11 – порт 1/0/5 и 08-C6-B3-33-33-33 – порт 1/0/12.
5. После обмена пакетами между PC1 и PC3, коммутатор больше не получает пакетов, отправленных PC1 и PC3. И записи в таблице MAC адресов, соответствующие этим устройствам удаляются через 300 или 2*300 секунд (т.е. простое или двойное время жизни). 300 секунд здесь это время жизни по умолчанию для записей в таблице MAC адресов. Время жизни может быть изменено на коммутаторе.
6.

16.1.2 Пересылка или фильтрация кадров

Коммутатор посылает или отфильтровывает принимаемые пакеты данных в соответствии с таблицей MAC адресов. Рассматривая для примера рисунок выше, предполагаем, что коммутатор изучил адреса PC1 и PC3, и пользователь вручную настроил соответствие портов для PC2 и PC4. Таблица MAC адресов коммутатора будет следующей:

MAC адрес	Номер порта	Кем добавлена запись
08-C6-B3-11-11-11	1/0/5	Динамическое обучение
08-C6-B3-22-22-22	1/0/5	Статическая конфигурация
08-C6-B3-33-33-33	1/0/12	Динамическое обучение
08-C6-B3-44-44-44	1/0/12	Статическая конфигурация

1. Отправка пакетов в соответствии с таблицей MAC адресов

Если PC1 посылает пакет к PC3, коммутатор отправляет данные, полученные с порта 1/0/5 на порт 1/0/12

2. Фильтрация данных в соответствии с таблицей MAC адресов

Если PC1 посылает сообщение PC2, коммутатор, проверив таблицу MAC адресов, находит PC2 и PC1 в одном физическом сегменте и отфильтровывает это сообщение (то есть сбрасывает это сообщение).

Коммутатором могут пересылаться три типа кадров:

- Broadcast frames;

- Multicast frames;
- Unicast frames;

Далее описывается, как коммутатор работает со всеми тремя типами пакетов:

1. Broadcast frame: Коммутатор может определять коллизии в домене, но только не для широковещательных доменов. Если VLAN'ы не установлены, все устройства, подключенные к коммутатору, считаются находящимися в одном широковещательном домене. Когда коммутатор получает Broadcast frame, он пересылает его во все порты. Если VLAN'ы сконфигурированы, таблица MAC адресов адаптируется в соответствии с дополнительной информацией о VLAN'ах. В этом случае коммутатор отправляет фрейм только на порты, находящиеся в том же VLANe.

2. Multicast frame: если многопользовательский домен неизвестен, коммутатор рассылает фрейм в том же VLANe, но, если включена функция IGMP snooping или сконфигурирована статическая многопользовательская группа, коммутатор будет посылать этот фрейм в порты многопользовательской группы.

3. Unicast frame: если VLAN'ы не сконфигурированы, то, если MAC адрес приемника есть в таблице MAC адресов коммутатора, коммутатор напрямую пересылает пакет в соответствующий порт. Если же адрес приемника в таблице не найден, коммутатор делает широковещательную рассылку этого фрейма. Если VLAN'ы сконфигурированы, коммутатор рассылает Unicast frame только внутри одного VLAN'а. Если MAC адрес найден в таблице, но принадлежит другому VLAN'у, коммутатор делает широковещательную рассылку фрейма в том VLANe, к которому принадлежит фрейм.

16.2 Конфигурирование таблицы MAC адресов

1. Конфигурирование времени жизни MAC адресов;
2. Конфигурирование статической фильтрации или пересылки;
3. Очистка динамической таблицы MAC адресов;

1. Конфигурирование времени жизни MAC адресов

Команда	Описание
Режим глобального конфигурирования	
mac-address-table aging-time <*0*|*aging-time*> **no mac-address-table aging-time**	Конфигурирование времени жизни MAC адресов

2. Очистка динамической таблицы MAC адресов

Команда	Описание
Режим администратора	
clear mac-address-table dynamic [address *<mac-addr>***] [vlan** *<vlan-id>***] [interface [ethernet | portchannel]** *<interface-name>***]**	Очистка динамической таблицы MAC адресов

3. Конфигурирование статической фильтрации или пересылки

Команда	Описание
Общий режим	
mac-address-table {static | static-multicast | blackhole} address *<mac-addr>* **vlan** *<vlan-id>* **[interface [ethernet | portchannel]** *<interface-name>***] | [source|destination|both]** **no mac-address-table {static | static-multicast | blackhole | dynamic} [address** *<mac-addr>***] [vlan** *<vlan-id>***] [interface [ethernet | portchannel]** *<interface-name>***]**	Конфигурирование статических записей для MAC адресов, статических многопользовательских записей, записей фильтрации пакетов.

4. Настройка обучения MAC адресов через управление процессором

Команда	Описание
Режим глобального конфигурирования	
mac-address-learning cpu-control **no mac-address-learning cpu-control**	Включение/отключение обучения MAC-адресов через управление CPU

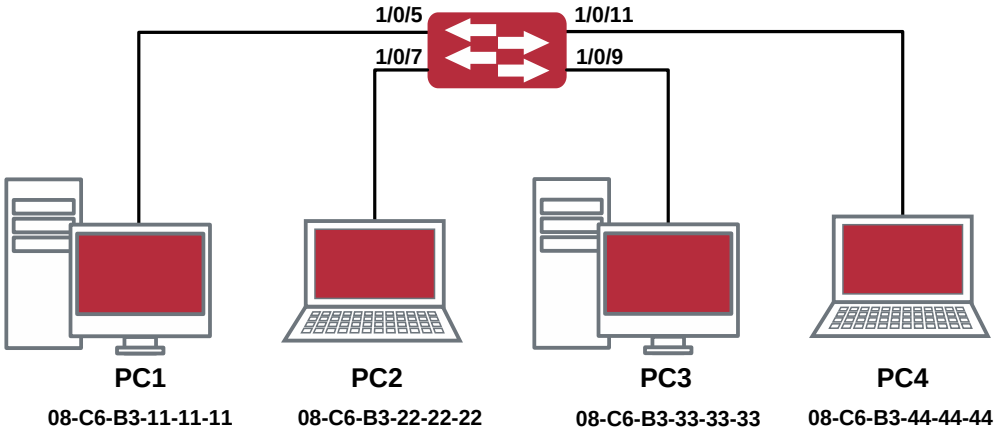
5. Настройка защиты отколлизий

Команда	Описание
Режим глобального конфигурирования	
mac-address-table avoid-collision **no mac-address-table avoid-collision**	Включение/отключение функции таблицы коллизии MAC-адресов, выданных ffp
show collision-mac-address-table	Показывает таблицу коллизий MAC-адресов
Режим администратора	
clear collision-mac-address-table	Очистить таблицу MAC-адресов

16.3 Примеры типичной конфигурации

Сценарий:

Четыре компьютера, как показано на рисунке, подключены к портам 1/0/5, 1/0/7, 1/0/9, 1/0/11 коммутатора. Все 4 компьютера принадлежат по умолчанию VLAN1. В соответствии с требованиями к сети, включено обучение динамическим адресам. PC1 содержит важные данные, и недоступен для других компьютеров из других физических сегментов; PC2 и PC3 статически приписаны к портам 7 и 9, соответственно.



Типичный пример конфигурации таблицы MAC адресов

Этапы конфигурации показаны ниже:

1. Установка MAC адреса 08-C6-B3-11-11-11 PC1 как фильтруемого.

```
Switch(config)#mac-address-table static 08-C6-B3-11-11-11 discard vlan 1
```

2. Установка статической связи для PC2 и PC3 с портами 7 и 9 соответственно.

```
Switch(config)#mac-address-table static address 08-C6-B3-22-22-22 vlan 1
interface ethernet 1/0/7
Switch(config)#mac-address-table static address 08-C6-B3-33-33-33 vlan 1
interface ethernet 1/0/9
```

16.4 Устранение неисправностей, связанных с таблицей MAC адресов

Если при использовании команды show mac-address-table, было выяснено, что на порту произошел сбой обучения MAC адресам устройств, подключенных к нему. Возможные причины:

- ❖ Подключенный кабель поврежден;
- ❖ На порту включен Spanning Tree в статусе «discarding» или порт только что подключился и Spanning Tree пока в статусе вычисления дерева. Дождитесь, пока вычисление структуры закончится и порт обучится MAC адресу;
- ❖ Если проблемы, описанные выше, не обнаружены, проверьте порт коммутатора и свяжитесь с тех.поддержкой для решения проблемы.

16.5 Дополнительные функции таблицы MAC адресов

16.5.1 Привязка MAC адресов

16.5.1.1 Общие сведения о привязке MAC адресов

Большинство коммутаторов поддерживают режим обучения MAC адресам. Каждый порт может динамически запомнить несколько MAC адресов, таким образом возможна передача потоков данных между известными MAC адресами внутри порта. Если срок жизни MAC адреса истек, пакет, направленный на этот адрес, будет разослан широковещательно.

Другими словами, MAC-адрес, которому обучился порт, будет использоваться для передачи пакетов к этому порту. Если соединение переключено на другой порт,

коммутатор снова выполнит обучение MAC-адресу и будет передавать данные новому порту.

Однако, в некоторых случаях политика управления или секретности может требовать, чтобы MAC адреса были прикреплены к портам, и только потоки с привязанных MAC адресов будут пропускаться к пересылке на порт. То есть, после привязки MAC адреса к порту, в этот порт могут передаваться только данные, предназначенные для данного MAC адреса. Потоки данных, предназначенные для других MAC адресов, не привязанных к данному порту, не будут пропускаться через порт.

16.5.1.2 Настройка привязки MAC адресов

1. Включение функции привязки MAC адресов на порту;
2. Привязка MAC адреса к порту;
3. Конфигурация параметров функции привязанных MAC адресов;
4. Конфигурация ловушки для уведомлений о MAC адресах;

1. Включение функции привязки MAC адресов на порту

Команда	Описание
Режим конфигурирования порта	
switchport port-security **no switchport port-security**	Включение функции привязки MAC адреса на порту и фиксация порта. Когда порт зафиксирован, функция обучения MAC адресам выключена: Команда «no switchport port-security»выключает функцию привязки MAC адреса на порту и восстанавливает функцию обучения MAC адресам на порту

2. Фиксация MAC адреса на порту

Команда	Описание
Режим конфигурирования порта	
switchport port-security aging **no switchport port-security aging**	Включает функцию таймера фиксации порта; Команда «no switchport port-security aging» восстанавливает значение по умолчанию.
switchport port-security mac-address [<*mac-address*> | sticky] **no switchport port-security mac-address [<*mac-address*> | sticky]**	Добавляет статические безопасные MAC адреса; Команда «no switchport port-security mac-address» удаляет статические безопасные MAC адреса.

Режим администратора	
clear port-security dynamic [address <*mac-addr*> **| interface** <*interface-id*>]	Очищает динамические MAC адреса, выученные на указанном порту.

3. Конфигурация параметров привязки MAC адресов

Команда	Описание
Режим конфигурирования порта	
switchport port-security maximum <*value*> **no switchport port-security maximum** <*value*>	Устанавливает максимальное число безопасных MAC адресов на порту; команда «no switchport port-security maximum» восстанавливает значение по умолчанию.
switchport port-security violation {protect | restrict | shutdown} [recovery] **no switchport port-security violation**	Установка режима нарушения на порту; команда «no switchport port-security violation» восстанавливает значение по умолчанию.

16.5.1.3 Устранение проблем привязки MAC адресов

Включение привязки MAC адресов на порту может быть неудачным по нескольким причинам. Ниже приводится несколько возможных причин и их устранение:

❖ Если привязанный MAC адрес недоступен на порту, убедитесь, что порт не входит в port-aggregation и не сконфигурирован как транковый. Привязанный MAC адрес уникален в конкретной конфигурации. Если вы хотите привязать MAC адрес, функции, упомянутые выше, должны быть выключены.

❖ Если безопасный адрес установлен как статический адрес и удален, тогда этот безопасный адрес не может быть использован, хотя он и будет существовать. Исходя из этого, рекомендуется избегать назначения статических адресов для портов, для которых включена привязка MAC адресов.

16.6 Конфигурация MAC notification

16.6.1 Введение в MAC notification

Функция MAC notification предназначена для уведомления. Добавляя или удаляя MAC-адреса, а именно, когда добавляются или удаляются устройства, администратор будет уведомлен об изменениях с помощью snmp trap сообщений.

16.6.2 Конфигурация уведомлений о MAC-адресах

6. Настройка глобально snmp
7. Настройка глобального MAC notification
8. Настройка интервала для отправки MAC уведомлений
9. Настройка размера таблицы истории
10. Настройка типа ловушки MAC уведомлений, поддерживаемых портом

11. Просмотр конфигурации и данных MAC уведомлений
12. Очистка статистики MAC notification

1. Настройка глобального snmp trap MAC notification

Команда	Описание
Глобальный режим конфигурирования	
snmp-server enable traps mac-notification **no snmp-server enable traps mac-notification**	Включает/выключает глобально snmp MAC notification

2. Настройка глобального MAC notification

Команда	Описание
Глобальный режим конфигурирования	
mac-address-table notification **no mac-address-table notification**	Включает/выключает глобально MAC notification

3. Настройка интервала для отправки MAC уведомлений

Команда	Описание
Глобальный режим конфигурирования	
mac-address-table notification interval <0-86400> **no mac-address-table notification interval**	Настройка интервала для отправки MAC уведомлений, команда no восстанавливает настройки по умолчанию

4. Настройка размера таблицы истории

Команда	Описание
Глобальный режим конфигурирования	
mac-address-table notification history-size <0-500> **no mac-address-table notification history-size**	Настройка размера таблицы истории, команда no восстанавливает настройки по умолчанию

5. Настройка типа ловушки MAC уведомлений, поддерживаемых портом

Команда	Описание
Режим конфигурирования порта	
mac-notification {added | all | removed} **no mac-notification**	Настройка или стирание типа ловушки MAC уведомлений, поддерживаемых портом

6. Просмотр конфигурации и данных MAC уведомлений

Команда	Описание
Режим администратора	
show mac-notification summary	Просмотр конфигурации и данных MAC уведомлений

7. Очистка статистики ловушки MAC уведомлений

Команда	Описание
Режим администратора	
clear mac-notification statistics	Очистка статистики ловушки MAC уведомлений

16.6.3 Пример MAC notification

IP-адрес станции сетевого управления (NMS) 1.1.1.5, IP-адрес агента 1.1.1.9. NMS получит Trap сообщение от агента. (Примечание: NMS может установить проверку подлинности в строку характер ловушки)

Процедура конфигурации:

```
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
```

16.6.4 Устранение неисправностей MAC уведомлений

Убедитесь, что сообщение ловушки отправляется успешно командой show и отладкой команды snmp.

17 НАСТРОЙКА ПРОТОКОЛА MSTP

17.1 Общие сведения о MSTP

MSTP (Multiple STP) – новая реализация протокола spanning-tree, основанная на протоколах STP и RSTP. Он работает на любых коммутаторах локальных сетей. Он вычисляет общее и внутреннее связующее дерево (CIST - common and internal spanning tree) для всей сети, которое содержит устройства, поддерживающие MSTP, STP и RSTP. Он так же вычисляет независимые экземпляры множества связующих деревьев (MSTI - multiple spanning-tree instances) для каждой области MST (MSTP domain). В MSTP используется адаптированная версия протокола RSTP, обеспечивающего быструю сходимость при построении связующего дерева, при этом одному и тому же экземпляру связующего дерева может быть сопоставлено множество сетей VLAN. MSTP обеспечивает различные маршруты для передачи данных и позволяет балансировать трафик. Более того, так как множественные VLAN'ы используют один и тот же экземпляр связующего дерева, MSTP может уменьшать количество построенных деревьев, что позволяет уменьшить нагрузку на процессор и уменьшить служебную полосу на каналах.

17.1.1 Регион MSTP

Так как одному экземпляру связующего дерева может быть сопоставлено множество VLAN, комитет, разрабатывающий стандарт IEEE 802.1s предложил развить концепцию MST. MST используется для привязки конкретной VLAN к конкретному экземпляру связующего дерева.

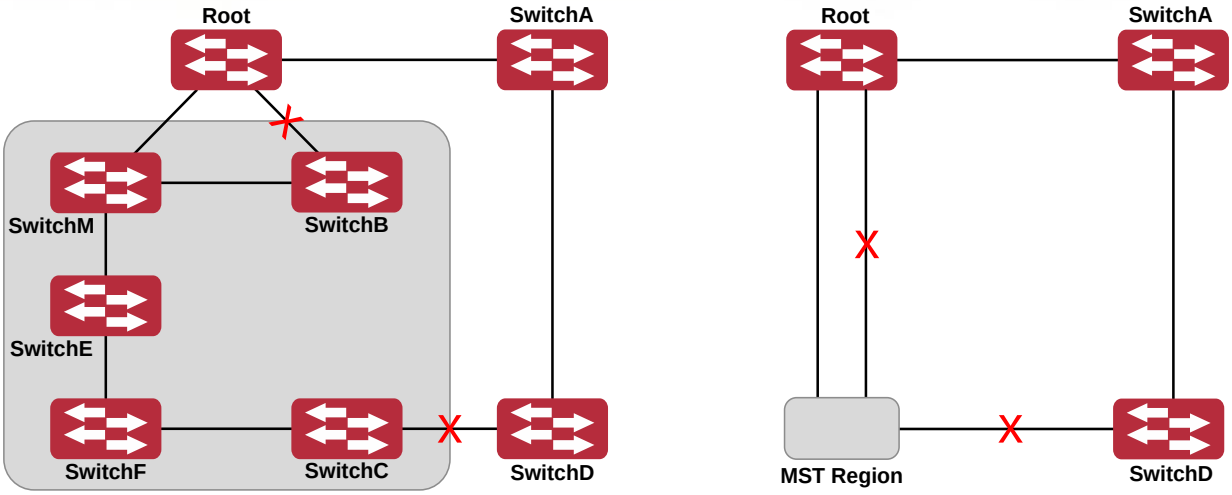
Регион MSTP состоит из одного или нескольких коммутаторов с одинаковым идентификатором MSID (MST Configuration Identification) и локальной сети (конкретный коммутатор в регионе MSTP является назначенным(designated) коммутатором локальной сети, на коммутаторах, закрепленных за локальной сетью, протокол STP не работает). Все коммутаторы в одном MSTP регионе имеют один MSID.

MSID содержит три атрибута:

- Конфигурационное имя: состоит из цифр и букв;
- Номер версии;
- Краткое описание конфигурирования: Сети VLAN, соответствующие экземплярам связующего дерева;

Коммутаторы с одинаковыми вышеописанными атрибутами считаются находящимися в одном регионе MST.

Когда MSTP вычисляет CIST в локальной сети с коммутаторами, регион MST рассматривается как один коммутатор. Рассмотрим рисунок ниже:



Пример CIST и региона MST

На схеме, если в одном коммутаторе используется STP, а в другом

RSTP, то порт между коммутатором M и коммутатором B должен быть блокирован. Однако, если в коммутаторах области, выделенной пунктиром, используется MSTP и сконфигурирован один и тот же регион MST, то протокол MSTP будет считать этот регион коммутатором. Поэтому блокирован один порт между коммутатором B и корневым узлом; кроме того, блокирован один порт коммутатора D.

17.1.1.1 Операции внутри одного и того же региона MSTP

Экземпляр связующего дерева (IST) связывает все коммутаторы MSTP региона. Когда IST сошелся, корневой узел IST становится управляющим узлом IST – в нем находится коммутатор с наименьшим ID моста и метрикой маршрута к корневому узлу CST. Если в сети имеется только один регион, управляющий узел IST одновременно является и корневым узлом CST. Если корневой узел CST находится вне региона, управляющим узлом IST является один из коммутаторов MSTP на границе региона.

При инициализации коммутатора MSTP он посылает пакеты BPDU, в которых объявляет себя корневым узлом CST и управляющим узлом IST, при этом метрики маршрута к этим узлам равны нулю. Кроме того, коммутатор инициализирует все свои экземпляры MST и объявляет себя корневым узлом. Если коммутатор принимает информацию от корневого узла MST верхнего уровня (с меньшим ID коммутатора, меньшей метрикой маршрута и т. д.), сохраненную для порта, он перестает объявлять себя управляющим узлом IST.

В регионе MST управляющий узел IST является единственным экземпляром связующего дерева, который принимает и посылает пакеты BPDU. Так как пакеты MST BPDU содержат информацию обо всех экземплярах, число таких пакетов, которое требуется обработать коммутатору для поддержки множества экземпляров связующего дерева, значительно уменьшается.

Все экземпляры MST одного и того же региона совместно используют одни и те же

таймеры протокола, однако каждый экземпляр MST имеет свои собственные параметры топологии, например ID корневого коммутатора, метрику маршрута к корневому узлу и т. д.

17.1.1.2 Операции между регионами MST

Если внутри сети существует несколько регионов или в ней уже существуют коммутаторы 802.1D, MSTP создает и обслуживает дерево CST, которое включает все регионы MST и все существующие коммутаторы с STP в сети. Для преобразования в дерево CST экземпляры MST комбинируются с IST на границе региона.

Экземпляр MSTI является истинным только внутри региона MST. Экземпляр MSTI никогда не совершает никаких действий с экземплярами MSTI других регионов MST. Коммутаторы в регионе MST принимают пакеты MST BPDU других регионов через граничные порты. Они могут только обрабатывать информацию, относящуюся к дереву CIST, и отбрасывают информацию MSTI.

17.1.2 Роли портов

Коммутатор MSTP присваивает портам роли, которые они должны играть в протоколе MSTP. Роли портов дерева CIST: Root Port, Designated Port, Alternate Port, Backup Port

Каждый порт MSTI имеет еще одну роль, более высшего порядка, чем вышеперечисленные роли: Master Port.

Роли портов в дереве CIST (Root Port, Designated Port, Alternate Port, Backup Port) — такие же, что и при протоколе RSTP.

17.1.3 Балансировка нагрузки в MSTP

В регионе MSTP сети VLAN могут быть привязаны к различным экземплярам, что может формировать различные топологии. Каждый экземпляр независим друг от друга и это позволяет им иметь собственные атрибуты, такие как приоритет устройства и метрику порта.

Следовательно, сети VLAN различных экземпляров имеют свои собственные маршруты. Для трафика сетей VLAN таким образом поддерживается балансировка нагрузки.

17.2 Конфигурирование MSTP

1. Включение протокола MSTP и установка рабочего режима;
2. Настройка параметров экземпляров связующего дерева;
3. Настройка параметров регионов MSTP;
4. Настройка временных параметров MSTP;
5. Настройка функции быстрой миграции MSTP;
6. Настройка формата пакетов на порту;
7. Настройка атрибутов связующего дерева на порту;
8. Настройка атрибутов snooping-ключа аутентификации;
9. Настройка режима FLUSH для изменений топологии;

1. Включение протокола MSTP и установка рабочего режима

Команда	Описание
Режим глобального конфигурирования и режим конфигурирования порта	
spanning-tree **no spanning-tree**	Включение/выключение MSTP
Режим глобального конфигурирования	
spanning-tree mode {mstp|stp|rstp} **no spanning-tree mode**	Установка рабочего режима MSTP.
Режим конфигурирования порта	
spanning-tree mcheck	Принудительно устанавливает для порта режим работы по протоколу MSTP

2. Настройка параметров экземпляров связующего дерева;

Команда	Описание
Режим глобального конфигурирования	
spanning-tree mst <instance-id> **priority** <bridge-priority> **no spanning-tree mst** *<instance-id>* **priority**	Позволяет задать приоритет коммутатора для указанного экземпляра связующего дерева.
spanning-tree priority *<bridge-priority>* **no spanning-tree priority**	Позволяет настроить приоритет связующего дерева на коммутаторе.
Режим конфигурирования порта	
spanning-tree mst *<instance-id>* **cost** *<cost>* **no spanning-tree mst** *<instance-id>* **cost**	Для указанного экземпляра связующего дерева позволяет установить метрику маршрута к порту.
spanning-tree mst *<instance-id>* **port-priority** *<port-priority>* **no spanning-tree mst** *<instance-id>* **port-priority**	Позволяет задать приоритет порта для указанного экземпляра связующего дерева.
spanning-tree mst *<instance-id>* **rootguard** **no spanning-tree mst** *<instance-id>* **rootguard**	Для указанного экземпляра связующего дерева позволяет задать защищенный корневой узел. Порты, для которых установлена защита, не могут быть преобразованы в корневые порты других типов.

spanning-tree rootguard **no spanning-tree rootguard**	Для текущего порта задает режим защищенного корневого порта в экземпляре связующего дерева0. Сконфигурированный защищенный порт не может быть преобразован в корневой порт других типов.
spanning-tree [mst <instance-id>] loopguard **no spanning-tree [mst <instance-id>] loopguard**	Включение функции отслеживания петли в конкретном частном дереве. Команда NO отключает данную функцию.

3. Настройка параметров регионов MSTP

Команда	Описание
Режим глобального конфигурирования	
spanning-tree mst configuration **no spanning-tree mst configuration**	Вход в режим конфигурирования региона MSTP. Команда NO возвращает значение по умолчанию.
Режим конфигурирования региона MSTP	
show	Показывает информацию о текущей рабочей системе.
instance <instance-id> **vlan** <vlan-list> **no instance** <instance-id> **[vlan <vlan-list>]**	Позволяет создать экземпляр связующего дерева и установить соответствие между VLAN и этим экземпляром
name <name> **no name**	Позволяет задать имя региона MSTP
revision-level *<level>* **no revision-level**	Позволяет задать номер ревизии конфигурирования регионаMSTP
abort	Выход из режима конфигурирования региона MSTP и возврат в режим глобального конфигурирования без сохранения конфигурации региона MSTP.
exit	Позволяет сохранить сделанные настройкм региона MSTP, выйти из режима настройки регионов MSTP и вернуться в глобальный режим конфигурирования.

no	Отмена одной команды или установка первоначального значения

4. Настройка временных параметров MSTP

Команда	Описание
Режим глобального конфигурирования	
spanning-tree forward-time *<time>* **no spanning-tree forward-time**	Позволяет задать время задержки передачи на коммутаторе
spanning-tree hello-time *<time>* **no spanning-tree hello-time**	Установка времени Hello для посылки сообщений BPDU.
spanning-tree maxage *<time>* **no spanning-tree maxage**	Установки времени жизни сообщений BPDU
spanning-tree max-hop *<hop-count>* **no spanning-tree max-hop**	Установка максимального числа хопов для сообщений BPDU в регионе MSTP.

5. Настройка функции быстрой миграции MSTP

Команда	Описание
Режим конфигурирования порта	
spanning-tree link-type p2p {auto|force-true|force-false} **no spanning-tree link-type**	Установка типа линии порта
spanning-tree portfast [bpdufilter|bpduguard] [recovery <30-3600>**]** **no spanning-tree portfast**	Позволяет задать порт, как граничный. Опция Bpdufilter служит для отбрасывания принятых сообщений BPDU. Опция bpduguard при приеме сообщения BPDU закрывает порт. Параметр no выключает режим пограничного порта, происходит преобразование в порт, который не находится на границе

6. Настройка формата пакетов на порту

Команда	Описание
Режим конфигурирования порта	
spanning-tree format standard **spanning-tree format privacy**	Позволяет настроить формат пакета связующего дерева порта. При выборе

spanning-tree format auto **no spanning-tree format**	опции standard пакет соответствует стандартам IEEE, при опцииprivacy пакет совместим с CISCO, auto означает, что формат определяется по принятому пакету

7. Настройка атрибутов связующего дерева на порту

Команда	Описание
Режим конфигурирования порта	
spanning-tree cost **no spanning-tree cost**	Позволяет задать метрику маршрута к порту
spanning-tree port-priority **no spanning-tree port-priority**	Позволяет задать приоритет порта
spanning-tree rootguard **no spanning-tree rootguard**	Позволяет установить порт, как не корневой
Режим глобального конфигурирования	
spanning-tree transmit-hold-count <tx-hold-count-value> **no spanning-tree transmit-hold-count**	Установка максимального значения счетчика задержки передачи на порту
spanning-tree cost-format {dot1d | dot1t}	Устанавливает формат метрики маршрута dot1d или dot1t

8. Настройка атрибутов snooping-ключа аутентификации

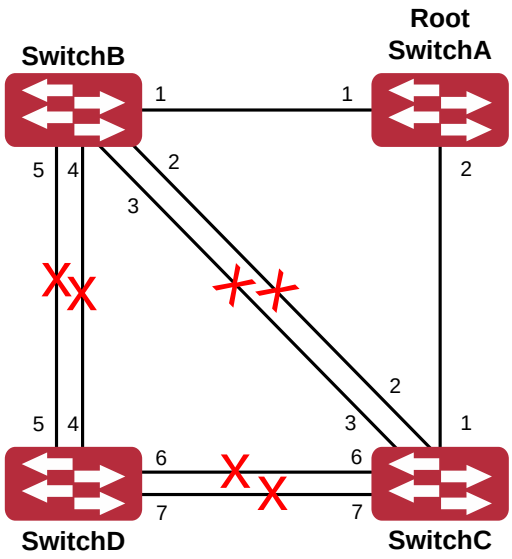
Команда	Описание
Режим конфигурирования порта	
spanning-tree digest-snooping **no spanning-tree digest-snooping**	Позволяет порту использовать строку аутентификации партнерского порта. Команда NO восстанавливает использование сгенерированной строки.

9. Настройка режима FLUSH для изменений топологии

Команда	Описание
Режим глобального конфигурирования	
spanning-tree tcflush {enable| disable| protect} **no spanning-tree tcflush**	Enable: связующее дерево строится сразу при изменении топологии;

	Disable: связующее дерево не строится при изменении топологии; Protect: связующее дерево строится раз в десять секунд; Команда no восстанавливает значение по умолчанию — изменение при изменении топологии.
Режим конфигурирования порта	
spanning-tree tcflush {enable| disable| protect} **no spanning-tree tcflush**	Позволяет настроить режим flush для порта. Команда no восстанавливает использование общих настроек режима на устройстве.

17.3 Пример применения MSTP



Типичный сценарий применения MSTP

Соединения между коммутаторами показаны на рисунке выше. Все коммутаторы работают в MSTP режиме по умолчанию. Их приоритеты мостов, приоритеты портов и стоимость маршрутов для портов стоят по умолчанию (равны). Параметры по умолчанию для коммутаторов показана ниже:

Имя моста		SwitchA	SwitchB	SwitchC	SwitchD
Bridge MAC Address		00-00-01	00-00-02	00-00-03	00-00-04
Bridge Priority		32768	32768	32768	32768
Port Priority	Port 1	128	128	128	
	Port 2	128	128	128	
	Port 3		128	128	
	Port 4		128		128
	Port 5		128		128
	Port 6			128	128
	Port 7			128	128
Route Cost	Port 1	200000	200000	200000	
	Port 2	200000	200000	200000	
	Port 3		200000	200000	
	Port 4		200000		200000
	Port 5		200000		200000
	Port 6			200000	200000
	Port 7			200000	200000

По умолчанию протокол MSTP создает топологию дерева с корнем на коммутаторе 1.

Порты, обозначенные «x» имеют состояние discarding (блокированы), на остальных портах передача разрешена.

Этапы настройки:

Шаг 1. Настройка привязки портов к VLAN:

- ❖ Создать VLAN 20, 30, 40, 50 на SwitchB, SwitchC и SwitchD;
- ❖ Настроить порты 1-7 как транковые на SwitchB, SwitchC и SwitchD;

Шаг 2. Установить SwitchB, SwitchC и SwitchD как принадлежащих одному дереву MSTP:

- ❖ Установить на SwitchB, SwitchC и SwitchD одно и то же имя региона, совпадающее с именем дерева mstp;
- ❖ Привязать VLAN 20 и VLAN 30 на SwitchB, SwitchC и SwitchD к экземпляру

связующего дерева 3;

❖ Приписать VLAN 40 и VLAN 50 на SwitchB, SwitchC и SwitchD к экземпляру связующего дерева 4;

Шаг 3. Настроить SwitchC как корневой коммутатор для экземпляра связующего дерева 3. Настроить SwitchD как корневой коммутатор для экземпляра связующего дерева 4:

❖ Настроить приоритет коммутатора для экземпляра связующего дерева 3 на SwitchC как 0;

❖ Настроить приоритет коммутатора для экземпляра связующего дерева 4 на SwitchD как 0.

Детальная конфигурация приведена ниже:

SwitchB:

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

SwitchC:

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

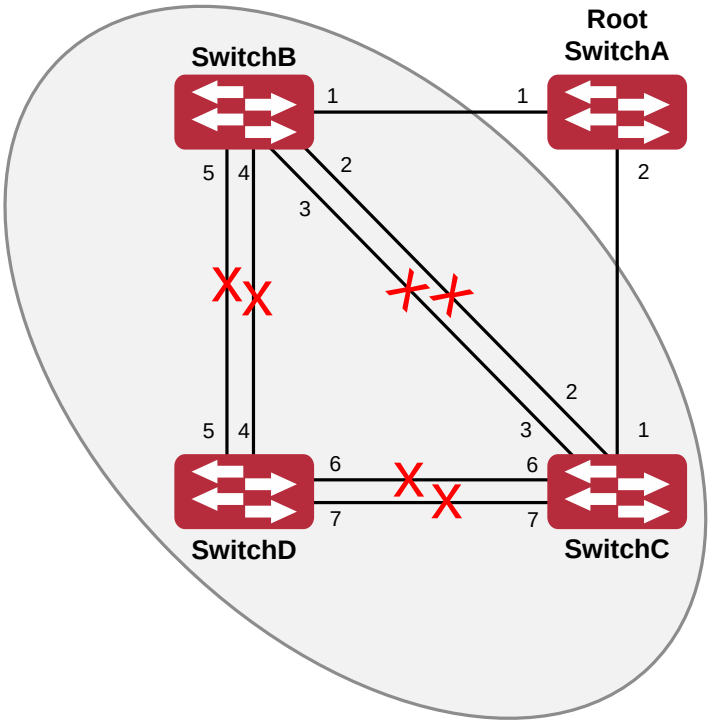
SwitchD:

```
SwitchD(config)#vlan 20
SwitchD(Config-Vlan20)#exit
SwitchD(config)#vlan 30
SwitchD(Config-Vlan30)#exit
SwitchD(config)#vlan 40
```

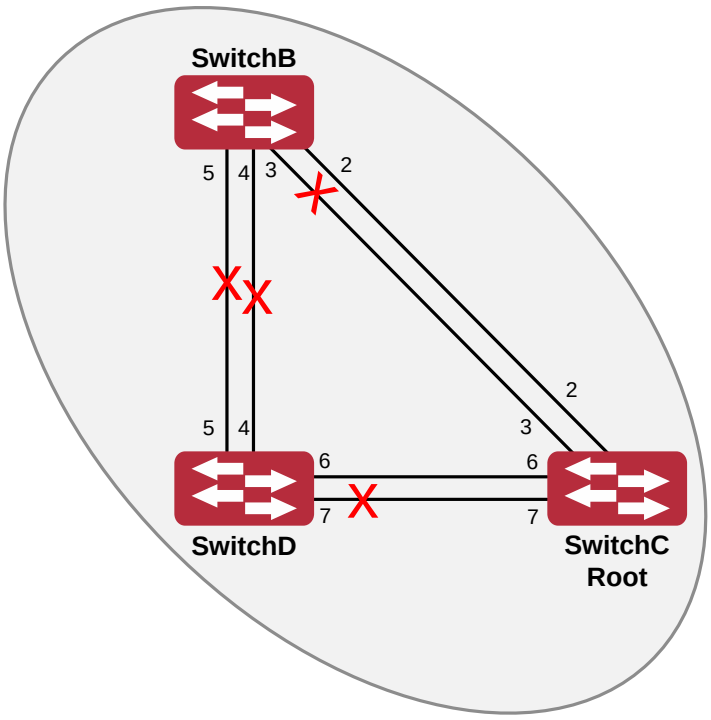
```
SwitchD(Config-Vlan40)#exit
SwitchD(config)#vlan 50
SwitchD(Config-Vlan50)#exit
SwitchD(config)#spanning-tree mst configuration
SwitchD(Config-Mstp-Region)#name mstp
SwitchD(Config-Mstp-Region)#instance 3 vlan 20;30
SwitchD(Config-Mstp-Region)#instance 4 vlan 40;50
SwitchD(Config-Mstp-Region)#exit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

После описанной выше настройки, SwitchA будет корневым коммутатором экземпляра связующего дерева 0. В регионе MSTP, к которому относятся SwitchB, SwitchC и SwitchD, SwitchB является корневым коммутатором региона для экземпляра связующего дерева 0, SwitchC является корневым коммутатором региона для экземпляра связующего дерева 3 и SwitchD является корневым коммутатором региона для экземпляра связующего дерева 4. Трафик VLAN 20 и 30 передается через топологию экземпляра связующего дерева 3. Трафик VLAN 40 и 50 передается через топологию экземпляра связующего дерева 4. Трафик с остальных VLAN передается через топологию экземпляра связующего дерева 0. Порт 1 на SwitchB является управляющим портом для экземпляров связующих деревьев 3 и 4.

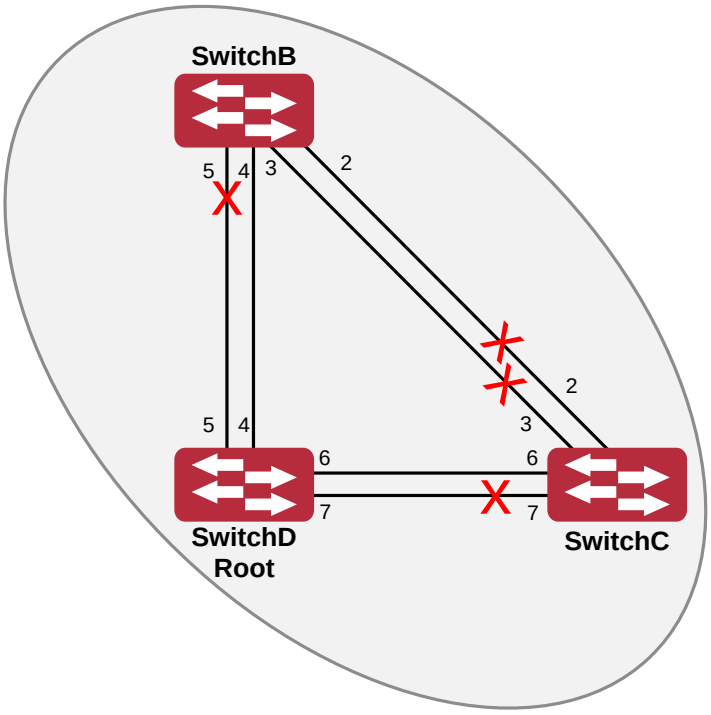
Протокол MSTP путем вычислений генерирует 3 топологии: экземпляров связующих деревьев 0, 3 и 4. Порты, обозначенные «x» имеют состояние discarding (блокированы). На остальных портах передача разрешена.



Топология экземпляра связующего дерева 0 после вычисления MSTP



Топология экземпляра связующего дерева 3 после вычисления MSTP



Топология экземпляра связующего дерева 4 после вычисления MSTP

17.4 Устранение неисправностей MSTP

Для того, чтобы протокол MSTP на порте смог работать, MSTP должен быть включен в режиме глобального конфигурирования.

Так как параметры MSTP взаимосвязаны, они должны соответствовать следующим требованиям:

- 2×(Bridge_Forward_Delay - 1.0 секунда) >= Bridge_Max_Age;
- Bridge_Max_Age >= 2×(Bridge_Hello_Time + 1.0 секунда);

В противном случае протокол MSTP может работать неправильно.

Если пользователи изменили параметры MSTP, они должны удостовериться в том, что изменены и топологии. Настройки глобального режима конфигурирования выполняются для коммутаторов. Остальные настройки выполняются для отдельных экземпляров связующего дерева.

18 НАСТРОЙКА QOS

18.1 Общие сведения о QoS

QoS (Quality of Service – качество сервиса) - набор возможностей которые позволяют создавать разделенные полосы для передаваемых по сети данных, тем самым обеспечивая лучший сервис для выбранного сетевого трафика. QoS - гарантия качества последовательной и предсказуемой передачи данных для обеспечения требований программ. QoS не создает дополнительной полосы передачи, но обеспечивает более эффективное управление полосой в соответствии с требованиями приложений и политикой управления сетью.

18.1.1 Термины QoS

QoS: Качество сервиса, обеспечение гарантированного качества сервиса для последовательной и предсказуемой передачи данных и выполнения требований программ.

Домен QoS: Домен QoS поддерживает устройства с QoS для формирования сетевой топологии, которая обеспечит качество сервиса. Такая топология называется доменом QoS.

CoS: Класс сервиса - классификационная информация, передаваемая фреймами 802.1Q на втором уровне. Занимает три бита поля Tag в заголовке фрейма и называется уровнем пользовательского приоритета в диапазоне от 0 до 7.

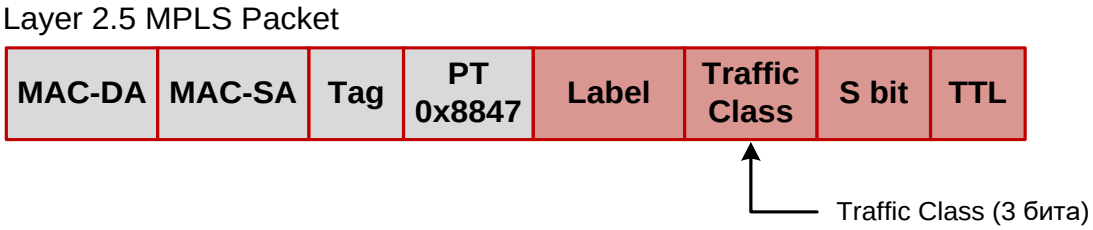
ToS: Тип сервиса. Однобайтовое поле, передаваемое в заголовке пакета IPv4 на третьем уровне для объявления типа сервиса IP пакета. Значением поля ToS может быть приоритет IP (IP Precedence) или значение DSCP.

IP Precedence: Приоритет IP. Классификационная информация передающаяся в заголовке пакета третьего уровня, занимающая 3 бита и могущая принимать значения от 0 до 7.

DSCP (Differentiated Services Code Point): коды разделенных сервисов, классификационная информация, передающаяся в заголовке IP пакета третьего уровня, занимает 6 бит, имеет значение от 0 до 63 и обратно совместима с приоритетом IP.

MPLS TC(EXP):

Поле MPLS означает класс обслуживания, имеет 3 бита для диапазона от 0 до 7.



Internal Priority: Внутренний приоритет, устанавливаемый процессором коммутатора. Возможный диапазон значений зависит от типа процессора. Сокращенно - Int-Prio или IntP.

Drop Precedence: Приоритет сброса. При обработке пакетов первыми сбрасываются пакеты с большим приоритетом сброса. Имеет значение 0 или 1. Сокращенно обозначается Drop-Prec или DP.

Classification: основное назначение механизма QoS, классифицирует передаваемые пакеты в соответствии с классификационной информацией, содержащейся в пакетах и списками контроля доступа(ACL).

Policing: действие механизма QoS на входе, которое устанавливает политики трафика и управляет классифицированными пакетами.

Remark: действие механизма QoS на входе, выполняющее пропуск, остановку или сброс пакета в соответствии с политиками трафика.

Scheduling: действие механизма QoS на выходе. Добавляет пакеты в соответствующие исходящие очереди основываясь на внутреннем приоритете. И принимает решение о посылке или сбросе пакетов в соответсвии с приоритетом сброса, алгоритмом посылки и важностью соответствующей очереди в исходящем потоке.

In-Profile: Траффик в рамках политики QoS(полоса пропускания или дополнительной полосой) называется In-Profile.

Out-of-Profile: Траффик в рамках политики QoS(полосы пропускания или дополнительной полосы) называется Out-of-Profile.

18.1.2 Реализация QoS

Для выполнения на коммутаторе программного QoS необходимо рассмотреть основную базовую модель. QoS не создает новой полосы в канале, но может максимально подстраивать конфигурацию текущих канальных ресурсов. Полная реализация QoS дает возможность полностью управлять сетевым трафиком. Ниже, как можно точнее, описывается сам принцип QoS.

Спецификация передачи данных в IP покрывает только адресацию и сервисы источника и приемника и, конечно, коррекцию передачи пакетов с помощью протоколов 4 уровня модели OSI и выше, таких как TCP. Однако, в большинстве случаев протокол IP использует максимально возможную пропускную способность вместо механизма поддержки и защиты полосы пакетной передачи. Это применимо для таких сервисов как почта и FTP, но при увеличении передачи мультимедийных коммерческих данных и

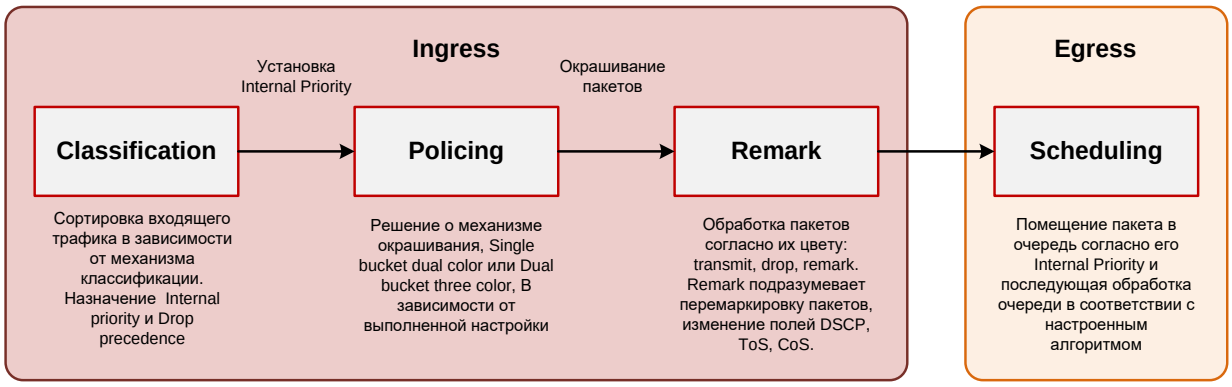
электронных бизнес-сервисов, метод максимальной загрузки не может удовлетворить требования необходимой полосы и низких задержек.

Базируясь на различных методах, QoS определяет приоритет для каждого входящего пакета. Классификационная информация содержится в заголовках IP пакетов третьего уровня и в заголовках фреймов 802.1Q второго уровня. QoS обеспечивает одинаковый сервис для пакетов одинакового приоритета, в то время как для пакетов с различающимися приоритетами предлагаются различающиеся операции. Маршрутизатор или коммутатор, поддерживающие сервис QoS, могут обеспечивать различную полосу передачи в соответствии с классификацией пакетов, помечать пакеты в соответствии с сконфигурированными политиками, а также сбрасывать некоторые низкоприоритетные пакеты в случае перегрузки полосы передачи.

Конфигурация QoS является гибкой, более простой или сложной в зависимости от топологии сети и устройств, а также глубины анализа входящего/исходящего трафика.

18.1.3 Базовая модель QoS

Базовая модель QoS состоит из 4 частей: Классификация, Применение политик, Пометка и Планирование, где классификация, применение политик и пометки – последовательные действия на входе, а работа с очередями и планирование – действия QoS на выходе.



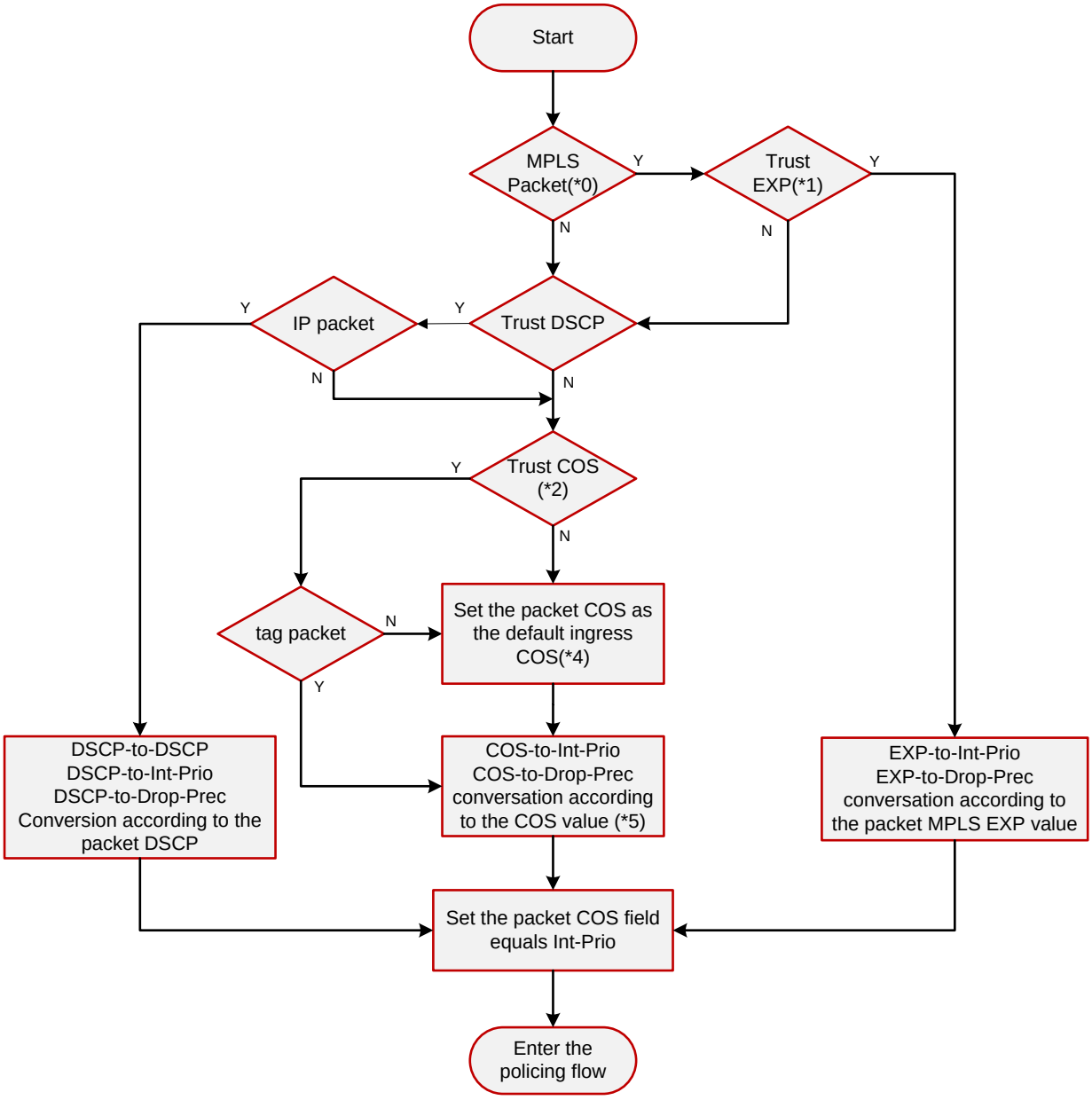
Базовая модель QoS

Классификация: классифицирует трафик в соответствии с классификационной информацией пакетов и генерирует значение внутреннего приоритета, основанное на классификационной инфрмации. Для различных типов пакетов классификация обеспечивается различным образом. Схема ниже показывает это.

Применение политик и пометка: Каждый пакет в классифицированном входящем трафике получает значение внутреннего приоритета и может далее подвергаться действию политик и помечаться.

Применение политик может быть выполнено на потоке данных для обеспечения различной полосы пропускания для различных классов трафика. Назначенная пропускная политика может быть «одна корзина-два цвета» (single bucket dual color) или «две корзины-три цвета» (dual bucket three color). Трафику присваиваются различные цвета и в соответствии с ними он может сбрасываться или пропускаться. К пропущенным пакетам применяется действие пометки, когда пакету назначается новый, более низкий

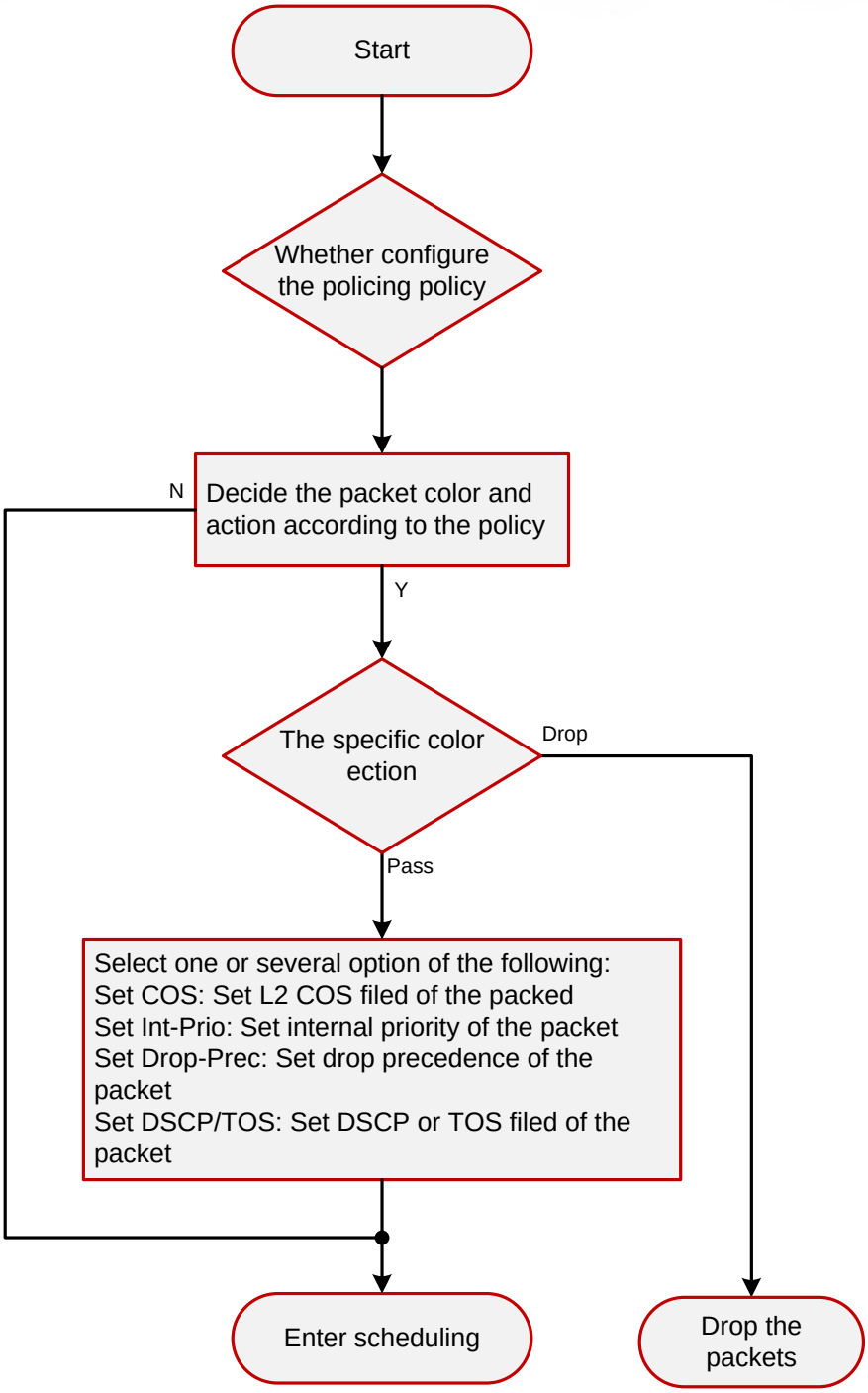
внутренний приоритет для замены существовавшего ранее более высокого внутреннего приоритета. Поля COS и DSCP будут модифицированы в соответствии с новым внутренним приоритетом на выходе. Следующая схема описывает эти операции.



Процесс классификации

Замечание 1: Значение CoS рассчитывается исходя из свойств пакета и никак не связано со значением внутреннего приоритета, полученным для потока.

Замечание 2: Если одновременно сконфигурированы проверка DSCP и CoS, то приоритет DSCP важнее COS.

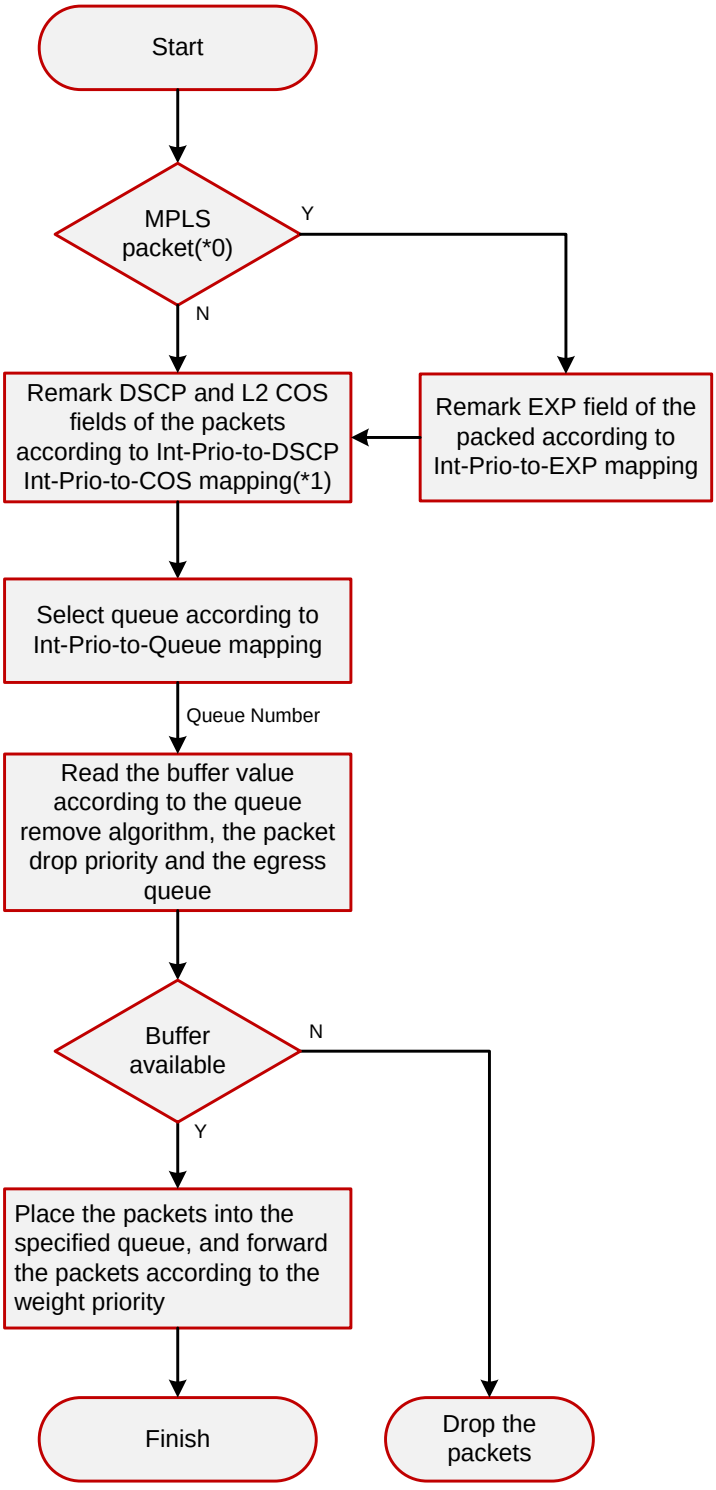


Процессы Регулирования и пометки

Замечание 1. Внутренний приоритет будет скрыт после установки. Установка внутреннего приоритета на трафик с определенным цветом покрывает установку внутреннего приоритета на трафик, не связанный с цветом.

Замечание 2. Сброс внутреннего приоритета пакетов осуществляется в соответствии с картой преобразования «внутренний приоритет - внутренний приоритет» (IntP-to-IntP). При классификации потока внутренний приоритет берется от источника или устанавливается действиями, не связанными с цветом.

Работа с очередями и планирование: существует внутренний приоритет для исходящих пакетов, в соответствии с ним планируется распределение пакетов по очередям с различным приоритетом и пакеты посылаются в соответствии с весовым приоритетом очереди и приоритетом сброса. Следующая схема описывает операции планирования.



Процессы планировки и управления очередями

18.2 Конфигурирование QoS

1. Конфигурирование карты классов;

Устанавливает классификационные правила в соответствии с ACL, CoS, VLAN ID, приоритетом IPv4, DSCP и IPv6 FL для классификации потока данных. Различные классы потоков данных обрабатываются по разным политикам.

2. Конфигурирование карты политик;

После классификации потока данных может быть создана карта политик, для связи с картой классов, созданной ранее и входом в режим класса. Тогда различные политики (такие как ограничение полосы, понижение приоритета назначением нового значения DSCP) могут применяться для различный потоков данных. Также можно определить набор политик, которые могут применяться для нескольких классов в карте политик.

3. Применение QoS на порту или VLAN интерфейсе;

Конфигурирование доверительного режима (trust mode) на порту или привязка политик к порту. Политики будут задействованы на порту только если они будут привязаны к нему. Политики так же могут быть привязаны к определенному VLAN. Не рекомендуется одновременно использовать карту политик на VLAN и на ее портах, в противном случае приоритет карты политик на порту будет выше.

4. Конфигурирование алгоритма управления очередями;

Конфигурирование алгоритма управления очередями, такого как sp, wdrr и других.

Конфигурирование распределения QoS.

Конфигурирование распределения из CoS в DP, из DSCP в DSCP, из IntP в DSCP.

1. Конфигурирование карты классов.

Команда	Описание
Режим глобального конфигурирования	
class-map <class-map-name> **no class-map** <class-map-name>	Создание карты классов и вход в режим карты классов; команда «**no class-map** <class-map-name>» удаляет указанную карту классов.
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}**	Установка согласованных критериев (классификация потока данных по ACL, CoS, VLAN ID, приоритетом IPv4, IPv6 FL или DSCP, и т.д.) для карты классов; команда No удаляет определенный согласованный критерий.

2. Конфигурирование карты политик

Команда	Описание
Режим глобального конфигурирования	
policy burst {1 | 2} <committed-burst-size>	Создание профиля ограничения всплесков траффика для последующий настройки policier.
policy-map <policy-map-name> **no policy-map** <policy-map-name>	Создание карты политик и вход в режим карты политик; команда NO удаляет определенную карту политик.
class *<class-map-name>* **[insert-before** <class-map-name>**]** **no class** <class-map-name>	После создания карты политик, ее можно связать с классом. Различные политики или новые значения DSCP могут быть применены к различным потокам данных в режиме классов; команда NO удаляет определенный класс.
set {ip dscp <new-dscp> | ip precedence <new-precedence> | internal priority <new-inp> | drop precedence <new-dp> | cos <new-cos>} **no set {ip dscp | ip precedence | internal priority | drop precedence |cos}**	Присваивает новый внутренний приоритет классифицированному трафику; Команда NO отменяет назначение новой величины.
policy <CIR_Kbits_per_second> burst-group <bucket_size_profile_ID> **no policy**	Конфигурация политики для классифицированного потока. Отдельные команды политик поддерживают три цвета. Анализирует рабочий режим виртуальной корзины, это может быть одна скорость-одна корзина, одна скорость — две корзины, две скорости — две корзины. Устанавливает соответствующие действия для различных цветов пакетов. Команда NO удаляет режим конфигурации.
accounting **no accounting**	Установка функции статистики для классифицированного трафика. После включения этой функции в режиме политики классов, добавляет статистику трафика по карте политики классов. В режиме одной корзины пакет может быть только зеленым или

	красным при применении политики. В выводимой информации будут два цвета (красный и зеленый) пакетов. В режиме двух корзин будут три цвета (зеленый, красный и желтый) пакетов.
Режим конфигурации карты политик классов	
drop **no drop** **transmit** **no transmit**	Сбрасывает или передает трафик в данном классе. Команда NO отменяет присвоенную функцию.

3. Применение QoS на порту или VLAN интерфейсе

Команда	Описание
Режим конфигурирования интерфейса	
mls qos trust dscp **no mls qos trust dscp**	Конфигурирование доверительного порта. Команда NO отменяет текущий режим доверительности на порту.
mls qos cos {*<default-cos>***}** **no mls qos cos**	Конфигурация значения CoS по умолчанию на порту; команда NO восстанавливает значение по умолчанию.
service-policy input *<policy-map-name>* **no service-policy input** *<policy-map-name>*	Применяет карту политик к конкретному порту; Команда NO удаляет соответствующую карту политик, примененную на порту. Выходная карта политик пока не поддерживается.
Режим глобального конфигурирования	
service-policy input <policy-map-name> **vlan** <vlan-list> **no service-policy input** <policy-map-name> **vlan** <vlan-list>	Применяет карту политик к конкретному VLAN интерфейсу. Команда NO удаляет соответствующую карту политик, примененную на VLAN интерфейсе.

4. Конфигурирование алгоритма управления очередями

Команда	Описание

Режим конфигурирования порта	
mls qos queue algorithm {sp | wrr | wdrr} **no mls qos queue algorithm**	Установка алгоритма управления очередями. По умолчанию алгоритм - wdrr
Режим глобального конфигурирования	
mls qos queue {wrr | wdrr} weight <weight0..weight3> **no mls qos queue weight**	Устанавливает вес очередей wdrr для всех портов. По умолчанию веса очередей 1 2 3 4

5. Конфигурирование преобразования QoS

Команда	Описание
Режим глобального конфигурирования	
mls qos map {cos-intp <intp1…intp8> | dscp-intp <in-dscp list> to <intp>} **no mls qos map {cos-intp | dscp-intp}**	Устанавливает приоритетную трансляцию для QoS. Команда NO восстанавливает значение трансляции по умолчанию

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

Команда	Описание
Режим администратора	
clear mls qos statistics [interface <interface-name> **| vlan** <vlan-id>**]**	Очистка счетчиков данных в карте политик на определенном порту или VLANe. Если у команды нет параметров, очищаются счетчики у всех карт политик.

7. Просмотр конфигурации QoS

Команда	Описание
Режим администратора	
show mls qos maps [cos-dp | dscp-dscp | dscp-intp | dscp-dp | intp-dscp]	Показывает конфигурацию QoS трансляции
show class-map [<class-map-name>**]**	Показывает карту классов QoS
show policy-map [<policy-map-name>**]**	Показывает карту политик QoS.

show mls qos {interface [<interface-id>**] [policy | queuing] | vlan** <vlan-id>**}**	Показывает конфигурацию QoS на порту.

18.3 Пример QoS

Пример 1:

Необходимо включить функцию QoS, изменить веса выходных очередей на порту Ethernet 1/0/1 на 1:1:2:2:4:4:8:8, также установить на порту режим доверительного CoS без изменения значения DSCP и установить значение CoS по умолчанию равным 5.

Этапы конфигурирования описаны ниже:

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

Результат конфигурации:

Когда в общем режиме включен QoS, для выходных очередей полоса пропускания для каждого порта поделена в пропорции 1:1:2:2:4:4:8:8. Когда пакеты, имеющие параметр CoS, приходят через порт ethernet 1/0/1 им назначается внутренний приоритет в соответствии со значением CoS. Значения CoS от 1 до 7 соответствуют очередям 1,2,3,4,5,6,7.8 соотвественно. Если входящий пакет не имеет установленного параметра CoS, он по умолчанию считается равным 5 и пакет помещается в очередь 6. Во всех проходящих пакетах значение DSCP не меняется.

Пример 2:

На порту Ethernet 1/0/2 необходимо установить полосу для пакетов из сегмента 192.168.1.0 в 10 Мб/с с дополнительной полосой в 4 Мб. Все пакеты, превышающие эту полосу, будут сброшены.

Этапы конфигурации показаны ниже:

```
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 burst 1 4000
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
```

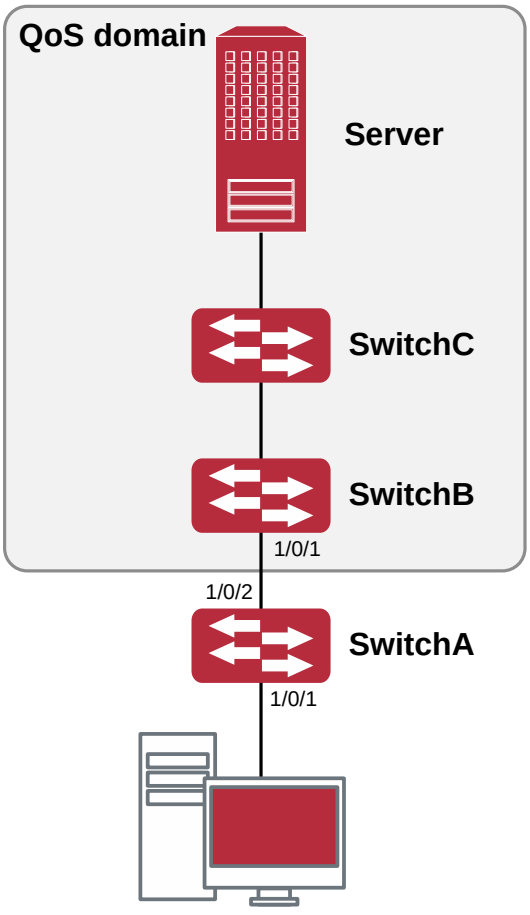
Результат конфигурации:

Лист доступа с именем 1 настроен для выборки сегмента 192.168.1.0. Функция QoS включена глобально. Создана карта классов с именем c1, лист ACL 1 включен в карту классов. Создана группа burst 1 определяющая максимальный всплеск траффика, превышающего гарантированную полосу CIR. Создана другая карта политик с именем p1. Карта p1 ссылается на карту c1. Установлены соответствующие политики для ограничения полосы и дополнительных расширений. Эта карта политик применена на порту ethernet

1/0/2. После того, как вышеуказанные настройки сделаны, полоса для пакетов из сегмента 192.168.1.0, проходящих через порт Ethernet 1/0/2, установлена в 10 Мб/с с дополнительным расширением в 4 Мб. Все пакеты, превышающие данные установки в данном сегменте, будут отброшены.

Пример 3:

Как показано на рисунке, внутри отмеченной области, находится QoS домен, SwitchA классифицирует различный трафик и назначает различные приоритеты IP. Для примера, установим приоритет CoS для пакетов из сегмента 192.168.1.0 равным 5 на порту ethernet1/0/1 (установим внутренний приоритет равным 40 и по умолчанию трансляцию внутреннего приоритета в dcsp как 40-40, соответствующий IP приоритет равным 5). Порт, подключенный к SwitchB – транковый. На SwitchB порт Ethernet 1/0/1, подключенный к SwitchA настроен как доверительный dscp. Таким образом внутри области QoS пакеты с различными приоритетами будут распределяться в различные очереди и получать соответствующую полосу передачи.



Типовая топология QoS

Этапы конфигурации описаны ниже:

Конфигурация QoS на SwitchA:

```
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 40
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
```

Конфигурация QoS на SwitchB:

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

18.4 Устранение неисправностей QoS

- ❖ доверительный режим cos и EXP может использоваться с другими доверительными режимами или картой политик;
- ❖ доверительный режим dscp может использоваться с другими доверительными режимами или картой политик. Эта конфигурация применяется для пакетов IPv4 и IPv6;
- ❖ Доверительные режимы exp, dscp и cos могут быть сконфигурированы одновременно. Приоритеты по старшинству: EXP>DSCP>COS;
- ❖ 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 политики может быть привязана только ко вхдящему направлению, выходящее направление не поддерживается;
- ❖ В настоящее время не рекомендуется одновременно использовать карты политик на VLAN и на его порту.

19 ПЕРЕНАПРАВЛЕНИЕ ПОТОКОВ

19.1 Общие сведения о перенаправлении потоков

Функция перенаправления потоков позволяет коммутатору передавать фреймы данных, применяя некие условия (определяемые ACL) на другой порт. Фреймы со специальными условиями называются классом потока, входящий порт данных называется портом источника перенаправления, а определенный выходной порт — портом приемника перенаправления. Обычно есть два вида применения перенаправления потоков: 1) Подключение анализатора потока (например, сниффера) или удаленного монитора к порту приемнику перенаправления для контроля и управления сетью, а также диагностики проблем на сети; 2) Специальные правила передачи для специальных типов фреймов данных.

Коммутатор может назначать только один порт - приемник для одинаковых классов потоков на порту-источнике, в то время как для различных классов потоков на порту источнике можно назначить различные порты - приемники. Одинаковый класс потока может применяться на различных портах - источниках.

19.2 Конфигурирование перенаправления потоков

1. Конфигурирование перенаправления потоков;
2. Проверка текущей конфигурации перенаправления потоков;

1. Конфигурирование перенаправления потоков

Команда	Описание
Режим конфигурирования порта	
access-group <*aclname*> **redirect to interface [ethernet** <*IFNAME*>**|**<*IFNAME*>**]** **no access-group** <*aclname*> **redirect**	Определение перенаправления потоков на порту; команда «**no access-group** <aclname> **redirect**» используется для удаления перенаправления потоков.

2. Проверка текущей конфигурации перенаправления потоков

Команда	Описание
Общий режим/Режим администратора	
show flow-based-redirect {interface [ethernet <IFNAME> **|**<*IFNAME*>**]}**	Показывает информацию о текущей конфигурации перенаправления потоков на порту/устройстве.

19.3 Примеры перенаправления потоков

Пример:

Требования пользователя к конфигурации состоят в следующем: перенаправление фреймов с исходящим IP адресом 192.168.1.111, принимаемых на порту 1, на порт 6.

Изменения конфигурации:

1. Настройка листа доступа. Условия выборки — IP адрес источника - 192.168.1.111
2.Применить перенаправление этого потока на порту 1.

Процедура конфигурации:

```
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
```

19.4 Устранение неисправностей перенаправления потоков

Если конфигурация перенаправления потока не работает, проверьте следующие причины, которые могут вызывать проблемы:

- ❖ Тип потока (лист доступа) может быть только следующих видов - стандартный ACL, расширенный ACL, именованный расширенный ACL, именованный стандартный ACL, стандартный IPv6 ACL и именованный стандартный IPv6 ACL;
- ❖ Параметры временного диапазона и диапазона портов не могут быть заданы листом доступа. Тип листа доступа должен быть permit;
- ❖ Порт перенаправления в функции перенаправления потоков должен быть 1000Мб;

20 КОНФИГУРИРОВАНИЕ SELECTIVE QINQ

20.1 Общие сведения о selective QinQ

20.1.1 Технология QinQ

Туннель Dot1q, который так же называют QinQ (802.1Q-in-802.1Q) является расширением стандарта 802.1Q. Основная идея заключается в упаковке метки клиентского VLAN (CVLAN tag) в метку VLAN держателя сервиса (SPVLAN tag). Пакет с двумя метками VLAN передается через магистральную сеть провайдера для предоставления пользователям простого туннеля 2-го уровня. Это просто и легко для управления, реализуемо только статической конфигурацией и особенно хорошо применимо для маленьких офисных сетей и небольших сетей второго уровня (METRO) использующих коммутаторы 3-го уровня как магистральные устройства.

Существует два типа QinQ: Basic QinQ и Selective QinQ. Приоритет selective QinQ выше, чем basic.

20.1.2 BasicQinQ

Basic QinQ базируется на порту. После конфигурации QinQ на порту, имеют ли принимаемые пакеты метку или нет, устройство упаковывает VLAN по умолчанию в пакет. Использование базового QinQ просто, но метод установки метки VLAN'а не selective.

20.1.3 Selective QinQ

Selective QinQ базируется на потоке данных. Он проверяет, содержит ли пакет внешнюю метку и упаковывает столько внешних меток, сколько их присутствует в потоке. Для примера: реализация возможностей selective QinQ в соответствии с пользовательскими метками VLAN'а, MAC адресами, Ipv4/IPv6 адресами, Ipv4/IPv6 протоколами и идентификаторами портов приложений и т.д. Таким образом, он может упаковывать внешние метки для пакетов и применять различные схемы для различных пользователей или методов.

20.2 Настройка selective QinQ

При использовании selective QinQ поток данных использует для передачи правила карты политик QoS.

1. Создать карту классов для классификации различных потоков данных;
2. Создать карту политик selective QinQ для связи с картой классов и настроить соответствующие операции;
3. Привязать карту политик selective QinQ к порту;

1. Конфигурирование карты классов

Команда	Описание
Режим глобального конфигурирования	
class-map <class-map-name> **no class-map** <class-map-name>	Создание карты классов и вход в режим карты классов, команда NO удаляет конкретную карту классов.

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}**	Настройка стандартного набора карты классов (классификация потока данных по листу доступа, CoS, VLAN ID, приоритету IPv4 или DSCP и т.д. Для карты классов); Команда NO удаляет определенный набор стандартов.

2. Конфигурирование карты политик selective QinQ

Команда	Описание
Режим глобального конфигурирования	
policy-map <policy-map-name> **no policy-map** <policy-map-name>	Создание карты политик и вход в режим карты политик, команда NO удаляет указанную карту политик.
class <*class-map-name*> **[insert-before <class-map-name>]** **no class** <class-map-name>	После того, как карта политик создана, она может быть привязана к классу. Команда NO удаляет указанную карту классов.
set {s-vid <new-vid> | c-vid <new-vid>} **no set {s-vid | c-vid}**	Указание внешней метки VLAN'а для классифицированного трафика. Команда NO отменяет операцию.

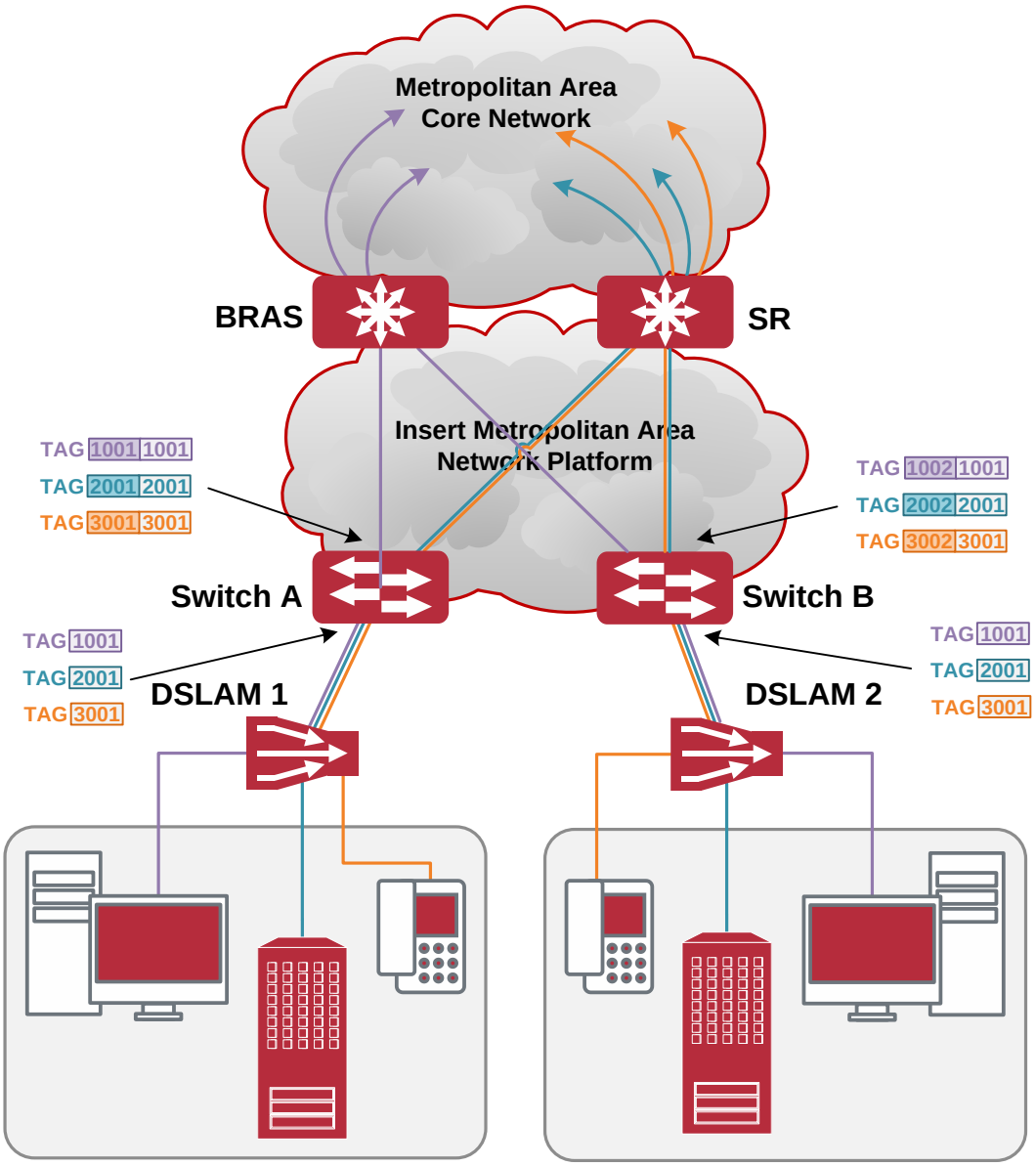
3. Привязка карты политик selective QinQ к порту

Команда	Описание
Режим конфигурирования порта	
service-policy input <*policy-map-name*> **no service-policy input** <*policy-map-name*>	Применяет карту политик к порту. Команда NO отменяет применение указанной карты политик к порту.

4. Показывает привязку карты политик selective QinQ к порту

Команда	Описание
Режим администратора	
show mls qos {interface [<interface-id>**]**	Показывает конфигурацию selective QinQ на порту.

20.3 Пример применения selective QinQ



Топология применения selective QinQ

Как показано на рисунке, первый пользователь использует три VLAN’а с метками 1001, 2001, 3001 соответственно на DSLAM1. VLAN1001 соответствует широковещательной сети, VLAN2001 соответствует Client Services, VLAN3001 соответствует VOIP. На соответствующем порту сети, имеющем функцию QinQ, пакеты будут упаковываться различными внешними метками в соответствии с VLAN ID пользователя. Пакет с меткой 1001 будет паковаться дополнительной внешней меткой 1001 (эта метка уникальна на данной сети), и по ней будет классифицирован на устройстве BRAS (центр хранения конфигурации). Пакеты с метками 2001 (или 3001) будут паковаться внешней меткой 2001 (или 3001) и классифицируются на устройстве SR в соответствии с правилами потоков.

Второй пользователь может использовать различные метки VLAN'ов на DSLAM2. Замечание: применяемые метки VLAN'ов для второго пользователя могут быть такими же, как для первого пользователя и пакеты с этими метками так же пакуются во внешнюю метку. На рисунке выше, внешняя метка для второго пользователя отличается от метки первого пользователя в соответствии с расположением DSLAM и расположением пользователя.

Если поток данных DSLAM1 идет через порт1 Switch A, конфигурация, следующая:

```
Switch(config)#class-map c1
Switch(config-classmap-c1)#match vlan 1001
Switch(config-classmap-c1)#exit
Switch(config)#class-map c2
Switch(config-classmap-c2)#match vlan 2001
Switch(config-classmap-c2)#exit
Switch(config)#class-map c3
Switch(config-classmap-c3)#match vlan 3001
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)#service-policy input p1
```

Если поток данных DSLAM2 идет через порт1 Switch B, конфигурация, следующая:

```
Switch(config)#class-map c1
Switch(config-classmap-c1)#match vlan 1001
Switch(config-classmap-c1)#exit
Switch(config)#class-map c2
Switch(config-classmap-c2)#match vlan 2001
Switch(config-classmap-c2)#exit
Switch(config)#class-map c3
Switch(config-classmap-c3)#match vlan 3001
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)# service-policy input p1
```

20.4 Устранение неисправностей selective QinQ

Если правила selective QinQ не могут быть привязаны к порту, проверьте нет ли проблем, вызванных следующими причинами:

- Проверьте, поддерживается ли selective QinQ сконфигурированными картами классов и политик;
- Убедитесь, что листы доступа включают разрешающие правила в карте классов, имеющих листы доступа;
- Проверьте, что коммутатор имеет достаточно памяти TCAM для передачи связей;

21 КОНФИГУРИРОВАНИЕ ФУНКЦИЙ 3-ГО УРОВНЯ

Коммутатор поддерживает только второй уровень переадресации, но можно настроить третий уровень управления портом для соединения всех видов протоколов управления на основе IP протокола.

21.1 Интерфейс 3-го уровня

21.1.1 Начальные сведения об интерфейсах 3-го уровня

В коммутаторах может быть создан интерфейс 3-го уровня. Он является не физическим интерфейсом, а виртуальным. Интерфейс 3-го уровня строится на интерфейсе VLAN. Интерфейс уровня 3 может содержать один или более интерфейсов уровня 2, принадлежащих одному и тому же VLAN, либо не содержать интерфейсов уровня 2. По крайней мере, один из интерфейсов уровня 2, содержащихся в интерфейсе уровня 3, должен быть включен (находиться в состоянииUP) — тогда будет включен и интерфейс уровня 3. В противном случае интерфейс уровня 3 будет выключен (будет находиться в состоянии DOWN). Коммутатор может использовать IP адреса, установленные на интерфейсах 3-го уровня, для коммуникации с другими устройствами через IP протокол. Коммутатор может пересылать IP пакеты между разными интерфейсами 3-го уровня.

21.1.2 Настройка интерфейса 3-го уровня

Последовательность настройки интерфейса 3-го уровня:

1. Создание интерфейса 3-го уровня;
2. Настройка описания VLAN интерфейса;

1. Создание интерфейса 3-го уровня

Команда	Описание
Режим глобального конфигурирования	
interface vlan *<vlan-id>* **no interface vlan** *<vlan-id>*	Создание VLAN интерфейса (VLAN интерфейс это интерфейс 3-го уровня); команда «no» удаляет VLAN интерфейс, созданный на коммутаторе.

2. Настройка описания VLAN интерфейса

Команда	Описание
Режим конфигурирования VLAN интерфейса	
description *<text>* **no description**	Настройка описания VLAN интерфейса. Команда «no»уберет описание VLAN интерфейса.

21.2 Настройка протокола IP

21.2.1 Введение в IPv4, IPv6

IPv4 это текущая версия глобального универсального Интернет-протокола. Практика доказала, что IPv4 является простым, гибким, открытым, мощным, а также легким в реализации протоколом. Он обладает хорошей совместимостью с различными протоколами верхнего и нижнего уровней. Хотя IPv4 почти не менялся с момента его появления в 80-х годах, он продолжает распространяться по всему миру вместе с распространением Интернет. Однако по мере роста инфраструктуры Интернет и услуг, использующих Интернет-приложения, выявляются и некоторые недостатки протокола IPv4, связанные с масштабом и сложностью сегодняшнего Интернета.

IPv6 — это шестая версия Интернет-протокола, следующее его поколение. IPv6 разработан IETF и должен заменить используемый в настоящее время Интернет-протокол версии 4 (IPv4). IPv6 был разработан специально для того, чтобы ликвидировать нехватку адресов IPv4, препятствующую дальнейшему развитию Интернет.

Наиболее важная проблема, которая решена в IPv6 — это добавление достаточного количества IP-адресов. Запас адресов IPv4 почти исчерпан, в то время как число пользователей Интернет растет в геометрической прогрессии. Объемы предоставляемых Интернет-услуг и число прикладных устройств продолжают расти опережающими темпами (домашние и малые офисные сети, IP-телефония, терминалы беспроводного информационного обслуживания, использующие Интернет и т. д.). В результате требуется все большее количество IP-адресов, предоставлять которые становится все более затруднительно. Работа по преодолению нехватки IPv4-адресов велась долгое время; были предложены различные технологии, позволяющие продлить срок эксплуатации, существующей IPv4-инфраструктуры, в том числе трансляция сетевых адресов NAT (Network Address Translation), технология CIDR (Classless Inter-Domain Routing) и т. д.

Хотя сочетание CIDR, NAT и частных адресов временно смягчило проблемы нехватки IPv4 адресов, NAT технология разрушила модель «из конца в конец» (end-to-end), которая являлась первоначальной целью замысла IP, сделав необходимым для промежуточных маршрутизаторов поддержание статуса каждого соединения, что значительно увеличивает задержки в сети и снижает производительность сети. Кроме того, трансляция сетевых адресов пакетов данных препятствует проверке безопасности соединений «из конца в конец», заголовок аутентификации IPSec – явный пример.

Поэтому, чтобы комплексно решить все виды проблем, существующих в IPv4, следующее поколение интернет-протокола IPv6, разработанное IETF, стало единственным возможным решением в настоящее время.

Прежде всего, 128-битная схема адресации протокола IPv6 гарантированно обеспечивает достаточное число глобально уникальных IP-адресов для узлов глобальной IP-сети— и по времени, и в пространстве. Кроме увеличения адресного пространства протокол IPv6 улучшает многие другие важные аспекты IPv4.

Иерархическая схема адресации облегчает объединение маршрутов, эффективно снижает количество записей таблицы маршрутизации и улучшает эффективность маршрутизации и обработки пакетов данных.

По сравнению с IPv4, конструкция заголовка IPv6 более совершенна. Заголовок содержит меньше полей данных, из него изъята контрольная сумма, что увеличивает скорость обработки основного заголовка IPv6. В заголовке IPv6 поле фрагмента может быть

показано как дополнительное расширенное поле, поэтому больше не будет необходимости в фрагментации пакетных данных в процессе их передачи в маршрутизаторе. Кроме того, эффективность работы маршрутизатора повышается за счет механизма обнаружения маршрута MTU (Path MTU Discovery Mechanism) работающего с источником пакетных данных.

Поддерживается автоматическая настройка адреса и Plug-And-Play. Большое количество хостов могут легко найти сетевые маршрутизаторы используя функцию автоматической конфигурации IPv6, автоматически получая глобально уникальные IPv6 адреса, что делает устройства, использующие протокол IPv6, устройствами Plug-And-Play. Функция автоматической настройки адреса, так же делает процесс смены адресов в существующей сети проще и удобнее, администраторам сети проще переходить от одного провайдера к другому.

Поддержка IPSec. IPSec обязателен в IPv6, в отличие от IPv4. IPv6 обеспечивает расширенный заголовок безопасности, который обеспечивает сервисы безопасности «из конца в конец», такие как контроль доступа, конфиденциальность и целостность данных, следовательно, делает проще реализацию механизмов шифрования, проверки и виртуальных частных сетей (VPN).

Улучшена поддержка мобильных IP-устройств и мобильных вычислительных устройств. Мобильный IP-протокол, определенный стандартом IETF, обеспечивает работу мобильных устройств в движении без разрыва существующего соединения. Эта сетевая функция приобретает сейчас все большую важность. В отличие от IPv4, мобильность IPv6 обеспечивается встроенным автоматическим конфигурированием для получения адреса передачи (Care-Of-Address). Поэтому при использовании IPv6 не требуется Другого Агента. Более того, при таком связывании включается Корреспондентский узел, связывающийся с Мобильным узлом напрямую. Это позволяет избежать удорожания системы из-за треугольного маршрута, требующегося при IPv4.

Удалось избежать и трансляции сетевых адресов. Целью введения NAT было использование механизма совместного и повторного использования одного и того же адресного пространства в различных сегментах сети. Этот механизм временно смягчает проблему нехватки IPv4-адресов, однако добавляются ограничения, накладываемые процессом трансляции адресов на сетевые устройства и приложения. Так как адресное пространство IPv6 значительно больше, то в трансляции адресов больше нет необходимости. В результате, проблемы с NAT и со стоимостью ее развертывания решаются естественным способом.

IPv6 сохранил и расширил поддержку существующих протоколов маршрутизации IGP (Internal Gateway Protocols) и EGP (Exterior Gateway Protocols). Например, протоколы маршрутизации IPv6, такие как RIPng, OSPFv3, IS-ISv6, MBGP4+ и т.д.

Расширена поддержка Multicast и увеличено количество Multicast адресов. Работая с broadcast функциями IPv4, такими как Router Discovery and Router Query, IPv6 multicast полностью заменил IPv4 broadcast в плане функций. Multicast не только экономит пропускную способность сети, но и повышает эффективность сети в целом.

21.2.2 Настройка IP протокола

Интерфейс 3-го уровня может быть настроен как IPv4 интерфейс либо как IPv6 интерфейс.

21.2.2.1 Настройка адреса IPv4

1. Настройка IPv4 адрес интерфейса 3-го уровня
2. Настройка шлюза по умолчанию.

1. Настройка IPv4 адрес интерфейса 3-го уровня

Команда	Описание
Режим конфигурирования VLAN интерфейса	
ip address *<ip-address> <mask>* **[secondary]** **no ip address [**<ip-address> <mask>**]**	Настройка IP адреса VLAN интерфейса; команда **no ip address [**<ip-address> <mask>**]** отменяет IP адрес VLAN интерфейса.

2. Настройка шлюза по умолчанию.

Команда	Описание
Глобальный режим конфигурирования	
ip route 0.0.0.0 0.0.0.0 <A.B.C.D> **no ip route 0.0.0.0 0.0.0.0 <A.B.C.D>**	Настройка статической маршрутизации. Команда no отменяет настройку.

21.2.2.2 Настройка адреса IPv6

Последовательность настройки адреса IPv6:
1. Базовая настройка IPv6
(1) Настройка адреса IPv6 интерфейса;
(2) Настройка статической маршрутизации IPv6;
2. Настройка IPv6 Neighbor Discovery
(1) Настройка количества сообщений DAD neighbor solicitation;
(2) Настройка интервала отправки сообщений neighbor solicitation;
(3) Настройка статических записей IPv6 соседей (neighbor);
(4) Удаление всех записей в таблице соседей IPv6;

1. Базовая настройка IPv6
(1) Настройка адреса IPv6 интерфейса

Команда	Описание
Режим конфигурирования интерфейса	
ipv6 address <ipv6-address/prefix-length> **[eui-64]** **no ipv6 address** <ipv6-address/prefix-length>	Настройка IPv6 адреса, включая объединяемые глобальные unicast адреса, site-local адреса и link-local адреса. Команда **no ipv6 address** <ipv6-address/prefix-length> отменяет IPv6 адрес.

(2) Настройка статической маршрутизации IPv6

Команда	Описание
Режим глобального конфигурирования	
ipv6 route <ipv6-prefix/prefix-length> **{**<nexthop-ipv6-address>**|**<interface-type interface-number> **| {**<nexthop-ipv6-address> <interface-type interface-number>**}} [distance]** **no ipv6 route** <ipv6-prefix/prefix-length> **{**<nexthop-ipv6-address>**|**<interface-type interface-number> **|{**<nexthop-ipv6-address> <interface-type interface-number>**}} [distance]**	Настройка статической маршрутизации IPv6. Команда no отменяет статическую маршрутизацию IPv6.

2. Настройка IPv6 Neighbor Discovery

(1) Настройка количества сообщений DAD neighbor solicitation

Команда	Описание
Режим конфигурирования интерфейса	
ipv6 nd dad attempts <value> **no ipv6 nd dad attempts**	Установка количества сообщений, отправляемых последовательно при обнаружении интерфейсом дубликата адреса. Команда no восстанавливает значение по умолчанию (1).

(2) Настройка интервала отправки сообщений neighbor solicitation

Команда	Описание
Режим конфигурирования интерфейса	
ipv6 nd ns-interval *<seconds>* **no ipv6 nd ns-interval**	Установка интервала отправки запросов соседям. Команда no восстанавливает значение по умолчанию (1 секунда).

(3) Настройка статических записей IPv6 соседей (neighbor)

Команда	Описание
Режим конфигурирования интерфейса	

ipv6 neighbor <ipv6-address> <hardware-address> **interface** <interface-type interface-name>	Установка статической записи в таблице соседей, включая IPv6 адрес соседа, MAC адрес и порт второго уровня.
no ipv6 neighbor *<ipv6-address>*	Удаление записи в таблице соседей.

(4) Удаление всех записей в таблице соседей IPv6

Команда	Описание
Режим администратора	
clear ipv6 neighbors	Очистка всех статических записей в таблице соседей.

21.2.3 Поиск неисправностей IPv6

Настройка времени жизни маршрутизатора не должна быть меньше интервала объявления маршрутизатора. Если подключенный PC не получил IPv6 адрес, необходимо проверить RA анонсирование на коммутаторе (выключено по умолчанию).

21.3 ARP

21.3.1 Введение в ARP

ARP (Address Resolution Protocol - протокол определения адреса) в основном используется для определения Ethernet MAC адреса по IP адресу. Коммутатор поддерживает статическую конфигурацию.

21.3.2 Список задач конфигурации ARP

Список задач конфигурации ARP:

1. Настроить статический ARP

Команда	Описание
Режим VLAN интерфейса	
arp *<ip_address>* *<mac_address>* {interface [ethernet] <portName>} **no arp <ip_address>**	Настраивает статическую запись ARP; команда no удаляет запись ARP указанного IP адреса.

21.3.3 Поиск неисправностей ARP

Если не проходит ping от коммутатора к устройствам, подключенным напрямую, можно использовать следующие действия для поиска и устранения возможной причины:

- ❖ Проверьте, есть ли соответствующая ARP запись на коммутаторе.
- ❖ Если ARP записи нет, включите отладку ARP и посмотрите условия приема/отправки ARP пакетов.
- ❖ Самая распространенная причина проблемы – дефектный кабель.

22 НАСТРОЙКА ФУНКЦИИ ПРЕДОТВРАЩЕНИЯ ARP СКАНИРОВАНИЯ

22.1 Введение в функцию предотвращения ARP сканирования

ARP сканирование — это обычный способ сетевой атаки. Для того, чтобы обнаружить все активные хосты в сегменте сети, источник атаки будет рассылать большое количество ARP сообщений, что будет занимать большую часть пропускной способности сети. Можно даже сделать атаку большим количеством трафика используя поддельные ARP сообщения, что приведет к коллапсу сети из-за исчерпания пропускной способности. Обычно ARP сканирование это просто предпосылка к другой, более опасной атаке, такой, как автоматическое заражение вирусом или последующее сканирование портов, сканирование уязвимостей, нацеленное на хищение информации, атака искаженными сообщениями, DOS атака и т.д.

Поскольку ARP сканирование угрожает безопасности и стабильности сети, очень важно его предотвратить. Коммутатор обеспечивает полное решение для предотвращения ARP сканирования: если в сегменте найден хост или порт с признаками ARP сканирования, коммутатор отрежет источник атаки для обеспечения безопасности сети.

Есть два метода предотвращения ARP сканирования: на основе порта и на основе IP. Метод на основе порта считает количество ARP сообщений, полученных с порта за определенный период, если число превышает заданный порог, порт будет выключен. Метод на основе IP считает количество ARP сообщений, полученных от IP адреса в сегменте за определенный период, если число превышает заданный порог, любой трафик от этого IP будет заблокирован до тех пор, пока порт, связанный с IP адресом, не будет погашен. Эти два метода могут быть включены одновременно. После того, как порт или IP адрес были заблокированы, пользователь может восстановить их статус используя функцию автоматического восстановления.

Чтобы повысить эффективность, пользователи могут настроить доверенные порты и IP адреса, ARP сообщения от которых не будут проверяться коммутатором. Таким образом нагрузка на коммутатор может быть значительно снижена.

22.2 Последовательность задач конфигурации предотвращения ARP сканирования

1. Включить функцию предотвращения ARP сканирования.
2. Настроить пороговое значение для метода, основанного на портах и метода, основанного на IP.
3. Настроить доверенные порты
4. Настроить доверенные IP
5. Настроить время автоматического восстановления
6. Посмотреть информацию, относящуюся к ARP сканированию, а также отладочную информацию.

1. Включить функцию предотвращения ARP сканирования.

Команда	Описание
Общий режим конфигурации	
anti-arpscan enable **no anti-arpscan enable**	Включение/выключение функции предотвращения ARP сканирования.

2. Настроить пороговое значение для метода, основанного на портах и метода, основанного на IP

Команда	Описание
Общий режим конфигурации	
anti-arpscan port-based threshold <threshold-value> **no anti-arpscan port-based threshold**	Установка порогового значения для метода, основанного на портах.
anti-arpscan ip-based threshold *<threshold-value>* **no anti-arpscan ip-based threshold**	Установка порогового значения для метода, основанного на IP.

3. Настроить доверенные порты

Команда	Описание
Режим конфигурации порта	
anti-arpscan trust <port | supertrust-port> **no anti-arpscan trust <port |supertrust-port>**	Установка атрибутов доверия портов.

4. Настроить доверенные IP

Команда	Описание
Общий режим конфигурации	
anti-arpscan trust ip *<ip-address>* [*<netmask>*] **no anti-arpscan trust ip *<ip-address>* [*<netmask>*]**	Установка атрибутов доверия IP.

5. Настроить время автоматического восстановления

Команда	Описание
Общий режим конфигурации	
anti-arpscan recovery enable **no anti-arpscan recovery enable**	Включение/выключение функции автоматического восстановления.
anti-arpscan recovery time *<seconds>* **no anti-arpscan recovery time**	Установка времени автоматического восстановления.

6. Посмотреть информацию, относящуюся к ARP сканированию, а также отладочную информацию

Команда	Описание
Общий режим конфигурации	
anti-arpscan log enable **no anti-arpscan log enable**	Включение/выключение функции журнала предотвращения ARP сканирования.
anti-arpscan trap enable **no anti-arpscan trap enable**	Включение/выключение функции SNMP Trap предотвращения ARP сканирования.
show anti-arpscan [trust <ip | port | supertrust-port> | prohibited <ip | port>]	Отображение состояния работы и конфигурации предотвращения ARP сканирования.
Режим администратора	
debug anti-arpscan *<port | ip>* **no debug anti-arpscan *<port | ip>***	Включение/выключение отладки предотвращения ARP сканирования.

22.3 Типовые примеры предотвращения ARP сканирования

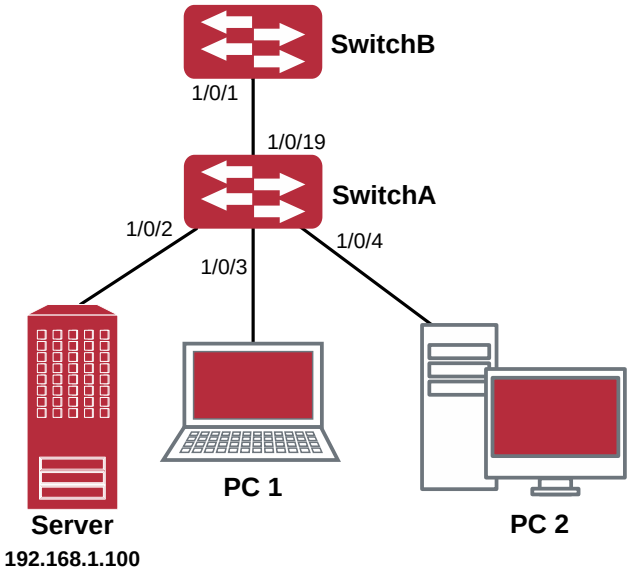
В сети, топология которой показана выше, порт E1/0/1 коммутатора B подключен к порту E1/0/19 коммутатора A, порт E1/0/2 коммутатора A подключен к файловому серверу (IP адрес 192.168.1.100/24), все остальные порты коммутатора A подключены к обычным PC. Следующая конфигурация может эффективно предотвратить ARP сканирование, не влияя на нормальную работу системы.

Последовательность настройки коммутатора A:

```
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

Последовательность настройки коммутатора B:
Switch B(config)# anti-arpscan enable
SwitchB(config)#interface ethernet1/0/1
SwitchB (Config-If-Ethernet 1/0/1)#anti-arpscan trust port
SwitchB (Config-If-Ethernet 1/0/1)exit
```



Типовой пример конфигурации предотвращения ARP сканирования

22.4 Поиск неисправностей предотвращения ARP сканирования

Предотвращение ARP сканирования по умолчанию выключено. После включения предотвращения ARP сканирования пользователь может включить отладку («debug anti-arpscan») для просмотра отладочной информации.

23 КОНФИГУРАЦИЯ ЗАЩИТЫ ОТ ПОДМЕНЫ ARP

23.1 Обзор

23.1.1 ARP (Address Resolution Protocol)

В общем, протокол ARP (RFC-826), в основном, отвечает за соотношение IP адреса соответствующему 48-битному физическому адресу, то есть MAC адресу, например, IP адрес 192.168.0.1, MAC адрес сетевой карты A0-12-34-FD-1D-2B.

Весь процесс соотношения состоит в том, что хост отправляет широковещательный (broadcast) пакет данных, включающий в себя информацию об IP адресе хоста назначения (ARP запрос), затем хост назначения отправляет исходному хосту пакет данных, включающий в себя информацию об IP адресе и MAC адресе. Таким образом, два хоста могут обмениваться информацией по MAC адресу.

23.1.2 Подмена ARP

С точки зрения протокола ARP, чтобы уменьшить ARP трафик в сети, если хост получит ARP ответ, который он не запрашивал, он так же добавит запись в свой ARP кэш, что делает возможным подмену ARP (ARP spoofing). Если хакер хочет прослушать обмен данными между двумя хостами в одной сети (даже если они подключены через коммутаторы), он отправляет пакет ARP ответа двум хостам по отдельности, это приводит к тому, что каждый из хостов считает MAC адрес хакера адресом другого хоста. Таким образом, вместо прямого обмена, хосты обмениваются трафиком через хост хакера. Хакеры не только получают необходимую им информацию. Им для успешной передачи необходимо всего лишь изменить некоторую информацию в пакете. В этом случае на компьютере хакера не нужно настраивать смешанный режим сетевой карты, т.к. пакеты данных поступают на компьютер хакера на физическом уровне, компьютер работает как ретранслятор.

23.1.3 Как предотвратить подмену ARP

Есть много видов атак, основанных на протоколе ARP. Большинство атак основаны на подмене ARP, так что очень важно предотвратить подмену ARP.

Механизм подмены ARP проникает в сеть, в первую очередь, путем подделки легального IP адреса, затем посылая много поддельных ARP пакетов коммутаторам, после чего коммутаторы заменяют правильные связки IP-MAC соответствующими связками из атакующих пакетов. Таким образом, коммутатор ошибочно отправляет пакеты атакующему хосту, и это действует на всей сети.

Основным методом предотвращения атак и подмены ARP на коммутаторах является отключение на коммутаторе функции автоматического обновления. Обманщик не сможет изменить правильные связки IP-MAC на коммутаторе, тем самым предотвращается неправильная пересылка пакетов. В то же время это не прерывает функцию автоматического обучения ARP. Таким образом, это значительно предотвращает подмену ARP.

ND это протокол обнаружения соседей в IPv6, аналогичный протоколу ARP по принципу действия, поэтому для предотвращения подмены ND мы делаем то же самое, что и для ARP.

23.2 Конфигурация предотвращения подмены ARP

Последовательностьт настройки предотвращения подмены ARP:

1. Отключить функцию автоматического обновления ARP
2. Отключить функцию автоматического обучения ARP
3. Поменять динамические ARP на статические

1. Отключить функцию автоматического обновления ARP

Команда	Описание
Общий режим и Режим порта	
ip arp-security updateprotect **no ip arp-security updateprotect**	Отключить/включить функцию автоматического обновления ARP.

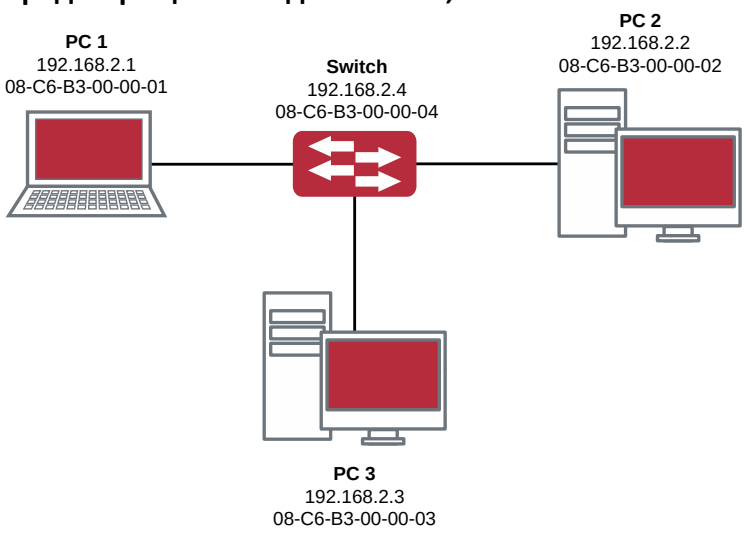
2. Отключить функцию автоматического обучения ARP, ND

Команда	Описание
Общий режим и Режим интерфейса	
ip arp-security learnprotect **no ip arp-security learnprotect**	Отключить/включить функцию автоматического обучения ARP.

3. Поменять динамические ARP, ND на статические

Команда	Описание
Общий режим и Режим порта	
ip arp-security convert	Поменять динамическ ие ARP на статические.

23.3 Пример предотвращения подмены ARP, ND



Описание оборудования

Оборудование	Конфигурация	Кол-во
Switch	IP:192.168.2.4;mac: 08-C6-B3-00-00-04	1
PC 1	IP:192.168.2.1;mac: 08-C6-B3-00-00-01	1
PC 2	IP:192.168.1.2;mac: 08-C6-B3-00-00-02	1
PC 3	IP:192.168.2.3;mac: 08-C6-B3-00-00-03	несколько

На диаграмме показана нормальная связь между PC 2 и PC 3. PC 1 хочет, чтобы коммутатор направлял ему пакеты, отправленные хостом PC 2. В первую очередь PC 1 отправляет пакет ARP ответа на коммутатор в формате: 192.168.2.3, 08-C6-B3-00-00-01, сопоставляя его MAC адрес с IP адресом хоста C, коммутатор обновляет ARP список и начинает отправлять пакеты для 192.168.2.3 на MAC адрес 08-C6-B3-00-00-01 address (адрес хоста PC 1).

В дальнейшем хост PC 1 пересылает принятые пакеты хосту PC 3, меняя адрес источника и адрес назначения. Так как ARP список своевременно обновляется, еще одной задачей для хоста A является непрерывная отправка ARP ответов и обновление ARP списка коммутатора.

Поэтому очень важно защитить ARP список, настроить запрещение ARP обучения в стабильной среде и затем изменить все динамические ARP записи на статические. Выученные ARP не будут обновляться и будут защищены.

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#arp 192.168.2.1 08-C6-B3-00-00-01 interface eth
1/0/2
Switch(Config-If-Vlan1)#interface vlan 2
Switch(Config-If-Vlan2)#arp 192.168.1.2 08-C6-B3-00-00-02 interface eth
1/0/2
Switch(Config-If-Vlan2#interface vlan 3
Switch(Config-If-Vlan3)#arp 192.168.2.3 08-C6-B3-00-00-03 interface eth
1/0/2
Switch(Config-If-Vlan3)#exit
Switch(Config)#ip arp-security learnprotect
Switch(Config)#
Switch(config)#ip arp-security convert
```

Если окружающая среда меняется, это позволяет запретить ARP обновления, как только ARP будет изучено, оно не может быть обновлено новым ARP ответом, данные будут защищены от прослушивания.

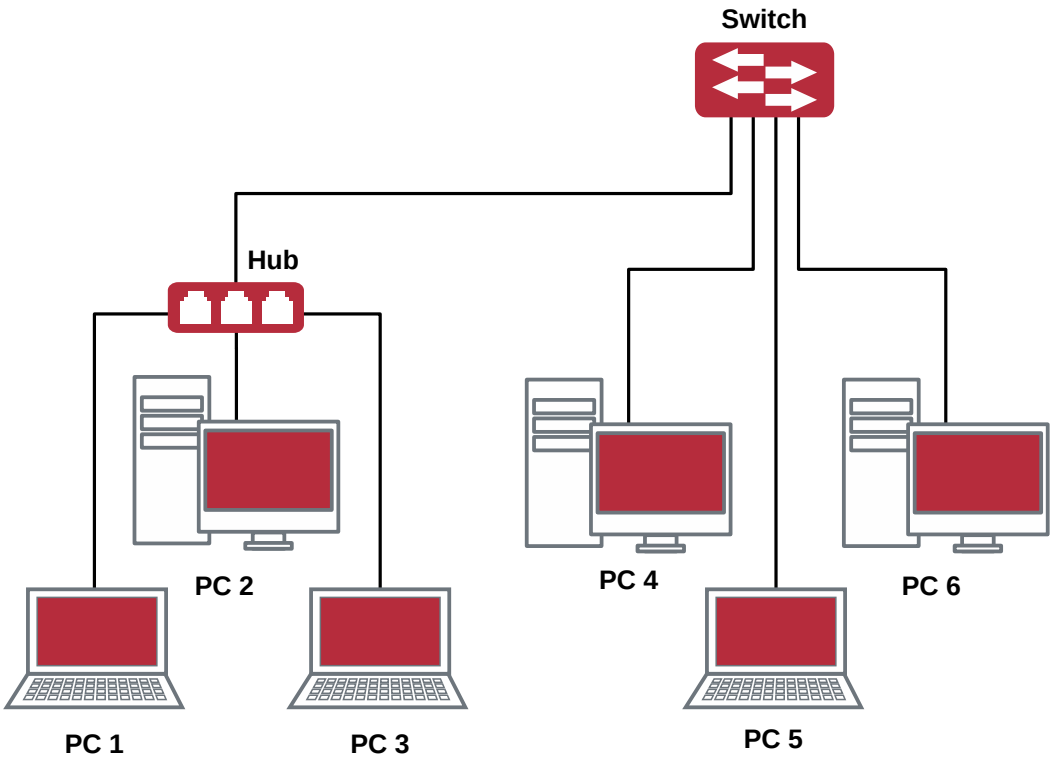
```
Switch#config
Switch(config)#ip arp-security updateprotect
```

24 НАСТРОЙКА ARP GUARD

24.1 Введение в ARP GUARD

Существует серьезная уязвимость в модели ARP протокола, которая заключается в том, что любое сетевое устройство может отправить ARP сообщение, чтобы объявить о связке IP и MAC адресов. Это делает возможным ARP мошенничество. Злоумышленники могут послать ARP запрос или ARP ответ чтобы информировать о неверной связке между IP адресом и MAC адресом, которая приведет к проблемам связи. Есть две формы ARP мошенничества: 1. PC4 отправляет ARP сообщение чтобы сообщить, что IP адрес PC2 привязан к MAC адресу PC4, это приведет к тому, что все IP пакеты, адресуемые PC2, будут отправлены к PC4, таким образом PC4 сможет просматривать все пакеты, адресованные PC2; 2. PC4 отправляет ARP сообщение чтобы сообщить, что IP адрес PC2 привязан к несуществующему MAC адресу, это приведет к тому, что PC2 не будет получать адресованные ему пакеты.

В частности, если злоумышленник, прибегая к ARP мошенничеству, выдает себя за шлюз, вся сеть выйдет из строя.



Схематичная диаграмма ARP GUARD

Мы используем фильтрующие элементы коммутатора для защиты ARP-записей важных сетевых устройств от подражания другими устройствами. Основной теорией этого является использование фильтрующих элементов коммутатора для проверки всех ARP сообщений, проходящих через порт. Если адрес источника ARP сообщения защищен, сообщения будут отброшены и не передадутся далее.

Функция ARP GUARD обычно используется для защиты шлюза от атак. Если все доступные компьютеры в сети будут защищены функцией ARP GUARD, для этого потребуется настроить на порту большое количество ARP GUARD адресов, что займет большую часть FFP записей в чипе, и, как результат, может отразиться на других приложениях. Так что это будет неправильно. Рекомендуется адоптировать свободные ресурсы согласно схеме доступа. Пожалуйста, обратитесь за подробностями к соответствующей документации.

24.2 Список задач конфигурации ARP GUARD

1. Настроить защищенные IP адреса

Команда	Описание
Режим конфигурации порта	
arp-guard ip <addr> **no arp-guard ip <addr>**	Настроить/удалить ARP GUARD адрес

25 КОНФИГУРАЦИЯ САМООБРАЩЕННОГО ARP (GRATUITOUS ARP)

25.1 Введение в самообращенный ARP

Самообращенный ARP это тип ARP запроса, отправляемый хостом и его IP адресом в качестве адреса назначения.

Basicрежим работы коммутаторов, следующий: на интерфейсах 3-го уровня может быть настроен интервал рассылки самообращенных ARP запросов или это может быть настроено глобально на всех интерфейсах.

Назначение самообращенного ARP следующее:

- Чтобы уменьшить частоту ARP запросов хостов к коммутатору. Хосты в сети периодически посылают ARP запросы к шлюзу чтобы обновить MAC адрес шлюза. Если коммутатор рассылает самообращенные ARP запросы, хостам не нужно отправлять эти запросы. Это уменьшит частоту отправки хостами ARP запросов на шлюз.
- Самообращенный ARP это метод предотвращения ARP мошенничества. Рассылаемый коммутатором самообращенный ARP заставит хосты обновить свой ARP кэш. Таким образом поддельный ARP не фунционирует.

25.2 Список задач конфигурации самообращенного ARP

1. Включить самообращенный ARP и настроить интервал отправки ARP запросов.
2. Отобразить конфигурацию самообращенного ARP.

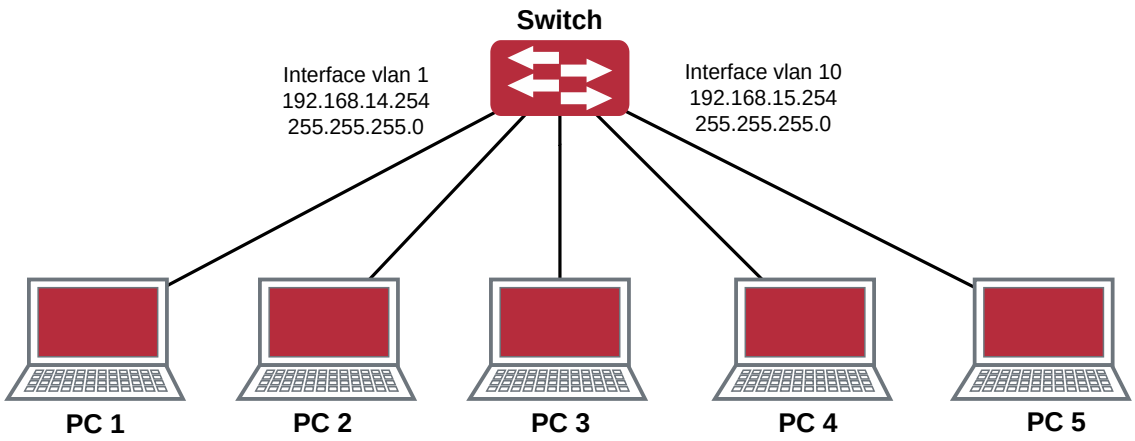
1. Включить самообращенный ARP и настроить интервал отправки ARP запросов.

Команда	Описание
Режим глобальной конфигурации и режим конфигурации интерфейса.	
ip gratuitous-arp <*5-1200*> **no ip gratuitous-arp**	Включить самообращенный ARP и настроить интервал отправки ARP запросов. Команда no отменяет самообращенный ARP.

2. Отобразить конфигурацию самообращенного ARP

Команда	Описание
Режим администратора и режим конфигурации	
show ip gratuitous-arp [interface vlan <*1-4094*>]	Отобразить конфигурацию самообращенного ARP.

25.3 Пример конфигурации самообращенного ARP



Пример настройки самообращенного ARP

Для топологии сети, показанной на рисунке, интерфейс коммутатора VLAN10 имеет IP адрес 192.168.15.254 и маску сети 255.255.255.0. Три компьютера – PC3, PC4, PC5 – подключены к этому интерфейсу. Интерфейс VLAN1 имеет IP адрес 192.168.14.254 и маску сети 255.255.255.0. Два компьютера – PC1 и PC2 - подключены к этому интерфейсу. Самообращенный ARP включается следующий конфигурацией:

Оба интерфейса используют самообращенный ARP.

```
Switch(config)#ip gratuitous-arp 300
Switch(config)#exit
```

Самообращенный ARP настроит только для одного интерфейса.

```
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 300
Switch(Config-if-Vlan10)#exit
Switch(config) #exit
```

25.4 Поиск неисправностей самообращенного ARP

Самообращенный ARP выключен по умолчанию. Когда самообращенный ARP включен, отладочную информацию можно получить, используя команду «debug ARP send».

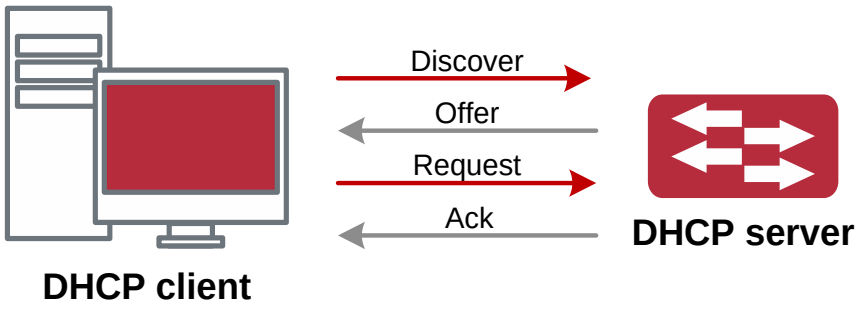
Если самообращенный ARP включен глобально, он может быть выключен только глобально. Если самообращенный ARP включен на интерфейсе, он может быть выключен только на интерфейсе.

26 КОНФИГУРАЦИЯ DHCP

26.1 Введение DHCP

DHCP [RFC2131] сокращенно от Dynamic Host Configuration Protocol (протокол динамической настройки хостов). Это протокол, который динамически назначает IP адрес из пула адресов, так же устанавливает другие сетевые параметры, такие как шлюз по умолчанию, DNS сервер и расположение в сети файла образа. DHCP это расширенная версия BOOTP. Это основная технология, которая не только может обеспечить загрузочной информацией бездисковые рабочие станции, но так же может освободить администраторов от ручного ведения IP адресного пространства и упростить пользователям процесс настройки. Еще одно преимущество DHCP в том, что он может снизить требования к количеству IP адресов, когда пользователь покидает сеть, его IP может быть назначен другому.

DHCP является протоколом типа «клиент-сервер», DHCP клиент запрашивает у DHCP сервера сетевой адрес и параметры конфигурации, сервер предоставляет клиенту сетевой адрес и параметры конфигурации. Если клиент и сервер находятся в разных подсетях, необходимо использовать DHCP ретранслятор (relay) для передачи DHCP пакетов между клиентом и сервером. Реализация DHCP представлена ниже:



Взаимодействие протокола DHCP

Разъяснение:

DHCP клиент рассылает в локальную подсеть широковещательные пакты DHCPDISCOVER.

DHCP сервер при получении пакета DHCPDISCOVER отправляет DHCP клиенту пакет DHCPOFFER вместе с IP адресами и другими сетевыми параметрами.

DHCP шлет широковещательный пакет DHCPREQUEST с информацией о DHCP сервере, который он выбрал из DHCPOFFER пакетов.

Выбранный клиентом DHCP сервер отправляет пакет DHCPACK и клиент получает IP адрес и другие параметры.

Эти четыре шага производят процесс динамической настройки хоста.

Однако, если DHCP сервер и DHCP клиент находятся в разных подсетях, сервер не получит широковещательные DHCP пакеты, отправленные клиентом и не ответит ему. В этом случае необходим DHCP ретранслятор (relay) для передачи таких DHCP пакетов между клиентом и сервером.

Коммутатор может работать и как DHCP сервер, и как DHCP ретранслятор. DHCP поддерживает не только динамическое назначение IP адресов, но так же ручную привязку адреса (например, указать определенный IP адрес для определенного MAC адреса или определенного ID устройства). Различия между динамическим и статическим назначением адресов: 1) динамически получаемый адрес может быть каждый раз разным; привязанный вручную адрес всегда будет одинаковый. 2) Время аренды IP адреса, полученного динамически, одинаково для всего адресного пула, и оно ограничено. Время аренды IP адреса, привязанного вручную, теоретически бесконечно. 3) Динамически выделяемые адреса не могут быть привязаны вручную. 4) Пул динамических адресов может наследовать параметры конфигурации сети пула динамических адресов, относящегося к сегменту.

26.2 DHCP Server Configuration

Список задач конфигурации DHCP сервера:

1. Включить/выключить сервис DHCP
2. Настроить адресный пул DHCP
(1) Создать/удалить адресный пул DHCP
(2) Настроить параметры адресного пула DHCP
(3) Настроить параметры ручного адресного пула DHCP
3. Включить ведение журнала для конфликтов адресов

1. Включить/выключить сервис DHCP

Команда	Описание
Общий режим	
service dhcp **no service dhcp**	Включить/выключить сервис DHCP.
Режим конфигурировани порта	
ip dhcp disbale **no ip dhcp disable**	Отключение не порте DHCP обслуживания, команда no отменяет отключение.

2. Настроить адресный пул DHCP
(1) Создать/удалить адресный пул DHCP

Команда	Описание
Общий режим	
ip dhcp pool <*name*> **no ip dhcp pool <*name*>**	Настроить адресный пул DHCP. Команда no отменяет пул адресов DHCP.

(2) Настроить параметры адресного пула DHCP

Команда	Описание
Режим адресного пула DHCP	
network-address <*network-number*> [mask | prefix-length] **no network-address**	Настройка области адресов, которые могут быть выделены адресному пулу. Команда no отменяет выделение адресного пула.
default-router [<addresSwitchA>[<addresSwitchB>[…<address8>]]] **no default-router**	Настройка шлюза по умолчанию для DHCP клиентов. Команда no отменяет шлюз по умолчанию.
dns-server [<addresSwitchA>[<addresSwitchB>[…<address8>]]] **no dns-server**	Настройка DNS сервера для DHCP клиентов. Команда no отменяет настройку DNS сервера.
domain-name <*domain*> **no domain-name**	Настройка доменного имени для DHCP клиентов. Команда no отменяет доменное имя.
netbios-name-server [<addresSwitchA>[<addresSwitchB>[…<address8>]]] **no netbios-name-server**	Настройка адреса WINS сервера. Команда no отменяет настройку.
netbios-node-type {b-node|h-node|m-node|p-node|<*type-number*>} **no netbios-node-type**	Настройка типа узла для DHCP клиентов. Команда no отменяет тип узла.
bootfile <filename> **no bootfile**	Настройка загрузочного файла для DHCP клиентов. Команда no отменяет загрузочный файл.
next-server [<addresSwitchA>[<addresSwitchB>[…<address8>]]] **no next-server [<addresSwitchA>[<addresSwitchB>[…<address8>]]]**	Настройка адреса сервера, размещающего загрузочный файл. Команда no отменяет удаляет адрес сервера.
option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>} **no option <*code*>**	Настройка сетевого параметра, определенного кодом опции. Команда no удаляет сетевой параметр.
lease {days [hours][minutes] | infinite} **no lease**	Настройка времени аренды адресов пула. Команда no удаляет настройку времени аренды.

max-lease-time {[<*days*>] [<*hours*>] [<*minutes*>] | infinite} **no max-lease-time**	Настройка максимальноговремени аренды адресов в адресном пуле, команда no восстанавливает настройки по умолчанию.
Общий режим	
ip dhcp excluded-address <*low-address*> [<*high-address*>] **no ip dhcp excluded-address <*low-address*> [<*high-address*>]**	Исключение из адресного пула адресов, которые не предназначены для динамического выделения.

(3) Настроить параметры ручного адресного пула DHCP

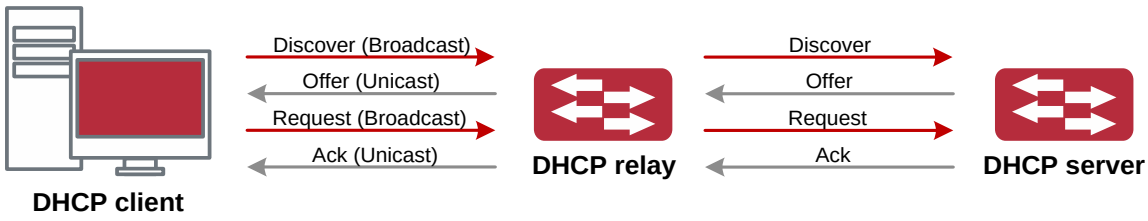
Команда	Описание
Режим адресного пула DHCP	
hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}] **no hardware-address**	Задать/удалить аппаратный адрес, при ручном назначении адреса.
host <address> [<mask> | <prefix-length>] **no host**	Задать/удалить IP адрес, который будет назначен заданному клиенту.
client-identifier <unique-identifier> **no client-identifier**	Задать/удалить уникальный ID пользователя.

3. Включить ведение журнала для конфликтов адресов

Команда	Описание
Общий режим	
ip dhcp conflict logging **no ip dhcp conflict logging**	Включить/выключить ведение журнала для DHCP адресов, чтобы обнаружить конфликты адресов.
Режим администратора	
clear ip dhcp conflict <*address* | all >	Удалить единичную запись конфликта или удалить все записи.

26.3 Конфигурация DHCP ретранслятора

Когда DHCP клиент и сервер находятся в разных сегментах, для передачи DHCP пакетов необходим DHCP ретранслятор. Использование DHCP ретранслятора делает необязательным настройку DHCP сервера для каждого сегмента, один DHCP сервер может обслуживать несколько сегментов, что эффективнее не только с точки зрения затрат, но и с точки зрения управления.



DHCP ретнанслятор

Как показано на рисунке, DHCP клиент и DHCP сервер находятся в разных подсетях. DHCP клиент выполняет те же четыре шага DHCP, как обычно, только к процессу добавлен DHCP ретранслятор.

Клиент шлет широковещательный пакет DHCPDISCOVER, DHCP ретранслятор вставляет свой собственный IP адрес в поле «relay agent» в пакете DHCPDISCOVER и пересылает пакет указанному DHCP серверу (для описания формата DHCP кадра обратитесь к RFC2131).

При получении пакета DHCPDISCOVER, пересылаемого через DHCP ретранслятор, DHCP сервер шлет клиенту пакет DHCPOFFER через DHCP ретранслятор.

DHCP клиент выбирает сервер и шлет широковещательный пакет DHCPREQUEST, DHCP ретранслятор таким же образом пересылает его серверу.

При получении пакета DHCPDISCOVER, пересылаемого через DHCP ретранслятор, DHCP сервер шлет клиенту пакет DHCPACK через DHCP ретранслятор.

Список задач конфигурации DHCP:

1. Включить DHCP ретранслятор.
2. Настроить DHCP ретранслятор для пересылки широковещательных DHCP пакетов.
3. Настройка share-vlan.

1. Включить DHCP ретранслятор.

Команда	Описание
Общий режим	
service dhcp **no service dhcp**	DHCP сервер и DHCP ретранслятор включаются при включении сервиса DHCP.

2. Настроить DHCP ретранслятор для пересылки широковещательных DHCP пакетов.

Команда	Описание
Общий режим	
ip forward-protocol udp bootps **no ip forward-protocol udp bootps**	Порт UDP 67 используется для пересылки широковещательных пакетов DHCP.
Режим конфигурации интерфейса	
ip helper-address *<ipaddress>* **no ip helper-address *<ipaddress>***	Установить адрес DHCP сервера. Команда **no ip helper-address <ipaddress>** отменяет настройку.

3. Настройка share-vlan.

Когда пользователь хочет использовать устройство второго уровня как DHCP ретранслятор, количество которых ограничего, то пользователь создает интерфейс третьего уровня на устройстве второго уровня, но использование интерфейса третьего уровня для share-vlan (может включать несколько sub-vlan, однако sub-vlan только соответствует share-vlan) может осуществлять DHCP ретранслятор, и одновременно на устройстве-ретрансляторе нужно включить опцию 82.

Команда	Описание
Общий режим	
ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist> **no dhcp relay share-vlan**	Создает/удаляет share-vlan и sub-vlan.

26.4 Примеры конфигурации DHCP

Сценарий 1:

Чтобы упростить настройку, компания использует коммутатор в качестве DHCP сервера. Адрес в VLAN-е управления - 10.16.1.2/16. Локальная сеть разделена на две сети – A и B, в соответствии с расположением офисов. Настройки сети для расположений A и B показаны ниже.

Пул A (сеть 10.16.1.0)		**Пул B (сеть 10.16.2.0)**	
Устройство	IP address	**Устройство**	IP address
Шлюз по умолчанию	10.16.1.200 10.16.1.201	**Шлюз по умолчанию**	10.16.1.200 10.16.1.201
DNS сервер	10.16.1.202	**DNS сервер**	10.16.1.202
WINS сервер	10.16.1.209	**WWW сервер**	10.16.1.209

Тип узла WINS	H-узел		
Время аренды	3 дня	**Время аренды**	1 день

В расположении A машине с MAC адресом 08-c6-b3-23-dc-ab назначен фиксированный IP адрес 10.16.1.210 и имя хоста «management».

```
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 08-c6-b3-23-dc-ab
Switch(dhcp-A1-config)#exit
```

Руководство по использованию: Когда DHCP/BOOTP клиент подключается к VLAN1 порту коммутатора, клиент может получить адрес только из сети 10.16.1.0/24 вместо 10.16.2.0/24. Это потому, что широковещательный пакет от клиента будет запрашивать IP адрес в том же сегменте VLAN интерфейса, а IP адрес VLAN интерфейса - 10.16.1.2/24, поэтому адрес, назначаемый клиенту, будет принадлежать сети 10.16.1.0/24.

Если DHCP/BOOTP клиент хочет получить адрес в сети 10.16.2.0/24, шлюз, пересылающий широковещательные пакеты клиента, должен принадлежать сети 10.16.2.0/24. Чтобы клиент получил адрес из пула 10.16.2.0/24, должна быть обеспечена связность между клиентским шлюзом и коммутатором.

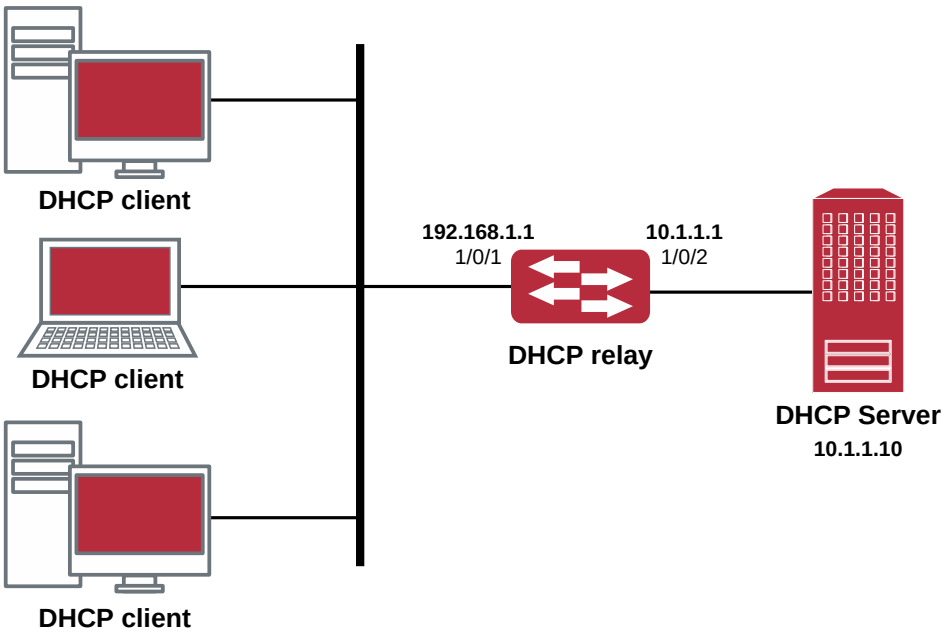
Сценарий 2:

Как показано на рисунке, маршрутизирующий коммутатор настроен в качестве DHCP ретранслятора. Адрес DHCP сервера - 10.1.1.10. Шаги конфигурации, следующие:

```
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
```

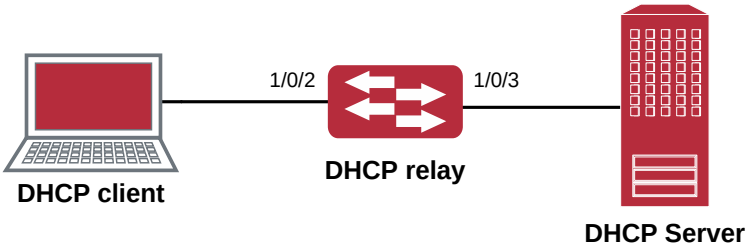
```
Switch(Config-Erthernet1/0/2)#switchport access vlan 2
Switch(Config-Erthernet1/0/2)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#ip forward-protocol udp bootps
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip help-address 10.1.1.10
Switch(Config-if-Vlan1)#exit
```

Заметка: Рекомендуется использовать комбинацию команд `ip forward-protocol udp <port>` и `ip helper-address <ipaddress>`. Команда `ip help-address` может быть настроена только на портах 3-го уровня и не может быть настроена на портах 2-го уровня.



Конфигурация DHCP ретранслятора

Сценарий 3:



Как показано на рисунке, клиент получает адрес через DHCP ретранслятор. Коммутатор является устройством второго уровня доступа с включенным DHCP-ретранслятором и опцией 82. Ethernet1/0/2 является портом доступа, включенным в VLAN3, Ethernet1/0/3 является транковым портом, соединненым с DHCP сервером, адрес которого 192.168.40.199. На коммутаторе создаются vlan 1 и интерфейс vlan 1,

настраивается IP адрес 192.168.40.50. Адрес DHCP-ретранслятора настраивается 192.168.40.199, и vlan3 настраивается как sub-vlan vlan1.

Конфигурация:

```
switch(config)#vlan 1
switch(config)#vlan 3
switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#switchport access vlan 3
switch(config)#interface ethernet 1/0/3
Switch(Config-If-Ethernet1/0/2)#switchport mode trunk
switch(config)#service dhcp
switch(config)#ip forward-protocol udp bootps
switch(config)#ip dhcp relay information option
switch(config)#ip dhcp relay share-vlan 1 sub-vlan 3
switch(config-if-vlan1)#ip address 192.168.40.50 255.255.255.0
switch(config-if-vlan1)#ip helper-address 192.168.40.199
```

26.5 Поиск неисправностей DHCP

Если DHCP клиенты не получают IP адреса и другие параметры сети, после проверки кабелей и клиентского оборудования, следует выполнить следующее:

Проверьте, запущен ли DHCP сервер, запустите его, если он не запущен. Если DHCP клиенты и серверы находятся не в одной физической сети, проверьте, имеет ли маршрутизатор, отвечающий за пересылку DHCP пакетов, функцию DHCP ретранслятора. Если на промежуточном маршрутизаторе нет функции DHCP ретранслятора, рекомендуется заменить этот роутер или обновить его ПО.

В таком случае, DHCP сервер должен быть проверен на предмет наличия адресного пула в том же сегменте, что и VLAN коммутатора, если такой пул не существует, его необходимо добавить.

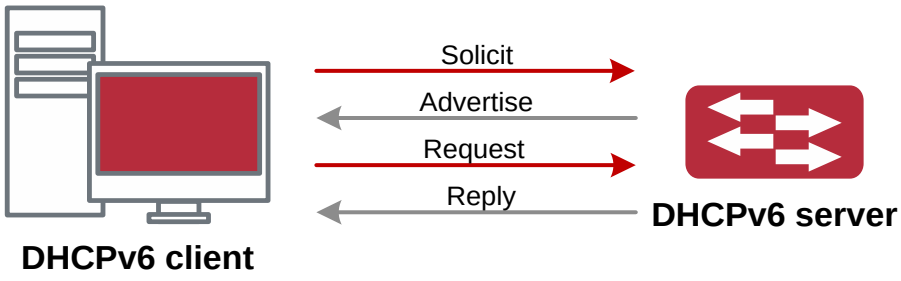
Адресный пул может быть либо динамическим, либо статическим. Например, если в пуле присутствуют команды «network-address» и «host», только одна из них вступит в силу. Кроме того, в ручной привязке только одна привязка IP-MAC может быть настроена в каждом пуле. Если необходимо несколько привязок, нужно создать отдельный адресный пул для каждой из них. Новая конфигурация в старом пуле перезапишет старую.

27 КОНФИГУРАЦИЯ DHCPV6

27.1 Введение DHCPv6

DHCPv6 [RFC3315] это IPv6 версия протокола динамической конфигурации хостов (DHCP). Этот протокол назначает IPv6 адреса и другие параметры настройки сети такие как: адрес DNS и доменное имя DHCP клиента, DHCPv6 является условной автоматической конфигурацией протокола IPv6. В процессе настройки адреса DHCP сервер присваивает IP адрес клиенту и предоставляет DNS адрес, доменное имя и информацию другой настройки, пакет DHCP может передаваться через делегированный ретранслятор, настройки адреса IPv6 и клиента записаны на сервере DHCPv6, все это повышает эффективность управления сетью. DHCPv6 может обеспечить расширенную функцию делегации префиксов. DHCPv6 сервер так же обеспечивает DHCPv6 сервис без отслеживания состояния, при котором назначаются только параметры конфигурации, такие как адрес DNS сервера и доменное имя, но не назначается IPv6 адрес.

Есть три объекта в протоколе DHCPv6 – клиент, сервер и ретранслятор. Протокол DHCPv6 основан на протоколе UDP. Клиент DHCPv6 отправляет запрос DHCP серверу или DHCP ретранслятору на порт назначения 547, DHCP сервер (или ретранслятор) отправляют ответы на порт назначения 546. DHCP клиент отправляет запросы (solicit) и заявки (request) DHCP серверу на multicast адрес ff02::1:2.



Согласование DHCPv6

Когда DHCPv6 клиент пытается запросить у DHCPv6 сервера IPv6 адрес и другие параметры, клиент должен сначала найти DHCPv6 сервер, затем уже запросить конфигурация у сервера.

Для обнаружения сервера DHCP клиент рассылает пакеты SOLICIT (запрос) на широковещательный адрес FF02::1:2.

Каждый DHCP сервер, получивший запрос, ответит клиенту сообщением ADVERTISE (предложение), которое содержит идентификатор сервера (DIUD) и его приоритет.

Возможно, что клиент получит несколько сообщений ADVERTISE. Клиент должен выбрать один сервер и ответить ему сообщением REQUEST (заявка), чтобы запросить адрес, предложенный в сообщении ADVERTISE.

Затем выбранный DHCPv6 сервер сообщением REPLY (ответ) подтверждает назначение клиенту IPv6 адреса и других настроек.

Данные четыре шага завершают процесс динамической настройки хоста. Тем не менее, если DHCPv6 сервер и DHCPv6 клиент не находятся в одной сети, сервер не получит широковещательный запрос от клиента и не ответит ему. В этом случае необходим DHCPv6

ретранслятор(relay), чтобы пересылать запросы между клиентом и сервером. В коммутаторе реализованы функции DHCPv6 сервера, relay и клиента делегации префиксов. Когда DHCPv6 ретранслятор получает сообщение от DHCPv6 клиента, он инкапсулирует его в пакет Relay-forward и доставляет следующему DHCPv6 ретранслятору или серверу. Приходящие от сервера к ретранслятору DHPCv6 сообщения инкапсулированы в пакет Relay-reply. Ретранслятор убирает инкапсуляцию и доставляет пакет DHCPv6 клиенту или следующему ретранслятору в сети.

В случае делегации IPv6 префиксов DHCPv6 сервер настроен на маршрутизаторе провайдера, а DHCPv6 клиент настроен на маршрутизаторе клиента, маршрутизатор клиента шлет маршрутизатору провайдера запрос на выделение префикса адресов и получает предварительно настроенный префикс, не настраевая префикс вручную. Затем клиентский маршрутизатор делит полученный префикс (длина которого не может быть меньше 64) на 64 подсети. Данные префиксы будут анонсированы сообщениями объявления маршрутизатора (RA) хостам, подключенным напрямую к клиенту.

27.2 Конфигурация DHCPv6 сервера

Список задач конфигурации DHCPv6 сервера:

1. Включить/выключить сервис DHCPv6
2. Настроить адресный пул DHCPv6
(1) Создать/удалить адресный пул DHCPv6
(2) Настроить параметры адресного пула DHCPv6
3. Включить функцию DHCPv6 сервера на порту

1. Включить/выключить сервис DHCPv6

Команда	Описание
Общий режим	
service dhcpv6 **no service dhcpv6**	Включить/выключить сервис DHCPv6.

2. Настроить адресный пул DHCPv6
(1) Создать/удалить адресный пул DHCPv6

Команда	Описание
Общий режим	
ipv6 dhcp pool <*poolname*> **no ipv6 dhcp pool <*poolname*>**	Создать/удалить адресный пул DHCPv6.

(2) Настроить параметры адресного пула DHCPv6

Команда	Описание
Режим конфигурации адресного пула DHCPv6	
network-address <ipv6-pool-start-address> {<ipv6-pool-end-address> | <prefix-length>} [eui-64] **no network-address**	Настроить диапазон IPv6 адресов, назначаемый пулом
dns-server <ipv6-address> **no dns-server *<ipv6-address>***	Настроить адрес DNS сервера для DHCPv6 клиента.
domain-name <domain-name> **no domain-name *<domain-name>***	Настроить доменное имя DHCPv6 клиента.
excluded-address *<ipv6-address>* **no excluded-address *<ipv6-address>***	Исключить IPv6 адрес, который не будет наначаться динамически.
lifetime {*<valid-time>* | infinity} {*<preferred-time>* | infinity} **no lifetime**	Настроить время действия или предпочтительное время адресного пула DHCPv6.

3. Включить функцию DHCPv6 сервера на порту.

Команда	Описание
Режим конфигурации интерфейса	
ipv6 dhcp server *<poolname>* [preference *<value>*] [rapid-commit] [allow-hint] **no ipv6 dhcp server *<poolname>***	Включить функцию DHCPv6 сервера на определенном порту и привязать используемый DHCPv6 адресный пул.

27.3 Конфигурация DHCPv6 ретранслятора

1. Список задач конфигурации DHCPv6 ретранслятора:
2. Включить/выключить сервис DHCPv6
3. Настроить DHCPv6 ретранслятор на порту

1. Включить/выключить сервис DHCPv6

Команда	Описание
Общий режим	
service dhcpv6 **no service dhcpv6**	Включить/выключить сервис DHCPv6.

2. Настроить DHCPv6 ретранслятор на порту

Команда	Описание
Режим конфигурации интерфейса	
ipv6 dhcp relay destination {[*<ipv6-address>*] [interface {*<interface-name>* | vlan *<1-4096>*}]} **no ipv6 dhcp relay destination {[*<ipv6-address>*] [interface {*<interface-name>* | vlan *<1-4096>*}]}**	Указать адрес назначения для передачи DHCPv6 пакетов. Команда no удаляет настройку.

27.4 Конфигурация сервера делегации префиксов DHCPV6

Список задач конфигурации сервера делегации префиксов DHCPv6:

1. Включить/выключить сервис DHCPv6
2. Настроить пул делегации префиксов
3. Настроить адресный пул DHCPv6
(1) Создать/удалить адресный пул DHCPv6
(2) Настроить пул делегации префиксов, используемый адресным пулом
(3) Настроить статическую привязку делегации префиксов
(4) Настроить другие параметры адресного пула DHCPv6
4. Включить функцию сервера делегации префиксов DHCPv6 на порту

1. Включить/выключить сервис DHCPv6

Команда	Описание
Общий режим	
service dhcpv6 **no service dhcpv6**	Включить/выключить сервис DHCPv6.

2. Настроить пул делегации префиксов

Команда	Описание
Общий режим	
ipv6 local pool <poolname> <prefix|prefix-length> <assigned-length> **no ipv6 local pool *<poolname>***	Настроить пул делегации префиксов.

3. Настроить адресный пул DHCPv6

(1) Создать/удалить адресный пул DHCPv6

Команда	Описание
Общий режим	
ipv6 dhcp pool <*poolname*> **no ipv6 dhcp pool <*poolname*>**	Создать/удалить адресный пул DHCPv6.

(2) Настроить пул делегации префиксов, используемый

Команда	Описание
Режим конфигурации адресного пула DHCPv6	
prefix-delegation pool <*poolname*> [lifetime {<*valid-time*> / infinity} {<*preferred-time*> | infinity}] **no prefix-delegation pool <*poolname*>**	Указать пул делегации префиксов, используемый адресным пулом и назначить префикс клиенту.

(3) Настроить статическую привязку делегации префиксов

Команда	Описание
Режим конфигурации адресного пула DHCPv6	
prefix-delegation <*ipv6-prefix/prefix-length*> <*client-DUID*> [iaid <*iaid*>] [lifetime {<valid-time> | infinity} {<*preferred-time*> | infinity}] **no prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]**	Настроить статическую привязку делегации префиксов.

(4) Настроить другие параметры адресного пула DHCPv6

Команда	Описание
Режим конфигурации адресного пула DHCPv6	
dns-server <ipv6-address> **no dns-server <*ipv6-address*>**	Настроить адрес DNS сервера для DHCPv6 клиента.
domain-name <domain-name> **no domain-name <*domain-name*>**	Настроить доменное имя DHCPv6 клиента.

4. Включить функцию сервера делегации префиксов DHCPv6 на порту

Команда	Описание
Режим конфигурации интерфейса	
ipv6 dhcp server *<poolname>* [preference *<value>*] [rapid-commit] [allow-hint] **no ipv6 dhcp server *<poolname>***	Включить функцию DHCPv6 сервера на определенном порту и привязать используемый DHCPv6 адресный пул.

27.5 Конфигурация клиента делегации префиксов DHCPv6

Список задач конфигурации клиента делегации префиксов DHCPv6:

1. Включить/выключить сервис DHCPv6
2. Включить функцию клиента делегации префиксов DHCPv6 на проту

1. Включить/выключить сервис DHCPv6

Команда	Описание
Общий режим	
service dhcpv6 **no service dhcpv6**	Включить/выключить сервис DHCPv6.

2. Включить функцию клиента делегации префиксов DHCPv6 на проту

Команда	Описание
Режим конфигурации интерфейса	
ipv6 dhcp client pd *<prefix-name>* [rapid-commit] **no ipv6 dhcp client pd**	Включить функцию клиента делегации префиксов DHCPv6 на проту и ассоциацию полученного префикса с настроенным универсальным префиксом.

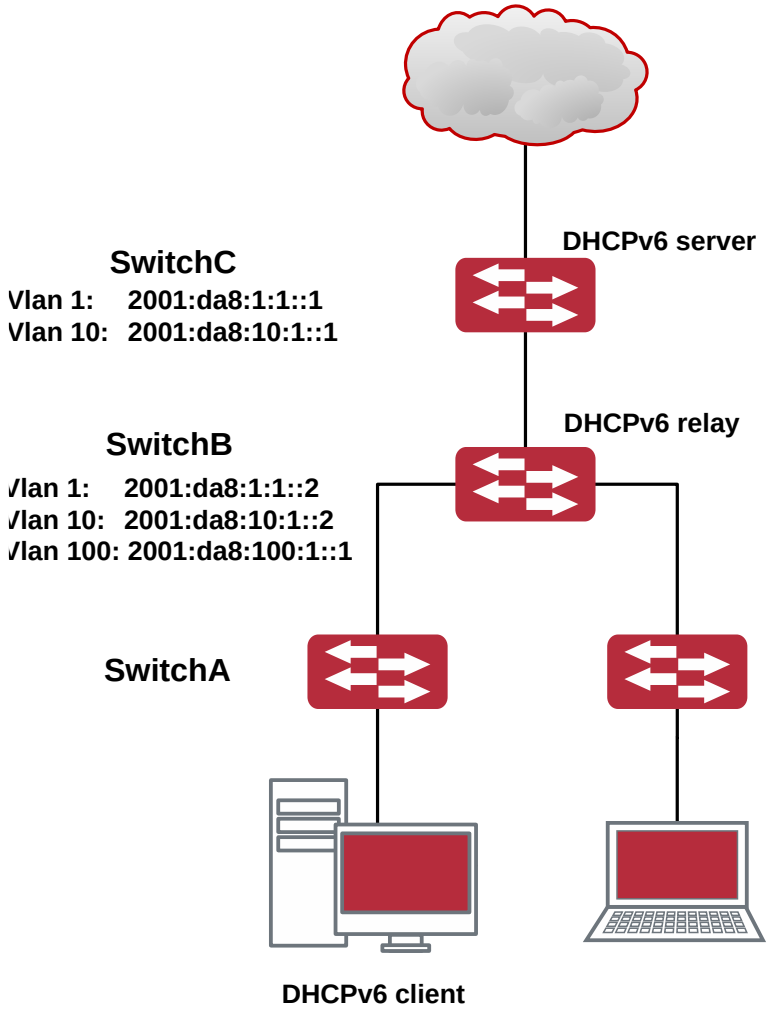
27.6 Примеры конфигурации DHCPv6

Пример 1:

При развертывании сетей IPv6 коммутаторы серии могут быть настроены в качестве DHPv6 серверов для управления распределением адресов IPv6. Поддерживаются оба режима DHCPv6 – с отслеживанием состояния и без него.

Топология:

На уровне доступа используется коммутатор 1 для подключения пользователей общежития. На первом уровне агрегации коммутатор 2 настроен как DHCPv6 ретранслятор. На втором уровне агрегации коммутатор 3 настроен как DHCPv6 сервер и соединен с магистральной сетью. На компьютерах должна быть установлена ОС не ниже Windows Vista, или любая другая в которой есть DHCPv6 клиент.



Конфигурация SwitchC:

```
SwitchC>enable
SwitchC#config
SwitchC(config)#service dhcpv6
SwitchC(config)#ipv6 dhcp pool EastDormPool
SwitchC(dhcpv6-EastDormPool-config)#network-address    2001:da8:100:1::1
2001:da8:100:1::100
SwitchC(dhcpv6-EastDormPool-config)#excluded-address 2001:da8:100:1::1
SwitchC(dhcpv6-EastDormPool-config)#dns-server 2001:da8::20
SwitchC(dhcpv6-EastDormPool-config)#dns-server 2001:da8::21
SwitchC(dhcpv6-EastDormPool-config)#domain-name dhcpv6.com
SwitchC(dhcpv6-EastDormPool-config)#lifetime 1000 600
SwitchC(dhcpv6-EastDormPool-config)#exit
SwitchC(config)#interface vlan 1
SwitchC(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::1/0/64
SwitchC(Config-if-Vlan1)#exit
SwitchC(config)#interface vlan 10
SwitchC(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::1/0/64
SwitchC(Config-if-Vlan10)#ipv6 dhcp server EastDormPool preference 80
SwitchC(Config-if-Vlan10)#exit
SwitchC(config)#
```

```
Конфигурация SwitchB:
SwitchB>enable
SwitchB#config
SwitchB(config)#service dhcpv6
SwitchB(config)#interface vlan 1
SwitchB(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::2/64
SwitchB(Config-if-Vlan1)#exit
SwitchB(config)#interface vlan 10
SwitchB(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::2/64
SwitchB(Config-if-Vlan10)#exit
SwitchB(config)#interface vlan 100
SwitchB(Config-if-Vlan100)#ipv6 address 2001:da8:100:1::1/0/64
SwitchB(Config-if-Vlan100)#no ipv6 nd suppress-ra
SwitchB(Config-if-Vlan100)#ipv6 nd managed-config-flag
SwitchB(Config-if-Vlan100)#ipv6 nd other-config-flag
SwitchB(Config-if-Vlan100)#ipv6 dhcp relay destination 2001:da8:10:1::1
SwitchB(Config-if-Vlan100)#exit
SwitchB(config)#
```

27.7 Поиск несиправностей DHCPv6

Если DHCPv6 клиент не может получить IPv6 адрес и другие сетевые параметры, после проверки кабелей и клиентского оборудования следует выполнить следующее:

❖ Проверьте, запущен ли DHCPv6 сервер, запустите его, если он не запущен. Если DHCPv6 клиенты и серверы находятся не в одной физической сети, проверьте, имеет ли маршрутизатор, отвечающий за пересылку DHCPv6 пакетов, функцию DHCPv6 ретранслятора. Если на промежуточном маршрутизаторе нет функции DHCPv6 ретранслятора, рекомендуется заменить этот роутер или обновить его ПО.

❖ Иногда хосты, подключенные к коммутаторам со включенным DHCPv6, не могут получить IPv6 адрес. В этой ситуации в первую очередь необходимо проверить, подключены ли порты, к которым подключены хосты, к порту, к которому подключен DHCPv6 сервер. Если подключено напрямую, убедиться, что адресный пул IPv6 VLAN-а, к которому принадлежит порт, находится в одной подсети с адресным пулом, настроенным на DHCPv6 сервере. Если подключены не на прямую, и между хостом и сервером настроен DHCPv6 ретранслятор, необходимо в первую очередь проверить, настроен ли правильный IPv6 адрес на интерфейсе коммутатора, к которому подключаются хосты. Если не настроен, настроить правильный IPv6 адрес. Если настроен, необходимо проверить, в одной ли подсети с DHCPv6 сервером находится настроенный IPv6 адрес. Если нет, пожалуйста, добавьте его в адресный пул.

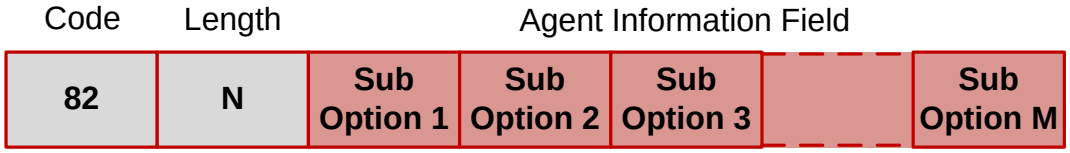
28 КОНФИГУРАЦИЯ ОПЦИИ 82 DHCP

28.1 Введение в опцию 82 DHCP

Опция 82 DHCP это опция информации ретранслирующего агента (Relay Agent). Опция 82 DHCP направлена на укрепление безопасности серверов DHCP и улучшения политики конфигурации IP адресов. Ретранслирующий агент добавляет опцию 82 (включающую физический порт доступа клиента, идентификатор устройства доступа и другую информацию) в DHCP запрос, полученный от клиента, затем пересылает его DHCP серверу. Когда DHCP сервер, который поддерживает функцию опции 82, получает сообщение, он выделяет клиенту IP адрес и другие параметры в соответствии с преднастроенными политиками и информацией в опции 82. В то же время DHCP сервер может идентифицировать все возможные атаки DHCP сообщениями в соответствии с информацией в опции 82 и защитить от них. DHCP ретранслирующий агент снимет опцию 82 с ответного сообщения и передаст его определенному порту устройства доступа, в соответствии с информацией о физическом порте в опции. Применение опции 82 DHCP прозрачно для клиента.

28.1.1 Структура сообщения опции 82 DHCP

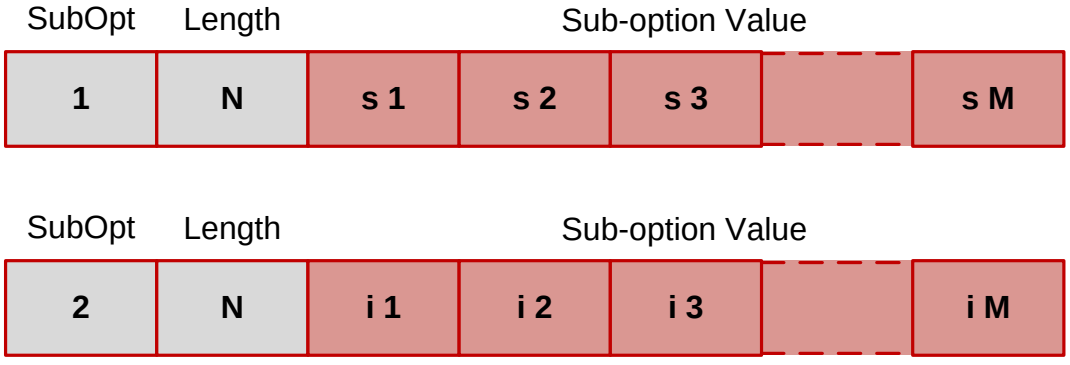
Сообщение DHCP может иметь несколько сегментов опций, опция 82 один из них. Она должна быть после других опций, но до опции 255. Вот ее формат:



Code: представляет порядковый номер опции информации ретранслирующего агента, опция 82 так называется потому, что RFC3046 определяет ее как 82.

Len: количество байт в поле информации агента, не включая два байта в сегменте Code и сегменте Len.

Опция 82 может иметь несколько суб-опций, требуется как минимум одна суб-опция. RFC3046 определяет следующие две суб-опции, формат которых показан ниже:



SubOpt: порядковый номер суб-опции, порядковый номер суб-опции Circuit-ID – 1, порядковый номер суб-опции Remote ID – 2.

Len: количество байт в суб-опции, не включая два байта в сегменте SubOpt и сегменте Len.

28.1.2 Механизм работы опции 82

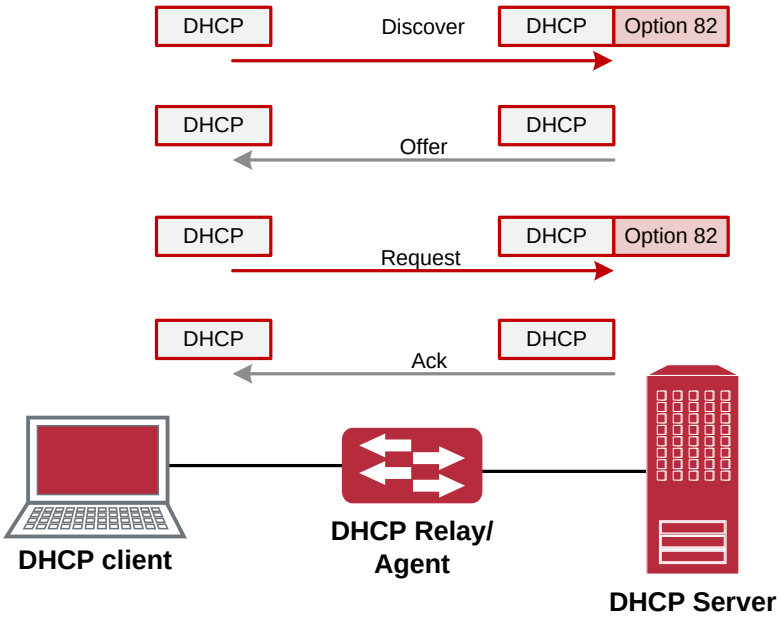


Диаграмма потоков опции 82 DHCP

Если DHCP ретранслирующий агент поддерживает опцию 82, DHCP клиент должен пройти следующие четыре шага, чтобы получить IP адрес от DHCP сервера: discover, offer, select и acknowledge. Протокол DHCP следует приведенной ниже процедуре:

1) DHCP клиент при инициализации посылает широковещательное сообщение запроса. Это сообщение не имеет опции 82.

2) DHCP ретранслирующий агент добавит опцию 82 к сообщению запроса, которое он получит, затем перешлет это сообщение DHCP серверу. По умолчанию суб-опция 1 опции 82 (Circuit ID) это информация об интерфейсе, к которому подключен DHCP клиент (VLAN и физической порт), но пользователь может настроить Circuit ID по своему усмотрению. Суб-опция 2 опции 82 (Remote ID) это MAC адрес устройства DHCP ретранслятора.

3) После получения DHCP запроса DHCP сервер выделит клиенту IP адрес и другую информацию, в соответствии с преднастроенными политиками и информацией в опции 82. Затем он направит DHCP ретранслирующему агенту ответное сообщение с DHCP конфигурацией и опцией 82.

4) DHCP ретранслирующий агент очистит ответное сообщение от опции 82 и направит его клиенту.

28.2 Список задач конфигурации опции 82 DHCP

1. Включить опцию 82 DHCP ретранслирующего агента

2. Настроить атрибуты интерфейса опции 82 DHCP
3. Включить опцию 82 DHCP сервера
4. Настроить формат по умолчанию опции 82 DHCP ретранслирующего агента
5. Настроить разделитель
6. Настроить метод создания опции 82
7. Проводить диагностику и поддержку опции 82 DHCP

1. Включить опцию 82 DHCP ретранслирующего агента.

Команда	Описание
Общий режим	
ip dhcp relay information option **no ip dhcp relay information option**	Включает функции опции 82 на ретранслирующем агенте коммутатора. Команда no выключает функцию.

2. Настроить атрибуты интерфейса опции 82 DHCP

Команда	Описание
Режим конфигурации интерфейса	
ip dhcp relay information policy {drop | keep | replace} **no ip dhcp relay information policy**	Устанавливает политики ретрансляции сообщения, которое уже содержит опцию 82. Режим drop означает, что сообщение, содержадее опцию 82, будет отброшено без какой либо обработки. Режим keep означает, что система оставит оригинальную опцию 82 и передаст сообщение серверу. Режим replace означает, что система заменит существующую опцию 82 своей и передаст сообщение серверу. Команда no установит политику в режим по умолчанию – **replace**.
Ip dhcp relay information option subscriber-id {standard | *<circuit-id>*} **no ip dhcp relay information option subscriber-id**	Устанавливает формат суб-опции 1 опции 82 (*Circuit* ID), **standard** означает стандартные названия VLAN и физического порта, например «Vlan2+Ethernet1/0//12», <**circuit-id**> это сожержание circuit-id, заданного пользователем (строка не более 64 символов). Команда no установит стандартный формат.
Общий режим	

ip dhcp relay information option remote-id {standard | *<remote-id>*} **no ip dhcp relay information option remote-id**	Устанавливает формат суб-опции 1 опции 82 (Remote ID). Команда no установит стандартный формат.

3. Включить опцию 82 DHCP сервера.

Команда	Описание
Общий режим	
ip dhcp server relay information enable **no ip dhcp server relay information enable**	Позволяет DHCP серверу коммутатора идентифицировать опцию 82. Команда no отключает эту функцию.

4. Настроить формат по умолчанию опции 82 DHCP ретранслирующего агента

Команда	Описание
Общий режим	
ip dhcp relay information option subscriber-id format {hex | acsii | vs-hp}	Устанавливает формат subscriber-id опции 82 ретранслирующего агента.
ip dhcp relay information option remote-id format {default | vs-hp}	Устанавливает формат remote-id опции 82 ретранслирующего агента.

5. Настроить разделитель

Команда	Описание
Общий режим	
ip dhcp relay information option delimiter [colon | dot | slash | space] **no ip dhcp relay information option delimiter**	Настраивает разделитель каждого параметра субопций в опции 82 в глобальном режиме. Команда no восстанавливает разделитель по умолчанию – **slash**.

6. Настроить медот создания опции 82

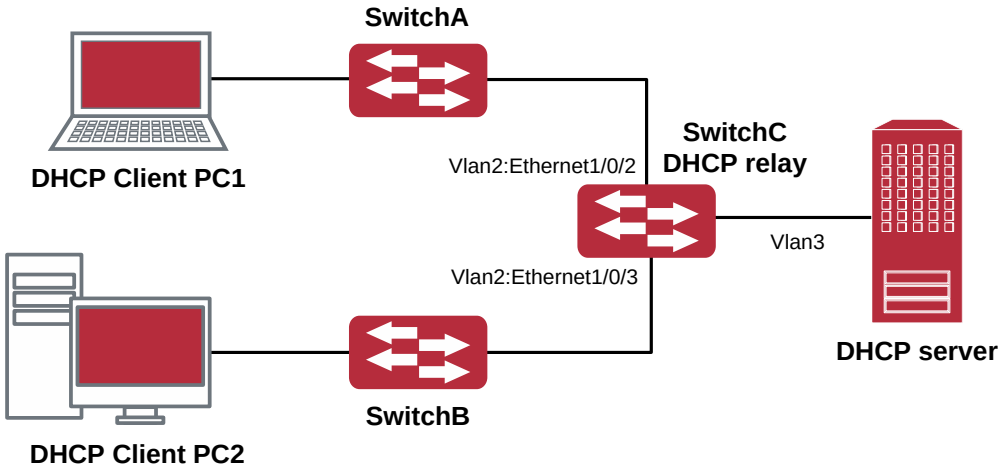
Команда	Описание
Общий режим	
ip dhcp relay information option self-defined remote-id {hostname | mac | string WORD}	Устанавливает медот создания опции 82, пользователи могут

no ip dhcp relay information option self-defined remote-id	самостоятельно определить параметры суб-опции remote-id.
ip dhcp relay information option self-defined remote-id format [ascii | hex]	Устанавливает пользовательский формат remote-id для опции 82.
ip dhcp relay information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD} **no ip dhcp relay information option self-defined subscriber-id**	Устанавливает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции circuit -id.
ip dhcp relay information option self-defined subscriber-id format [ascii | hex]	Устанавливает пользовательский формат circuit -id для опции 82.

7. Проводить диагностику и поддержку опции 82 DHCP

Команда	Описание
Режим администратора	
show ip dhcp relay information option	Отображает информацию о состоянии опции 82 в системе, включая все параметры настройки.
debug ip dhcp relay packet	Используется для отображения информации об обработке пакетов в DHCP ретранслирующем агенте, включая действия «добавить»и «очистить».

28.3 Примеры применения опции 82 DHCP



Типовой пример применения опции 82 DHCP

В данной схеме оба коммутатора второго уровня (A и B) подключены к коммутатору третьего уровня (C), который передает DHCP запросы от клиентов серверу. Если опция 82 выключена, DHCP сервер не сможет распознать, из какой подсети клиент, и все клиенты, подключенные к SwitchA и SwitchB, будут получать адреса из общего адресного пула DHCP сервера. После включения опции 82, т.к. коммутатор 3 добавляет к запросу информацию о порте, сервер сможет распознать, в какой сети находится клиент (SwitchA или SwitchB) и, таким образом, сможет выделять разное адресное пространство двум подсетям, чтобы упростить управление сетью.

Конфигурация SwitchC (MAC адрес 08:B6:C3:00:00:01):

```
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
```

Linux ISC DHCP сервер поддерживает опцию 82, его конфигурационный файл /etc/dhcpd.conf:

```
ddns-update-style interim;
ignore client-updates;

class "Switch3Vlan2ClasSwitchA»{
match if option agent.circuit-id = "Vlan2+Ethernet1/0/2» and option agent.remote-id=08:B6:C3:00:00:01;
}

class "Switch3Vlan2ClasSwitchB»{
match if option agent.circuit-id = "Vlan2+Ethernet1/0/3» and option agent.remote-id=08:B6:C3:00:00:01;
}

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 "Switch3Vlan2ClasSwitchA";
}
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 "Switch3Vlan2ClasSwitchB";
}
}
```

Теперь DHCP сервер будет выделять адреса для узлов с коммутатора 2 из диапазона 192.168.102.21 ~ 192.168.102.50, а для коммутатора 1 из диапазона 192.168.102.51 ~ 192.168.102.80.

28.4 Поиск неисправностей опции 82 DHCP

Опция 82 DHCP реализована как подфункция модуля DHCP ретранслятора. Прежде, чем ее использовать, необходимо убедиться, что DHCP ретранслирующий агент настроен правильно.

Опция 82 требует взаимодействия DHCP ретранслятора и DHCP сервера. DHCP сервер должен установить политику выделения адресов основываясь на сетевой топологии DHCP ретранслятора, но, даже если ретранслятор работает нормально, выделение адресов может не получиться. Если в сети больше одного ретранслятора, уделите внимание политике передачи DHCP запросов.

При реализации функции опции 82 DHCP ретранслятора, подробная информация о процессе работы функции опции 82 DHCP ретранслятора может быть получена командой «debug ip dhcp relay packet». Эта информация может помочь в поиске неисправностей.

При реализации функции опции 82 DHCP севера, подробная информация о процессе работы функции опции 82 DHCP сервера может быть получена командой «debug ip dhcp server packet». Эта информация может помочь в поиске неисправностей.

29 ОПЦИИ 60 И 43 DHCP

29.1 Введение в опции 60 и 43 DHCP

DHCP сервер анализирует пакеты от DHCP клиента. Если приходит пакет с опцией 60, сервер принимает решение возвращать ли DHCP-клиенту пакеты с опцией 43 в соответствии с опцией 60 и настраивает параметры 60 и 43 в адресном пространстве сервера DHCP.

Настройка соответствующих опций 60 и 43 в адресном просторанстве DHCP-сервера:

1. В адресном пространстве настраиваются опции 60 и 43 одновременно. Приходит DHCP пакет с опцией 60 от DHCP клиента, если он совпадает с опцией 60 адресного пространства DHCP сервера, DHCP клиент получит опцию 43, настроенную в адресном пространстве, иначе опция 43 DHCP клиенту не возвращается.
2. В адресном пространстве настраивается только опция 43, совпадающая с любой опцией 60. Если получен DHCP пакет с опцией 60 от DHCP клиента, то DHCP клиент получит опцию 43, настроенную в адресном пространстве.
3. Если в адресном пространстве настроена только опция 60, то DHCP клиент не получит опцию 43.

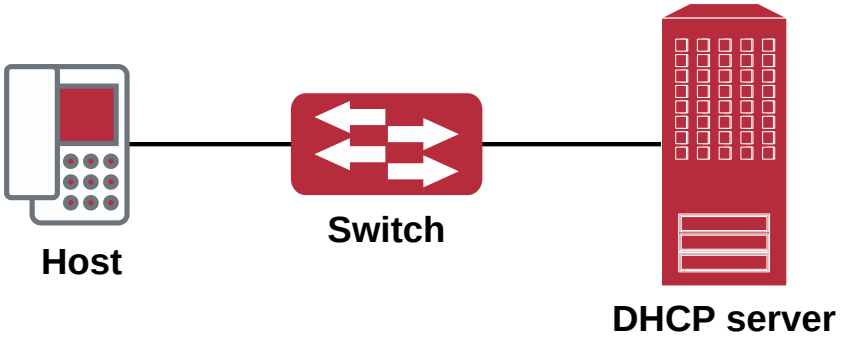
29.2 Настройка опций 60 и 43 на DHCP

1. Базовые настройки опций 60 и 43.

Команда	Описание
Режим конфигурации адресного пространства	
option 60 ascii LINE	Настройка опции 60 в символьной строке в формате ascii в режиме ip-адресного пространства DHCP
option 43 ascii LINE	Настройка опции 43 в символьной строке в формате ascii в режиме ip-адресного пространства DHCP
option 60 hex WORD	Настройка опции 60 в символьной строке в формате hex в режиме ip-адресного пространства DHCP
option 43 hex WORD	Настройка опции 43 в символьной строке в формате hex в режиме ip-адресного пространства DHCP
option 60 ip A.B.C.D	Настройка опции 60 в символьной строке в формате IP в режиме ip-адресного пространства DHCP

option 43 ip A.B.C.D	Настройка опции 43 в символьной строке в формате IP в режиме ip-адресного пространства DHCP
no option 60	Удаление настроек опции 60 в режиме адресного пространства
no option 43	Удаление настроек опции 43 в режиме адресного пространства

29.3 Пример настройки опций 60 и 43 DHCPv6



Fit AP получает IP адрес и опцию 43 – признак DHCP сервера для отправки одноадресного discovery запроса на беспроводый контроллер. DHCP сервер настраивает опцию 60 в соответствии с опцией 60 Fit AP и возвращает 43 опцию FTP AP.

Настройка DHCP сервера

```
router(config)#ip dhcp pool a
router (dhcp-a-config)#option 60 ascii AP1000
router (dhcp-a-config)#option 43 ascii 192.168.10.5,192.168.10.6
```

29.4 Устранение неисправностей 60 и 43 опций DHCP

Если возникают проблем при настройке DHCP опций 60 и 43, пожалуйста убедитесь, что проблемы не вызваны следующими причинами:

- ❖ Проверьте включена ли функция службы DHCP
- ❖ Если настроено адресное пространство опции 60, убедитесь, что оно сочетается с опцией 60 в пакетах

30 ОПЦИИ 37, 38 DHCPV6

30.1 Введение в опции 37, 38 DHCPv6

DHCPv6 (протокол динамической конфигурации хостов для IPv6) разработан для адресной схемы IPv6 и используется для назначения хостам IPv6 префиксов, IPv6 адресов и других конфигурационных параметров.

Если DHCPv6 клиент хочет запросить параметры конфигурации от DHCPv6 сервера, находящегося в другом сегменте, то для этого потребуется DHCPv6 ретранслятор. DHCPv6 сообщение, принятое ретранслятором, инкапсулируется в «relay-forward» пакеты, переправляемые серверу, который затем отвечает DHCPv6 ретранслятору пакетами «relay-reply». Затем ретранслятор восстанавливает из этих пакетов DHCPv6 сообщение и пересылает его клиенту.

Есть некоторые проблемы при использовании DHCPv6 ретранслятора, например: как назначить IP адрес в фиксированном диапазоне конкретным пользователям? Как избежать нелегального присвоения IP адресов, вызванного атакой, нацеленной на исчерпание свободных адресов? Как избежать нелегальных DHCPv6 клиентов, использующих MAC адрес других клиентов? Эти проблемы решаются посредством опций 37 и 38 DHCPv6 (RFC4649 и RFC4580).

Опции 37 и 38 DHCPv6 подобны опции 82 DHCP. DHCPv6 ретранслятор добавляет опции 37 и 38 к пересылаемым запросам и убирает эти опции из ответов сервера. Таким образом применение опций 37 и 38 прозрачно для клиента.

По опциям 37 и 38 DHCPv6 сервер может аутентифицировать DHCPv6 клиента и DHCPv6 ретранслирующее устройство, назначать и управлять клиентскими адресами, тем самым предотвращать различные DHCPv6 атаки. Так как сервер определяет, с какого порта доступа пришел запрос, он может ограничить количество выделяемых адресов на порт доступа, тем самым предотвратить атаку, нацеленную на исчерпание адресов. Однако RFC4649 и RFC4580 не определяют, как сервер будет использовать опции 37 и 38, пользователь может использовать их по своему усмотрению.

30.2 Список задач конфигурации опции 37, 38 DHCPv6

1. Конфигурация базовых опций Dhcpv6 snooping
2. Конфигурация базовых опций Dhcpv6 ретранслятора
3. Конфигурация базовых опций Dhcpv6 сервера

1. Конфигурация базовых опций Dhcpv6 snooping

Команда	Description
Общий режим	
ipv6 dhcp snooping remote-id option **no ipv6 dhcp snooping remote-id option**	Включает поддержку опции 37 в DHCPv6 snooping. Команда no выключает поддержку.
ipv6 dhcp snooping subscriber-id option **no ipv6 dhcp snooping subscriber-id option**	Включает поддержку опции 38 в DHCPv6 snooping. Команда no выключает поддержку.
ipv6 dhcp snooping remote-id policy {drop | keep | replace} **no ipv6 dhcp snooping remote-id policy**	Устанавливает политику пересылки пакетов, уже содержащих опцию 37. **drop** – система просто отбросит пакеты с опцией 37; **keep** – система сохранит исходную опцию 37 и перешлет пакет серверу; **replace** – система заменит существующую опцию 37 своей и перешлет пакет серверу. Команда no устанавливает политику **replace**.
ipv6 dhcp snooping subscriber-id policy {drop | keep | replace} **no ipv6 dhcp snooping subscriber-id policy**	Устанавливает политику пересылки пакетов, уже содержащих опцию 38. **drop** – система просто отбросит пакеты с опцией 38; **keep** – система сохранит исходную опцию 38 и перешлет пакет серверу; **replace** – система заменит существующую опцию 38 своей и перешлет пакет серверу. Команда no устанавливает политику **replace**.
ipv6 dhcp snooping subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |) **no ipv6 dhcp snooping subscriber-id select delimiter**	Настраивает пользовательскую конфигурацию опций subscriber-id, Команда no восстанавливает конфигурацию по умолчанию, т.е. заводской номер вместе с VLAN MAC.
ipv6 dhcp snooping subscriber-id select (sp|sv|pv|spv) delimiter WORD (delimiter WORD |)	Настраивает пользовательскую конфигурацию опций subscriber-id, Команда no восстанавливает

no ipv6 dhcp snooping subscriber-id select delimiter	конфигурацию по умолчанию, т.е. название VLAN вместе с названием порта.
Режим порта	
ipv6 dhcp snooping remote-id <remote-id> **no ipv6 dhcp snooping remote-id**	Задает форму добавления опции 37. <remote-id> это содержание поля remote-id в определенной пользователем опции 37, строка не боле 128 символов. Команда no восстанавливает конфигурацию по умолчанию, т.е. заводской номер вместе с VLAN MAC.
ipv6 dhcp snooping subscriber-id <subscriber-id> **no ipv6 dhcp snooping subscriber-id**	Задает форму добавления опции 38. <subscriber-id> это содержание поля subscriber-id в определенной пользователем опции 38, строка не боле 128 символов. Команда no восстанавливает конфигурацию по умолчанию, т.е. название VLAN вместе с названием порта, например "Vlan2+Ethernet1/0/2".

2. Конфигурация базовых опций Dhcpv6 ретранслятора

Команда	Description
Общий режим	
ipv6 dhcp relay remote-id option **no ipv6 dhcp relay remote-id option**	Включает поддержку опции 37 в DHCPv6 ретрансляторе. Команда no выключает поддержку.
ipv6 dhcp relay subscriber-id option **no ipv6 dhcp relay subscriber-id option**	Включает поддержку опции 38 в DHCPv6 ретрансляторе. Команда no выключает поддержку.
ipv6 dhcp relay remote-id delimiter WORD **no ipv6 dhcp relay remote-id delimiter**	Настраивает пользовательскую конфигурацию опций remote-id. Команда no восстанавливает конфигурацию по умолчанию, т.е. заводской номер вместе с VLAN MAC.
ipv6 dhcp relay subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |) **no ipv6 dhcp relay subscriber-id select delimiter**	Настраивает пользовательскую конфигурацию опций subscriber -id. Команда no восстанавливает конфигурацию по умолчанию, т.е. название VLAN вместе с названием порта.

Режим конфигурации интерфейса 3-о уровня	
ipv6 dhcp relay remote-id <remote-id> **no ipv6 dhcp relay remote-id**	Задает форму добавления опции 37. <remote-id> это содержание поля remote-id в определенной пользователем опции 37, строка не боле 128 символов. Команда no восстанавливает конфигурацию по умолчанию, т.е. заводской номер вместе с VLAN MAC.
ipv6 dhcp relay subscriber-id <subscriber-id> **no ipv6 dhcp relay subscriber-id**	Задает форму добавления опции 38. <subscriber-id> это содержание поля subscriber-id в определенной пользователем опции 38, строка не более 128 символов. Команда no восстанавливает конфигурацию по умолчанию, т.е. название VLAN вместе с названием порта, например "Vlan2+Ethernet1/0/2".

3. Конфигурация базовых опций Dhcpv6 сервера

Команда	Description
Общий режим	
ipv6 dhcp server remote-id option **no ipv6 dhcp server remote-id option**	Включает поддержку опции 37 в DHCPv6 сервере. Команда no выключает поддержку.
ipv6 dhcp server subscriber-id option **no ipv6 dhcp server subscriber-id option**	Включает поддержку опции 38 в DHCPv6 сервере. Команда no выключает поддержку.
ipv6 dhcp use class **no ipv6 dhcp use class**	Включает поддержку использования DHCPv6 классов при присвоении адресов. Команда no выключает это, не удаляя настройки классов DHCPv6.
ipv6 dhcp class <class-name> **no ipv6 dhcp class <class-name>**	Определяет DHCPv6 класс и входит в режим конфигурации DHCPv6 класса. Команда no удаляет класс.
Режим конфигурации интерфейса	
ipv6 dhcp server select relay-forward **no ipv6 dhcp server select relay-forward**	Включает выбор опций 37 и 38 внутреннего уровня, когда в пакете, пришедшем от ретранслятора, существует

	несколько опций 37 или 38. Команда no возвращает настройку по умолчанию, т.е. выбор опций 37 и 38 оригинальных пакетов.
Режим конфигурации DHCPv6 класса	
{remote-id <remote-id> | subscriber-id <subscriber-id>} **no {remote-id <remote-id> | subscriber-id <subscriber-id>}**	Настраивает опции 37 и 38, которые соответствуют классу.
class <class-name> **no class <class-name>**	Ассоциирует класс с пулом адресов и входит в режим конфигурации класса в пуле адресов. Команда no убирает ассоциацию.
address range <start-ip> <end-ip> **no address range <start-ip> <end-ip>**	Устанавливает диапазон адресов для DHCPv6 класса. Команда no удаляет диапазон. Форма записи «префикс/длина» не поддерживается.

30.3 Примеры опицй 37, 38 DHCPv6

30.3.1 Пример опций 37, 38 в DHCPv6 Snooping

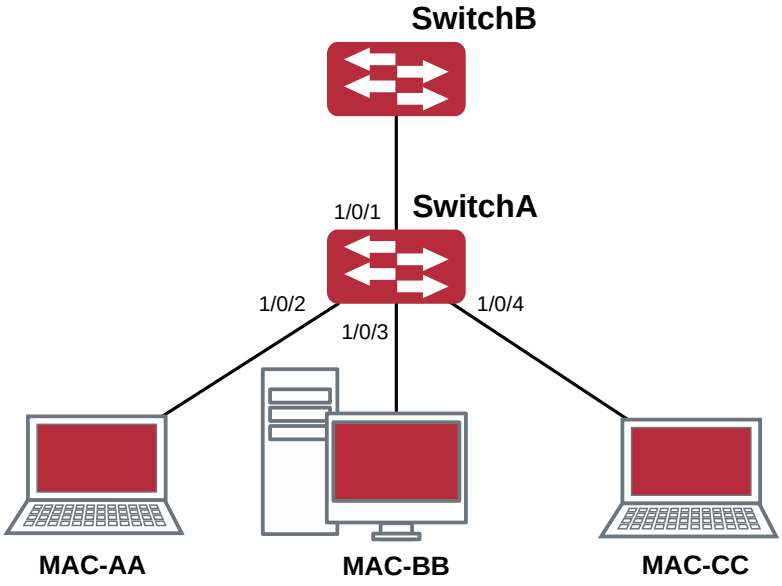


Схема опций в DHCPv6 Snooping

Согласно схеме Mac-AA, Mac-BB и Mac-CC – обычные пользователи, подключенные к недоверенным интерфейсам 1/0/2, 1/0/3 и ¼ соответственно. Они получают IP адреса 2010:2, 2010:3 и 2010:4 по DHCPv6; DHCPv6 сервер подключен к доверенному интерфейсу 1/0/1. Настроено три политики выделения адресов (классов), CLASSWITCHA соответствует

опции 38, CLASSWITCHB соответствует опции 37, а CLASSWITCHC – опциям 37 и 38. В пуле адресов EastDormPool запросам, соответствующим классам CLASSWITCHA, CLASSWITCHB и CLASSWITCHC будут назначены адреса из диапазонов 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 A включена функция DHCPv6 snooping и настроены опции 37 и 38.

Конфигурация 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 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 EastDormPool
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 CLASSWITCHA
SwitchB(dhcpv6-class-clasSwitchA-config)#remote-id     a0-12-34-00-00-01
subscriber-id vlan1+Ethernet1/0/1
SwitchB(dhcpv6-class-clasSwitchA-config)#exit
SwitchB(config)#ipv6 dhcp class CLASSWITCHB
SwitchB(dhcpv6-class-clasSwitchB-config)#remote-id     a0-12-34-00-00-01
subscriber-id vlan1+Ethernet1/0/2
SwitchB(dhcpv6-class-clasSwitchB-config)#exit
SwitchB(config)#ipv6 dhcp class CLASSWITCHC
SwitchB(dhcpv6-class-clasSwitchC-config)#remote-id     a0-12-34-00-00-01
subscriber-id vlan1+Ethernet1/0/3
SwitchB(dhcpv6-class-clasSwitchC-config)#exit
SwitchB(config)#ipv6 dhcp pool EastDormPool
SwitchB(dhcpv6-eastdormpool-config)#class CLASSWITCHA
SwitchB(dhcpv6-pool-eastdormpool-class-clasSwitchA-config)#address
range 2001:da8:100:1::3 2001:da8:100:1::30
SwitchB(dhcpv6-pool-eastdormpool-class-clasSwitchA-config)#exit
witchB(dhcpv6-eastdormpool-config)#class CLASSWITCHB
SwitchB(dhcpv6-pool-eastdormpool-class-clasSwitchB-config)#address
range 2001:da8:100:1::31 2001:da8:100:1::60
SwitchB(dhcpv6-eastdormpool-config)#class CLASSWITCHC
SwitchB(dhcpv6-pool-eastdormpool-class-clasSwitchC-config)#address
range 2001:da8:100:1::61 2001:da8:100:1::100
```

```
SwitchB(dhcpv6-pool-eastdormpool-class-clasSwitchC-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 EastDormPool
SwitchB(config-if-vlan1)#exit
SwitchB(config)#
```

30.3.2 Пример опций 37, 38 на DHCPv6 ретрансляторе

Пример 1:

При развертывании IPv6 сети для выделения IPv6 адресов может быть использована функция сервера DHCPv6 на маршрутизирующем устройстве, если специальный сервер используется для равномерного распределения и управления IPv6 адресами. DHCPv6 сервер поддерживает оба режима, с отслеживание состояния (stateful) и без него (stateless).

На уровне доступа используется SwitchA для подключения пользователей общежития; на первом уровне аггрегации SwitchB, он настроен кк DHCPv6 ретранслятор; на втором уровне аггрегации SwitchC настроен как DHCPv6 сервер, и он соединён с магистральной сетью. На компьютерах должна быть утсановлена ОС, которая поддерживает функцию DHCPv6 client.

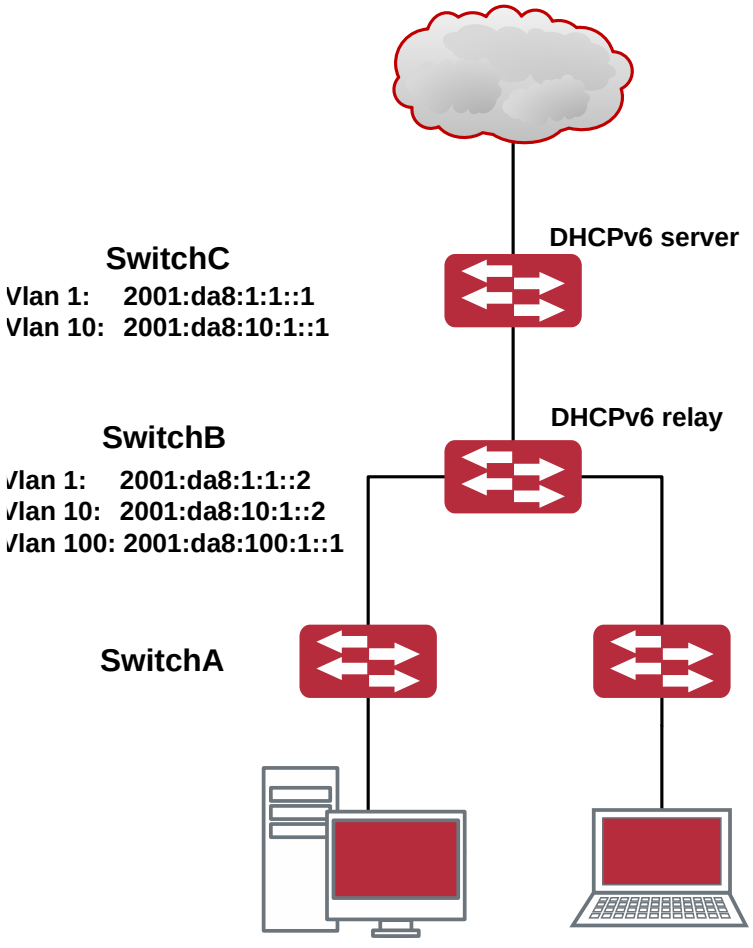


Схема применения опций в DHCPv6 ретрансляторе

Конфигурация SwitchB:

```
SwitchB(config)#service dhcpv6
SwitchB(config)#ipv6 dhcp relay remote-id option
SwitchB(config)#ipv6 dhcp relay subscriber-id option
SwitchB(config)#vlan 10
SwitchB(config-vlan10)#int vlan 10
SwitchB(config-if-vlan10)#ipv6 address 2001:da8:1:::2/64
SwitchB(config-if-vlan10)#ipv6 dhcp relay destination 2001:da8:10:1::1
SwitchB(config-if-vlan10)#exit
```

30.4 Поиск неисправностей опций 37, 38 DHCPv6

Пакеты запросов, отсылаемые DHCPv6 клиентом, это multicast пакеты, полученные устройством внутри его VLAN. Если DHCPv6 сервер хочет получать пакеты от клиента, клиент и сервер должны находиться в одном VLAN, иначе необходимо использовать DHCPv6 ретранслятор.

Обработка опций 37,38 при DHCPv6 snooping может проходить одним из следующих образов: заменить оригинальные опции 37,38 своими; отбросить пакет с опциями 37,38; не выполнять операцию добавления, передачи или отбрасывания пакета. Поэтому, если IPv6 адрес не получен в соответствии с опциями 37,38, пожалуйста, проверьте настройки политик DHCPv6 snooping на втором устройстве. DHCPv6 сервер по умолчанию получает опции 37,38 из пакета, отправленного клиентом, так же может получать их из пакета, отправленного ретранслятором.

DHCPv6 сервер проверяет только опции 37,38, добавленные первым DHCPv6 ретранслятором, это значит, что в пакетах ретранслятора действительны только опции 37,38 самого глубокого уровня.

31 КОНФИГУРАЦИЯ DHCP SNOOPING

31.1 Введение в DHCP Snooping

DHCP Snooping означает, что коммутатор наблюдает за процессом присвоения IP адресов по протоколу DHCP. Это предотвращает появление нелегальных DHCP серверов и DHCP атаки путем настройки доверенных и недоверенных портов. DHCP сообщение с доверенных портов передается без проверки. При типичной конфигурации доверенные порты используются для подключения DHCP сервера или DHCP ретранслятора, а к недоверенным портам подключаются клиенты. С недоверенных портов коммутатор будет пересылать только DHCP запросы, но не ответы. Если с недоверенного порта получено сообщение DHCP ответа, коммутатор поднимет тревогу и предпримет определенные действия с портом, согласно настройкам, например выключение или создание «black hole».

Если включена привязка DHCP Snooping, коммутатор сохранит в соответствующей таблице связующую информацию о каждом DHCP клиенте с недоверенного порта (включая MAC адрес, IP адрес, аренду IP, номера VLAN и порта). Имея такую информацию DHCP Snooping, можно комбинировать с другими модулями, такими, как dot1x и ARP, или самостоятельно реализовать контроль доступа пользователей.

Защита от поддельного DHCP сервера: если коммутатор перехватывает ответ DHCP сервера (включая DHCPOFFER, DHCPACK и DHCPNAK), он поднимет тревогу и предпримет определенные действия, согласно настройкам (выключение порта или создание «black hole»).

Защита от перегрузки DHCP: Чтобы избежать большого количества сообщений DHCP, атакующих процессор, пользователь может ограничить скорость получения DHCP пакетов на доверенных и недоверенных портах.

Запись данных привязки DHCP (dhcp snooping binding): DHCP snooping при пересылке DHCP пакетов будет записывать данные (ip + mac). Можно так же загрузить эти данные на сервер в целях восстановления утерянной информации. Данные привязки, в основном, используются для настройки динамических пользовательских портов dot1x. За подробной информацией о dot1x обратитесь, пожалуйста, к главе «Настройка dot1x».

Добавление связующего ARP: можно добавить статическую связку ARP в соответствии с динамическими данными, чтобы предотвратить ARP мошенничество.

Добавление доверенных пользователей: можно добавить записи в список доверенных пользователей в соответствии с параметрами связующих данных; эти пользователи получат доступ ко всем ресурсам без dot1x аутентификации.

Автоматическое восстановление: через некоторое время после выключения порта или создания «black hole», нужно автоматически убрать блокировку порта или MAC адреса и отправить при этом информацию на сервер через syslog.

Функция журнала: Когда коммутатор обнаруживает ненормальные пакеты, он должен отправить информацию на сервер журнала через syslog.

Шифрование приватных сообщений: связь между коммутатором и внутренней системой управления безопасностью сети TrustView происходит через приватные сообщения. Пользователи могут шифровать эти сообщения в версии 2.

Функция добавление опции 82: различные sub опции 82 добавляются в DHCP сообщение в соответствии со статусом аутентификации пользователя.

31.2 Последовательность задач конфигурации DHCP Snooping

1. Включить DHCP Snooping
2. Включить функцию привязки DHCP Snooping
3. Включить функцию привязки ARP DHCP Snooping
4. Включить функцию опции 82 DHCP Snooping
5. Установить версию приватных пакетов
6. Установить зашифрованный ключ DES для приватных пакетов
7. Установить адрес DHCP сервера
8. Настроить доверенные порты
9. Включить функцию привязки DHCP Snooping DOT1X
10. Включить функцию привязки DHCP Snooping USER
11. Добавить записи в статический список
12. Установить действия защиты
13. Установить ограничение скорости передачи DHCP сообщений
14. Включить отладку
15. Настроить атрибуты опции 82 DHCP Snooping

1. Включить DHCP Snooping

Команда	Описание
Глобальный режим	
ip dhcp snooping enable **no ip dhcp snooping enable**	Включить/выключить DHCP Snooping.

2. Включить функцию привязки DHCP Snooping

Команда	Описание
Глобальный режим	
ip dhcp snooping binding enable **no ip dhcp snooping binding enable**	Включить/выключить функцию привязки DHCP Snooping.

3. Включить функцию привязки ARP DHCP Snooping

Команда	Описание
Глобальный режим	
ip dhcp snooping binding arp **no ip dhcp snooping binding arp**	Включить/выключить функцию привязки ARP DHCP Snooping.

4. Включить функцию опции 82 DHCP Snooping

Команда	Описание
Глобальный режим	
ip dhcp snooping information enable **no ip dhcp snooping information enable**	Включить/выключить функцию опции 82 DHCP Snooping.

5. Установить версию приватных пакетов

Команда	Описание
Глобальный режим	
ip user private packet version two **no ip user private packet version two**	Настроить/удалить версию приватных пакетов.

6. Установить зашифрованный ключ DES для приватных пакетов

Команда	Описание
Глобальный режим	
enable trustview key 0/7 <*password*> **no enable trustview key**	Настроить/удалить зашифрованный ключ DES для приватных пакетов.

7. Установить адрес DHCP сервера

Команда	Описание
Глобальный режим	
ip user helper-address A.B.C.D [port <udpport>] source <ipAddr> (secondary|) **no ip user helper-address (secondary|)**	Настроить/удалить адрес DHCP сервера.

8. Настроить доверенные порты

Команда	Описание
Режим порта	
ip dhcp snooping trust {vlan <vlan-list>} **no ip dhcp snooping trust {vlan <vlan-list>}**	Сделать порт доверенным. Команда no отменяет настройку.

9. Включить функцию привязки DHCP Snooping DOT1X

Команда	Описание
Режим порта	
ip dhcp snooping binding dot1x **no ip dhcp snooping binding dot1x**	Включить/выключить функцию привязки DHCP Snooping DOT1X.

10. Включить функцию привязки DHCP Snooping USER

Команда	Описание
Режим порта	
ip dhcp snooping binding user-control **no ip dhcp snooping binding user-control**	Включить/выключить функцию привязки DHCP Snooping USER.

11. Добавить записи в статический список

Команда	Описание
Глобальный режим	
ip dhcp snooping binding user *<mac>* address *<ipAddr>* vlan *<vid>* interface (ethernet|) *<ifname>* **no ip dhcp snooping binding user *<mac>* interface (ethernet|) *<ifname>***	Добавить/удалить записи в статический список.

12. Установить действия защиты

Команда	Описание
Режим порта	
ip dhcp snooping action {shutdown|blackhole} [recovery *<second>*] **no ip dhcp snooping action**	Установить/отменить автоматические защитные действия на портах.

13. Установить ограничение скорости передачи DHCP сообщений

Команда	Описание
Глобальный режим	
ip dhcp snooping limit-rate <*pps*> **no ip dhcp snooping limit-rate**	Установить ограничение скорости передачи DHCP сообщений.

14. Включить отладку

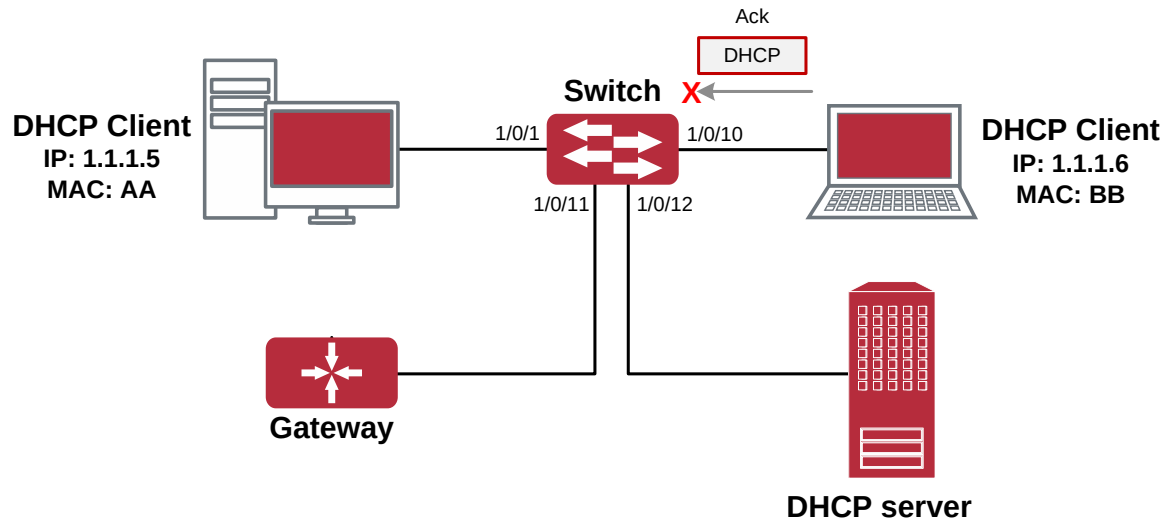
Команда	Описание
Режим администратора	
debug ip dhcp snooping packet **debug ip dhcp snooping event** **debug ip dhcp snooping update** **debug ip dhcp snooping binding**	Пожалуйста, обратитесь к соответствующей главе поиска неисправностей.

15. Настроить атрибуты опции 82 DHCP Snooping

Команда	Описание
Глобальный режим	
ip dhcp snooping information option subscriber-id format {hex | acsii | vs-hp | vs-huawei}	Устанавливает формат subscriber-id опции 82 DHCP snooping.
ip dhcp snooping information option remote-id {*<remote-id>* | standard | vs-cisco | vs-huawei} **no ip dhcp snooping information option remote-id**	Устанавливает содержание суб-опции remote-id опции 82. Команда no возвращает стандартный формат.
ip dhcp snooping information option allow-untrusted **no ip dhcp snooping information option allow-untrusted**	Разрешает недоверенным портам принимать DHCP пакеты с опцией 82. Если не включено, все недоверенные порты будут отбрасывать DHCP пакеты с опцией 82.
ip dhcp snooping information option delimiter [colon | dot | slash | space] **no ip dhcp snooping information option delimiter**	Устанавливает разделитель для параметров суб-опций опции 82. Команда no устанавливает разделитель по умолчанию – slash.

ip dhcp snooping information option self-defined remote-id {hostname | mac | string WORD} **no ip dhcp snooping information option self-defined remote-id**	Задает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции remote-id.
ip dhcp snooping information option self-defined remote-id format [ascii | hex]	Пользовательский формат remote-id для опции 82.
ip dhcp snooping information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac) | string WORD} **no ip dhcp snooping information option type self-defined subscriber-id**	Задает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции circute-id.
ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]	Пользовательский формат circuit-id для опции 82.
Режим порта	
ip dhcp snooping information option subscriber-id {standard | <*circuit-id*>} **no ip dhcp snooping information option subscriber-id**	Устанавливает содержание суб-опции circuit-id опции 82. Команда no возвращает стандартный формат.

31.3 Типовое применение DHCP Snooping



Типовой применение

Как показано на рисунке, устройство Mac-AA – обычный пользователь, подключенный к недоверенному порту 1/0/1 коммутатора, получает IP настройки через DHCP, IP адрес клиента 1.1.1.5. DHCP сервер и шлюз подключены к доверенным портам

коммутатора, 1/0/11 и 1/0/12 соответственно. Злоумышленник Mac-BB, подключенный к недоверенному порту 1/0/1 коммутатора, пытается подделать DHCP сервер (посылая пакеты DHCPACK). Функция DHCP Snooping на коммутаторе эффективно обнаружит и блокирует такой тип сетевой атаки.

Последовательность настройки:

```
switch#
switch#config
switch(config)#ip dhcp snooping enable
switch(config)#interface ethernet 1/0/11
switch(Config-If-Ethernet1/0/11)#ip dhcp snooping trust
switch(Config-If-Ethernet1/0/11)#exit
switch(config)#interface ethernet 1/0/12
switch(Config-If-Ethernet1/0/12)#ip dhcp snooping trust
switch(Config-If-Ethernet1/0/12)#exit
switch(config)#interface ethernet 1/0/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
switch(Config-Port-Range)#
```

31.4 Поиск неисправностей DHCP Snooping

31.4.1 Наблюдение и отладочная информация

Команда «debug ip dhcp snooping» может быть использована для получение отладочной информации.

31.4.2 Помощь в поиске неисправностей

Если возникает проблема с использованием функции DHCP Snooping, пожалуйста, проверьте следующее:

Включена ли функция DHCP Snooping глобально;

Если порт не реагирует на ложный DHCP пакет, проверьте, настроен ли этот порт как недоверенный.