Ethernet-коммутаторы доступа L2+

Серии QSW-3420, QSW-3750, QSW-3750 rev. R, QSW-4610

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 программы либо, когда внутриполосное управление недоступно. Например, пользователь может через консольный порт присвоить программе IP-адрес для доступа по Telnet.

Процедура управления программой через консольный интерфейс, описана ниже:

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

Рисунок 1-1. 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 (COM), с установленным эмулятором терминала, таким как PuTTY
Кабель серийного порта	Один конец подключается к серийному порту RS-232 (COM), а другой к порту Console коммутатора
Коммутатор	Требуется работающий порт Console

Шаг 2. Включение и настройка эмулятора терминала PuTTY.

После установки соединения, запустите PuTTY. PuTTY — свободно распространяемый клиент для различных протоколов удалённого доступа, включая SSH, Telnet. Также имеется возможность работы через последовательный порт (Serial port, COM-порт).

1. Запустите PuTTY и выберете тип подключения – Serial. В поле «Serial line» укажите номер последовательного порта, например, COM7. Затем в поле «Speed» необходимо задать скорость передачи данных (baudrate) — 9600 бит/с.

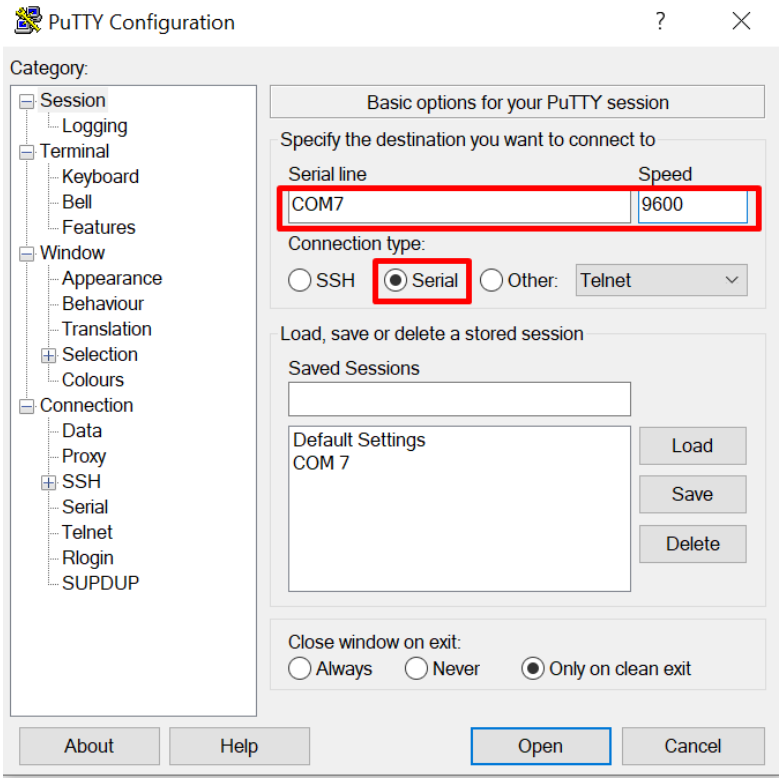


Рисунок 1-2. Основныве настройки PuTTY

2. Для облегченного повторного подключения с использованием PuTTY, следует сохранить настройки сессии. Для этого необходиомо в поле «Saved Session» ввести название сессии (например, Switch1) и нажать кнопку «Save».

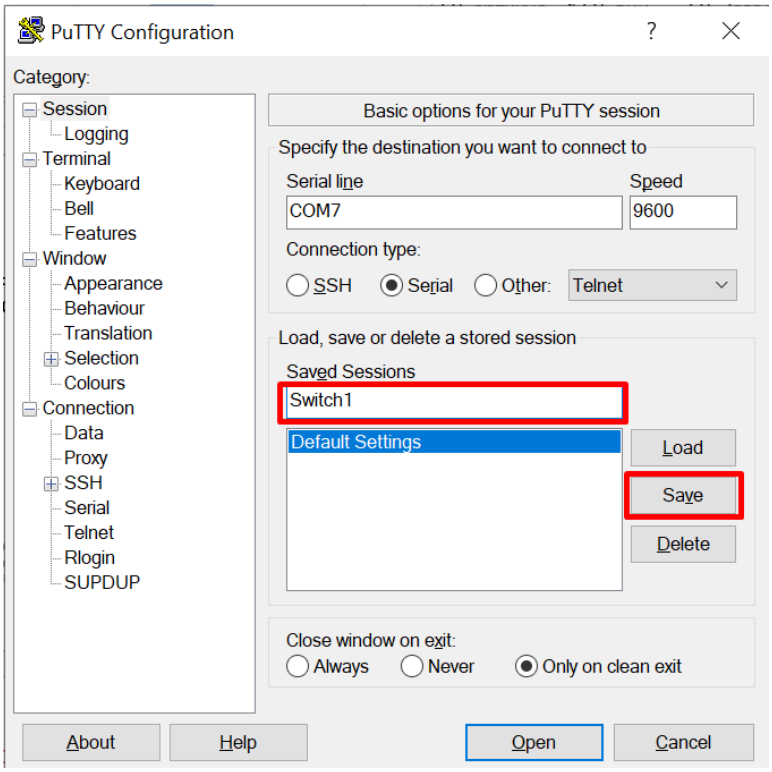


Рисунок 1-3.Сохранение сессии в PuTTY

3. Выберите сохраненную сессию и нажмите копку «Open».

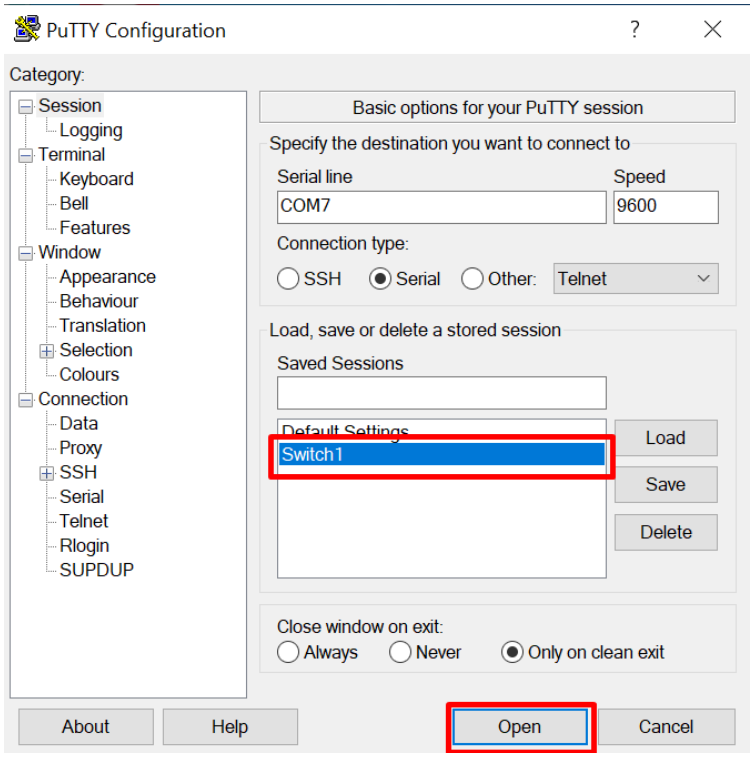


Рисунок 1-4. Запуск сохраненной сессии

Шаг 3. Вызов командного интерфейса (CLI) коммутатора.

Включите коммутатор и дождитесь полной загрузки. После чего в окне PuTTY появятся следующие сообщения — это пользовательский режим коммутатора.

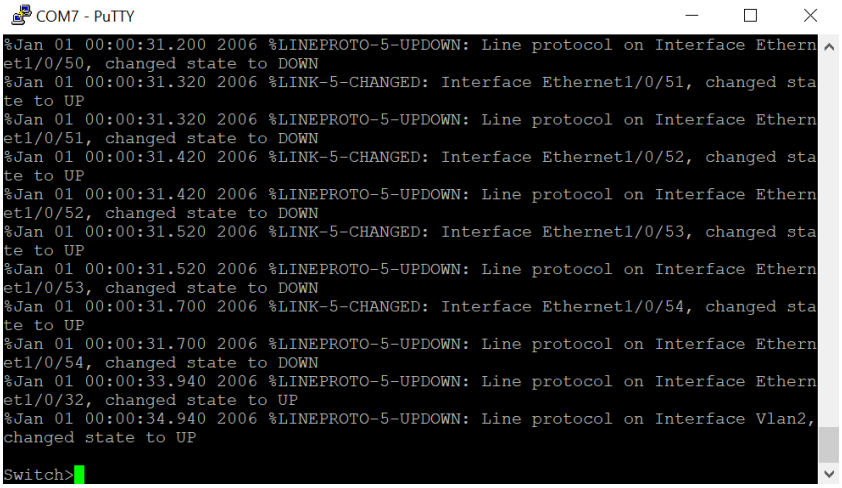


Рисунок 1-5. Коммутатор загрузился

Нажмите клавишу «Enter» и теперь можно вводить команды управления коммутатором. Детальное описание команд приведено в последующих главах.

1.1.2. Внутриполосное управление.

Внутриполосное управление относится к управлению посредством доступа к коммутатору с использованием Telnet, или HTTP, а также SNMP. Внутриполосное управление включает функции управления коммутатора для некоторых устройств, подключенных к нему. В тех случаях, когда внутриполосное управление из-за изменений, сделанных в конфигурации коммутатора работает со сбоями, для управления и конфигурирования коммутатора можно использовать внеполосное управление.

1.1.2.1. 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):

Рисунок 1-6. 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 10.1.128.251/24. Тогда IP-адрес хоста может быть 10.1.128.252/24. С помощью команды “ping 192.168.0.10” можно проверить, доступен коммутатор или нет.
- Команды настройки IP-адреса для интерфейса VLAN1 указаны ниже. Перед применением внутриполосного управления, IP-адрес коммутатора должен быть настроен посредством внеполосного 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>
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.

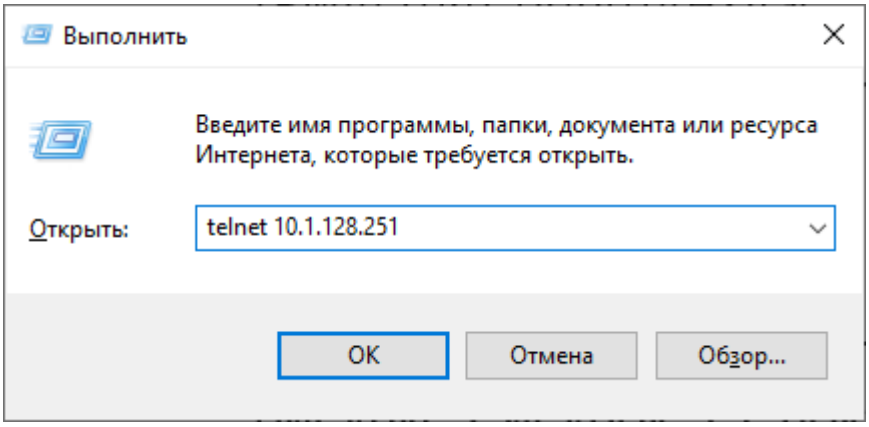


Рисунок 1-7. Запуск программы Telnet-клиент в Windows.

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.

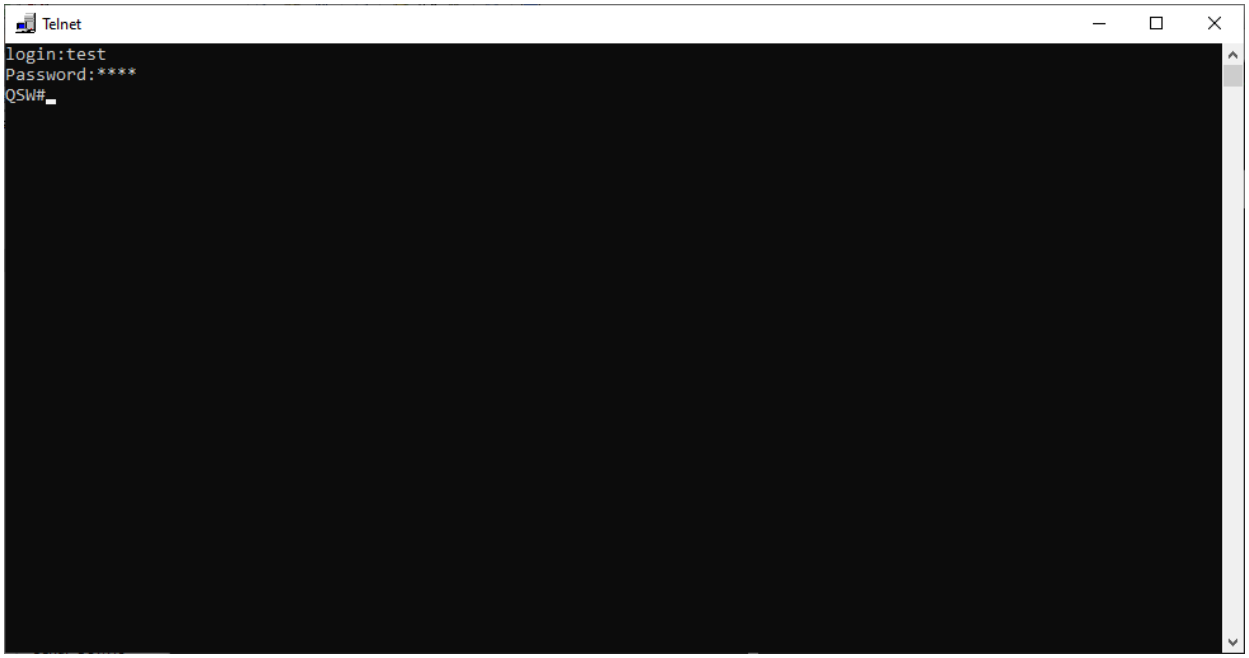


Рисунок 1-8. Настройка. Вид Telnet-интерфейса

1.1.2.2. Управление через HTTP

Чтобы управлять коммутатором через веб-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 Веб стало возможным, нужно ввести команду ip http server в глобальном режиме конфигурирования:

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

Шаг 2. Запуск веб-браузера на хосте.

Необходимо открыть веб-браузер на хосте и ввести IP-адрес коммутатора, или непосредственно запустить HTTP-протокол в Windows. К примеру, IP-адрес коммутатора “10.1.128.251”.

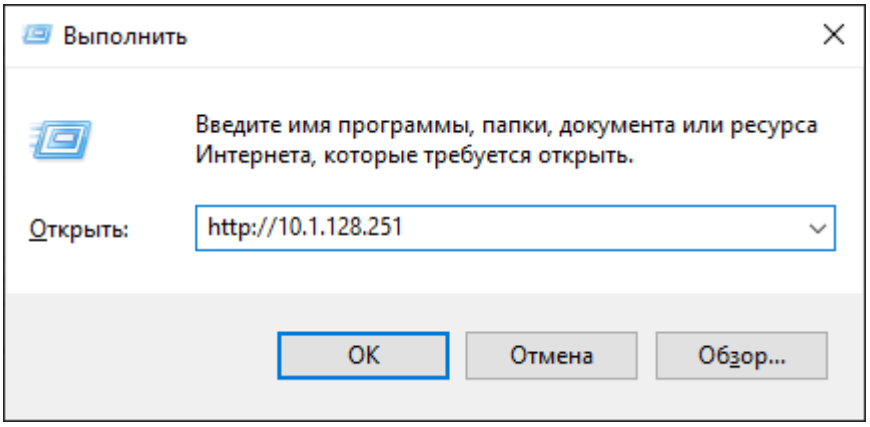


Рисунок 1-9. Запуск HTTP-протокола

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 веб-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
```

Веб-интерфейс входа выглядит следующим образом.

Рисунок 1-10. Веб-интерфейс входа.

Введите достоверные имя пользователя и пароль, затем вы попадете в главное меню настройки веб-интерфейса, как это показано ниже.

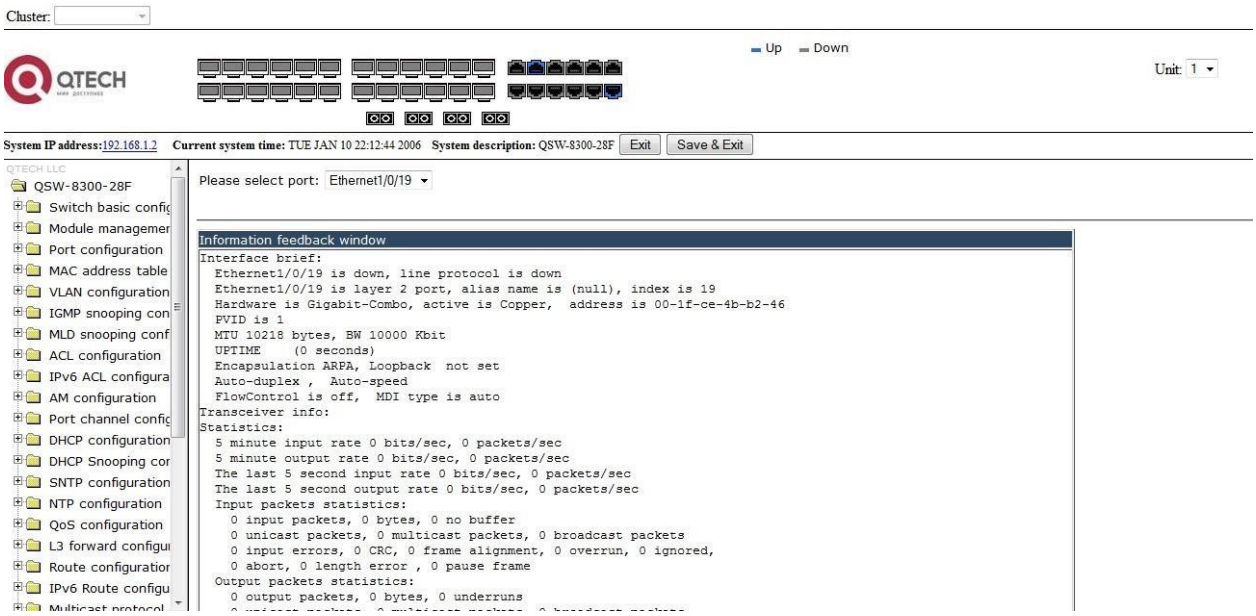


Рисунок 1-11. Главное меню настройки веб-интерфейса.

ПРИМЕЧАНИЕ: при настройке коммутатора, имя коммутатора пишется английскими буквами.

1.1.2.3. 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 пинговать 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

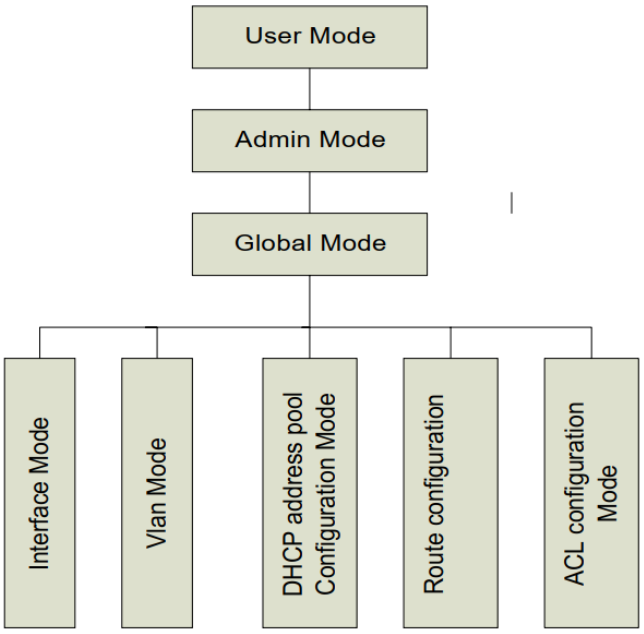


Рисунок 1-12. Режимы настройки Shell

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 конфигурациии 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.

1.2.2. 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

Тип Интерфейса	Команда	Действие команды	Выход
Ethernet-порт	Наберите команду interface ethernet <interface-list> в режиме глобального конфигурирования	Настройка поддерживаем ого 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

1.2.3. 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.

1.2.4. 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.

1.2.5. 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

1.2.6. 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 команды 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 <string> snmp-server community rw <string>

1.2.7. 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)	

Клавиша (и)	Функция
Ctrl +c	Остановка непрерывных процессов команд, таких как пинг и т.д.
Tab	В процессе ввода команды Tab может быть использован для ее завершения, если нет ошибок

1.2.8. 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
“?”	Под любой командной строкой введите "?", чтобы получить список команд для текущего режима с кратким описанием. 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. Введите "?" сразу после строки. Это покажет все команды, которые начинаются с этой строки

1.2.9. Проверка ввода

1.2.9.1. 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.

1.2.9.2. 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

Отображаемое сообщение ошибки	Пояснение
Invalid command or parameter	Команда существует (признается), но задан неправильный параметр
This command is not exist 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

1.2.10. 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	Выходит из текущего режима и возвращается в режим администратора, только когда пользователь находиться 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 флеш-память

Команда	Пояснение
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 появиться 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

Команда	Описание
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 обеспечене, 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 VLAN-интерфейса
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 и 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 MID, 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 MID, как показано на рисунке ниже:

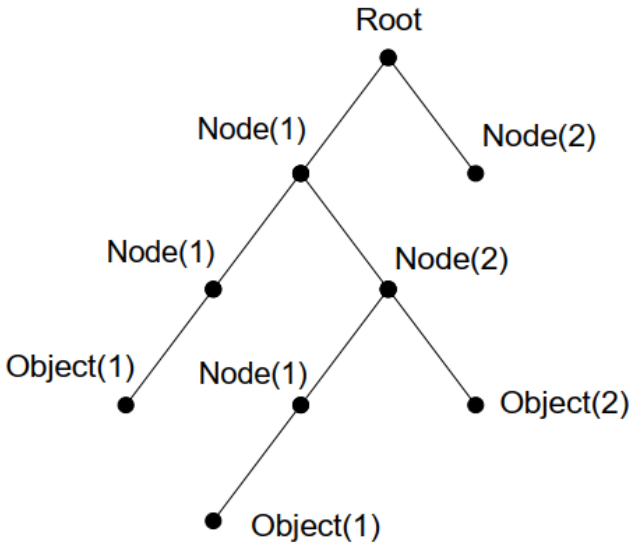


Рисунок 2-1. Пример дерева ASN.1

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/v2c и SNMP v3. Также коммутатор поддерживает базовые MIB-II, RMON публичные MIB и другие публичные MID, 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.

MID 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 enabled no snmp-server enabled	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/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/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

Команда	Описание
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 dcstrap
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 пинга (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 поразумевает 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”. IMG-файл может быть сохранен только во флеш-памяти с определенным названием nos.img.

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.

Рисунок 2-2. Консольный кабель связи

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]: setconfig
Host IP Address: [10.1.1.1] 192.168.1.2
Server IP Address: [10.1.1.2] 192.168.1.66
FTP(1) or TFTP(2): [1] 2
Network interface configure OK.
[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 пинга с сервера. Если пинг успешен, запустите команду "load" в BootROM-режиме. Если это не удается, устранените неполадоки. Ниже показана конфигурация для обновления файла образа системы:

```
[Boot]: load nos.img Loading...
Loading file ok!
```

Шаг 5.

Выполнить замену nos.img в режиме BootROM. Показанные далее команды конфигурации позволяют сохранить образ файла системы:

```
[Boot]: write nos.img
File nos.img exists, overwrite? (Y/N)?[N] y
Writing nos.img.....
Write nos.img OK.
[Boot]:
```

Шаг 6.

Выполняем загрузку файла boot.rom на коммутатор, основные действия, такие же, как и в шаге 4.

```
[Boot]: load boot.rom
```

```
Loading...
Loading file ok!
```

Шаг 7.

Далее выполняем запись boot.rom в режиме BootROM. Этот шаг позволяет сохранить обновленный файл.

```
[Boot]: write boot.rom
File boot.rom exists, overwrite? (Y/N)?[N] y
Writing boot.rom.....
Write boot.rom OK.
[Boot]:
```

Шаг 8.

После удачного обновления выполните команду “run” или “reboot” в режиме BootROM для возврата в интерфейс настройки CLI.

```
[Boot]:run (or reboot)
```

Остальные команды в BootROM-режиме:

DIR command

Команда DIR - используется для вывода списка существующих файлов во флеш-памяти.

```
[Boot]: dir
boot.rom 327,440 1900-01-01 00:00:00 --SH
boot.conf83 1900-01-01 00:00:00 --SH
nos.img 2,431,631 1980-01-01 00:21:34 ----
startup-config2,922 1980-01-01 00:09:14 ----
temp.img2,431,631 1980-01-01 00:00:32 ----
```

CONFIG RUN command

Используется для настройки файла IMG для запуска при запуске системы и файла конфигурации для запуска при восстановлении конфигурации.

```
[Boot]: config run
Boot File: [nos.img] nos.img
Config File: [boot.conf]
```

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 простого 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 и 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 флеш-память в коммутаторе.

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

FLASH: флеш-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 флеш-память. Коммутатор позволяет загрузить файл образа системы через FTP в режиме Shell только с определенным названием nos.img, другие файлы IMG будут отклонены.

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 флеш-памяти. Если устройство поддерживает CF, файл конфигурации хранится во флеш-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 флеш-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.

1.1. Загрузка файлов FTP/TFTP-клиентом.

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

1.2. 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.

2.1. Запуск FTP-сервера.

Команда	Пояснение
Глобальный режим	
ftp-server enable no ftp-server enable	Запуск сервера, команда “no” выключает сервер

2.2. 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

2.3. Изменение времени ожидания FTP-сервера.

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

3. Настройка TFTP-сервера.

3.1. Запуск TFTP-сервера.

Команда	Пояснение
Глобальный режим	
tftp-server enable no tftp-server enable	Запуск сервера, команда “no” выключает сервер

3.2. Изменение времени ожидания TFTP-сервера.

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

3.3. 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.

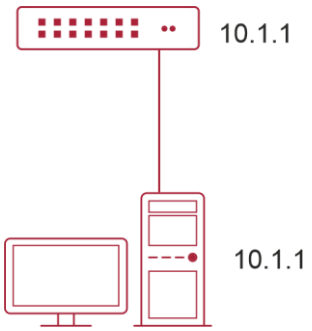


Рисунок 2-3. Загрузка nos.img файла FTP/TFTP-клиентом

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.

2.5.4. Настройка FTP

Настройка компьютера:

Запустите программное обеспечение FTP-сервера на компьютере и установите имя пользователя "Switch" 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: //Switch:switch@10.1.1.1/12_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 “Switch” 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 “Switch”, 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: //Switch: 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.

2.5.4.1. Устранение неисправностей FTP/TFTP

2.5.4.1.1. 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.

Следующее сообщение, отображается при успешном получении 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.
recv total = 1526037
************************
write ok
150 Opening ASCII mode data connection for nos.img (1526037 bytes).
226 Transfer complete.
```

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.

2.5.5. 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 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.

```
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 1000GX-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 1/2-5”. 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.
   - 2.1. Конфигурация режима combo для combo портов.
   - 2.2. Включить/выключить порты.
   - 2.3. Конфигурация имени порта.
   - 2.4. Конфигурация типа кабеля на порту.
   - 2.5. Конфигурация скорости и дуплекса на порту.
   - 2.6. Конфигурация контроля полосы пропускания.
   - 2.7. Конфигурация управления траффиком.
   - 2.8. Включение/выключение функции распознавания петли.
   - 2.9. Конфигурация контроля широковещательных штормов на коммутаторе.
   - 2.10. Конфигурация режима сканирования порта.
   - 2.11. Конфигурация контроля нарушения скорости на порту.
   - 2.12. 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 | copper-preferred-auto | fiber | sfp-preferred-auto}	Установка режима комбо-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]] [auto | full | half |]] | 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 100/1000 BASE-TX или 100 BASE-FX. 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 1000 BASE-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

Команда	Описание
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 } no switchport flood-control {bcast|mcast|ucast }	Конфигурирование коммутатора не передавать широковещательные, многопользовательские и персональные 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 300 с). 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

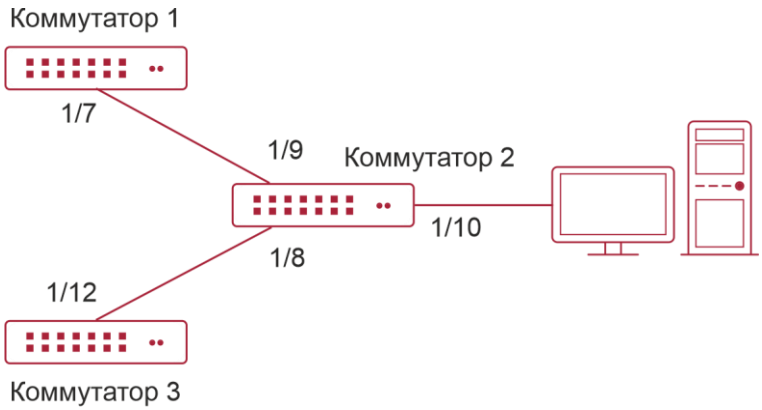


Рисунок 3-1. Пример конфигурации порта

VLAN не сконфигурированы на коммутаторе. По умолчанию используется VLAN1.

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

Конфигурация приведена ниже:

Switch1:

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

Switch2:

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

```
Switch2(config)#monitor session 1 destination interface ethernet 1/10
Switch3:
Switch3(config)#interface ethernet 1/12
Switch3(Config-If-Ethernet1/12)#speed-duplex force100-full
Switch3(Config-If-Ethernet1/12)#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

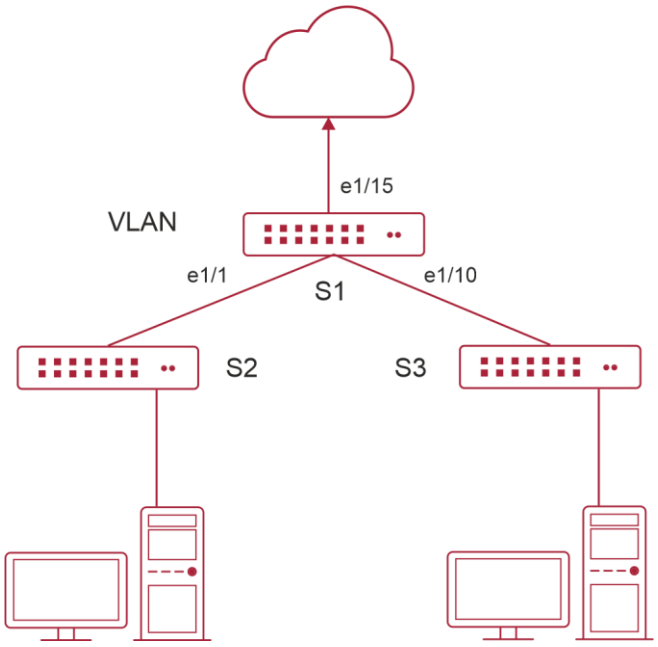


Рисунок 4-1. Типовые примеры функции изоляции портов

Топология и конфигурация коммутаторов показана на рисунке выше. Порты e1/1, e1/10 и e1/15 все принадлежат к VLAN 100. Требование заключается в том, чтобы после включения функции изоляции портов на коммутаторе switch1 порты e1/1 и e1/10 на этом коммутаторе не могли связываться друг с другом и оба могли связываться с портом e1/15, смотрящим в сеть. То есть связи между любыми парами низлежащих портов нет, и в то же время связь между любым низлежащим портом и вышестоящим работает. Вышестоящий порт может работать с любым портом нормально.

Конфигурация коммутатора S1:

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

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 запомненным 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| learning} 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

Рисунок 5-1. 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 1/1
Switch(Config-If-Ethernet1/1)#loopback-detection special-vlan 1-3
Switch(Config-If-Ethernet1/1)#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.

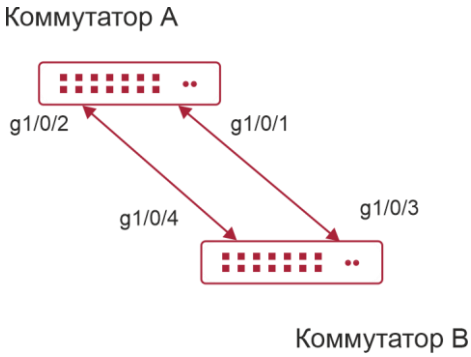


Рисунок 6-1. Перекрестное оптическое соединение

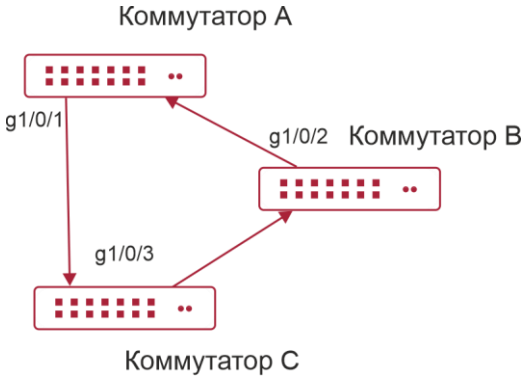


Рисунок 6-2. Один из концов каждого оптического соединения не подключен

Такой вид проблем часто возникает в ситуации, когда или интерфейс, или GBIC (Giga Bitrate interface Converter — конвертер интерфейса со скоростью 1 Гбит) 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 с

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

Команда	Описание
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

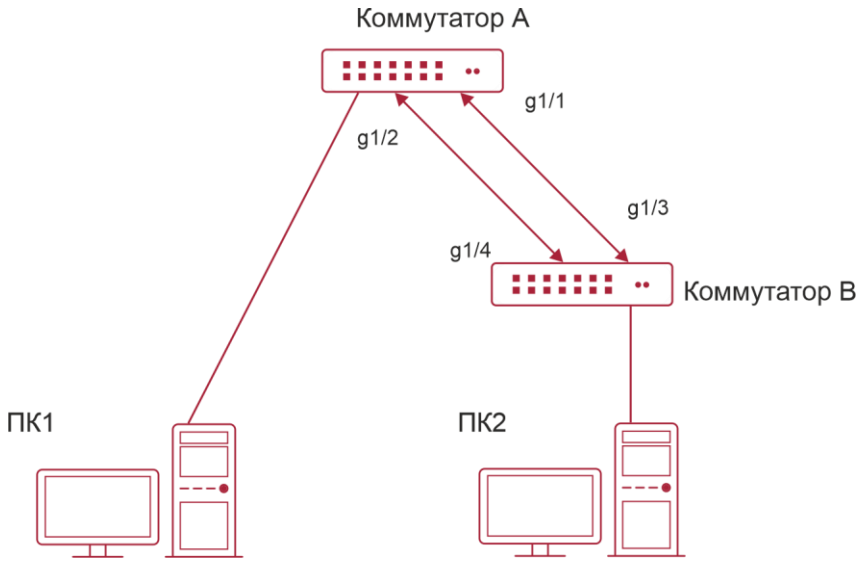


Рисунок 6-3. Оптическое перекрестное соединение

В сетевой топологии на рисунке порты g1/1 и g1/2 на коммутаторе A, а также порты g1/3 и g1/04 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 порты g1/1 и g1/2 на коммутаторе A, а также порты g1/3 и g1/04 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 1/1
SwitchA (Config-If-Ethernet1/1)#uldp enable
SwitchA (Config-If-Ethernet1/1)#exit
SwitchA(config)#interface ethernet1/2
SwitchA(Config-If-Ethernet1/2)#uldp enable
```

Последовательность конфигурации коммутатора B:

```
SwitchB(config)#uldp enable
```

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

В результате порты g1/1 и g1/2 на коммутаторе A будут заблокированы функцией ULDP и на дисплее терминала PC1 появится следующая информация.

```
%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/1 need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/1 shut down!
%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/2 need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/2 shutted down!
```

Порты g1/3 и g1/4 на коммутаторе B будут заблокированы функцией ULDP и на дисплее терминала PC2 появится следующая информация.

```
%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/3 need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/3 shutted down!
%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/4 need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/4 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 1/3 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 – 86 400 секунд).

Команда рестарта и механизм перезагрузки порта воздействуют только на порт, который был выключен функцией ULDP. Порты, выключенные вручную, пользователями или другими функциями не могут быть рестартованы 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 LLDP-функции 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

Команда	Описание
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

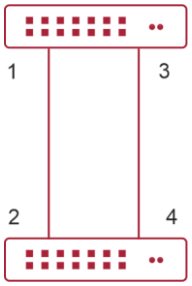


Рисунок 7-1. Типовой пример конфигурации функции LLDP

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 1/4
SwitchA(Config-If-Ethernet1/4)# lldp transmit optional tlv portDesc sysCap
SwitchA(Config-If-Ethernet1/4)exit
```

Коммутатор B. Последовательность команд конфигурации:

```
SwitchB(config)#lldp enable
SwitchB(config)#interface ethernet1/1
```

```
SwitchB(Config-If-Ethernet1/1)# lldp mode receive
SwitchB(Config-If-Ethernet1/1)#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 членами 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.

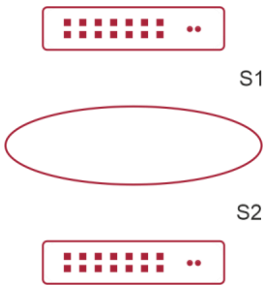


Рисунок 8-1. Агрегирование портов

Как показано выше, коммутатор S1 объединил порты в Port channel. Пропускная полоса Port channel равна сумме пропускных способностей четырех портов. Когда необходимо передать трафик с коммутатора S1 на S2, 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 равильной 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. 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 членами 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.

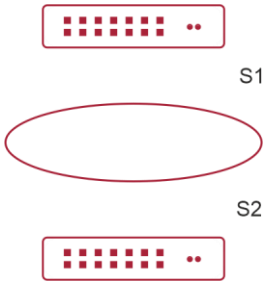


Рисунок 8-2. Конфигурация порта-канала в LACP

Имеется два коммутатора S1 и S2. Порты 1,2,3,4 на коммутаторе S1 – порты доступа и добавлены в группу1 в активном режиме. Порты 6,8,9,10 на коммутаторе S2 – 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 1/1-4
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 1/6
Switch2(Config-If-Ethernet1/6)#port-group 2 mode passive
Switch2(Config-If-Ethernet1/6)#exit
Switch2(config)#interface ethernet 1/8-10
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)#
```

Результат конфигурации:

Коммутатор сообщит, что агрегирование прошло успешно. Порты 1,2,3,4 коммутатора S1 входят в группу Port-Channel1, а порты 6,8,9,10 коммутатора S2 входят в группу Port-Channel2.

Вариант 2. Конфигурация Port channel в режиме ON.

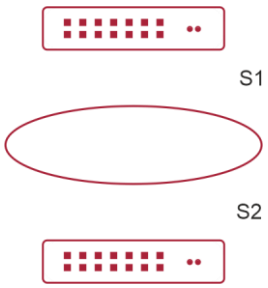


Рисунок 8-3. Конфигурация port channel в режиме ON

Как показано на рисунке, порты 1,2,3,4 коммутатора S1 – порты доступа и будут добавлены в группу1 с режимом ON. Порты 6,8,9,10 коммутатора S2 – тоже порты доступа и будут добавлены в группу2 с режимом ON.

Этапы конфигурации показаны ниже:

```
Switch1#config
Switch1(config)#interface ethernet 1/1
Switch1(Config-If-Ethernet1/1)#port-group 1 mode on
Switch1(Config-If-Ethernet1/1)#exit
Switch1(config)#interface ethernet 1/2
Switch1(Config-If-Ethernet1/2)#port-group 1 mode on
Switch1(Config-If-Ethernet1/2)#exit
Switch1(config)#interface ethernet 1/3
Switch1(Config-If-Ethernet1/3)#port-group 1 mode on
Switch1(Config-If-Ethernet1/3)#exit
Switch1(config)#interface ethernet 1/4
Switch1(Config-If-Ethernet1/4)#port-group 1 mode on
Switch1(Config-If-Ethernet1/4)#exit
Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/6
Switch2(Config-If-Ethernet1/6)#port-group 2 mode on
Switch2(Config-If-Ethernet1/6)#exit
Switch2(config)#interface ethernet 1/8-10
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 S1 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. 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:

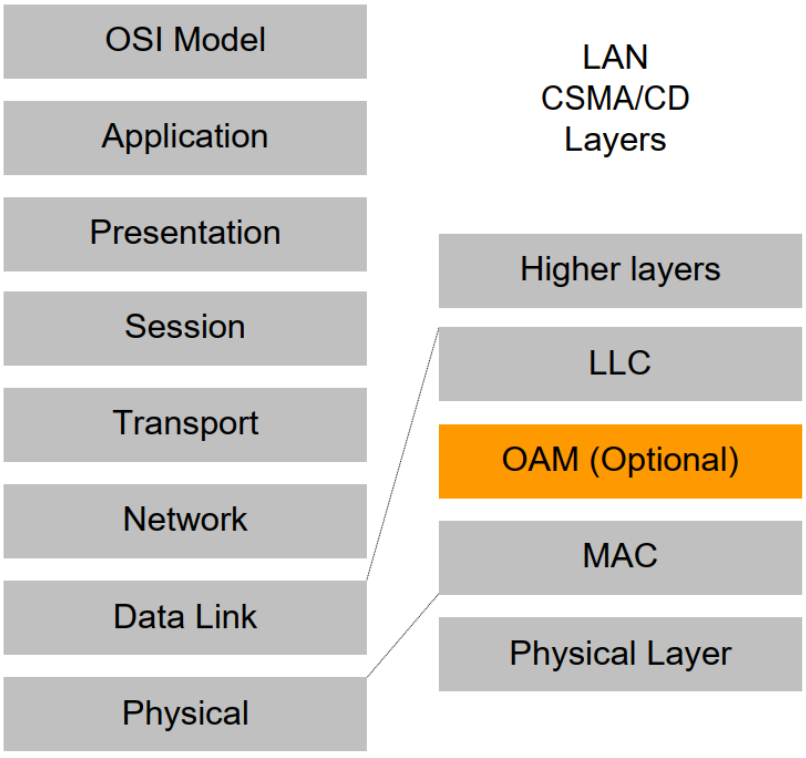


Рисунок 10-1. Положение OAM в OSI модели сети

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 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».

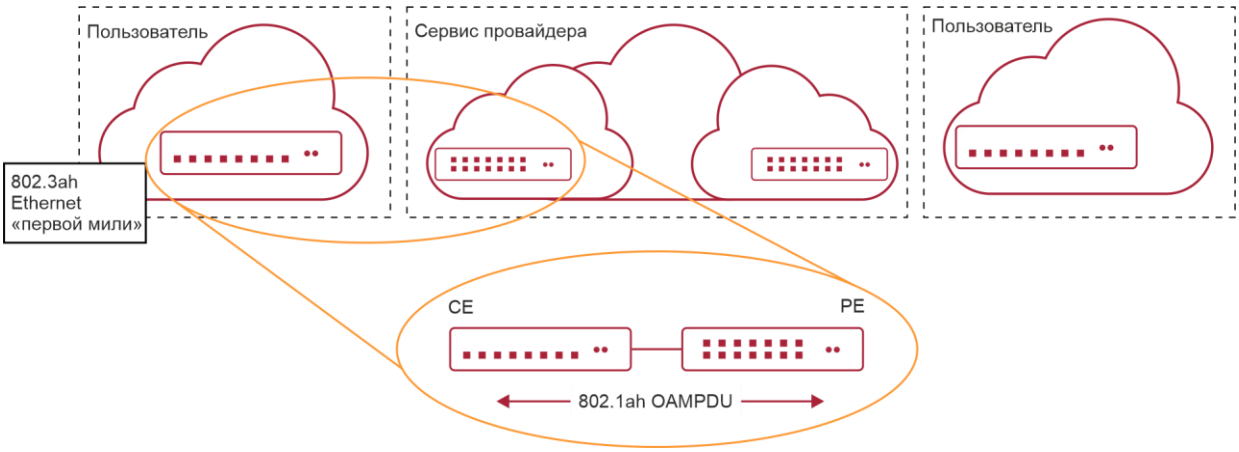


Рисунок 10-2. Типовое применение OAM-топологии

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>} no ethernet-oam errored-frame-period {threshold low | window }	Конфигурирование нижнего порога ошибок и окна фиксации периода 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

Команда	Описание
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 билжнем 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} no ethernet-oam errored-frame-seconds threshold high	Конфигурирование верхнего предела ошибочных секунд приема фреймов. Команда NO 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.

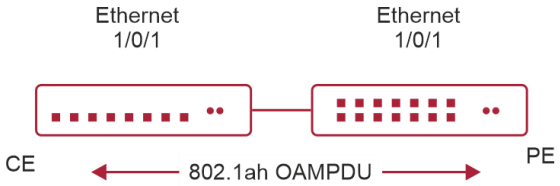


Рисунок 10-3. Типовая топология применения OAM

Процедура конфигурации: (опуская конфигурацию SNMP и логгирования).

Конфигурация клиентского устройства (CE):

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

Другие параметры используются по умолчанию.

Конфигурация на PE:

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

Другие параметры используются по умолчанию.

При необходимости использования удаленной петли используется следующая команда.

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

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

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

Выполнение следующей команды отключает поддержку удаленной петли.

```
CE(config-if-ethernet1/1)#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 доступно неавторизированных устройств сети, проверяя MAC-адрес источика 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 повышае 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>]	Настройка 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}} no switchport port-security violation aging {static | time | type}	Включает время или тип старения port-security на интерфейсе

Команда	Описание
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

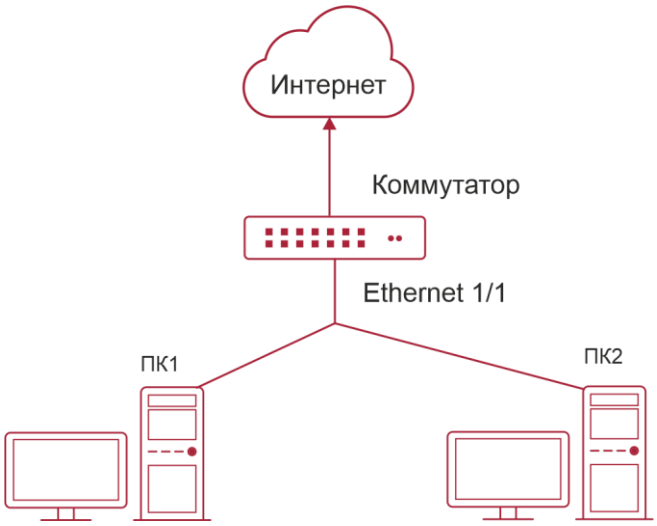


Рисунок 11-1. Типичная схема топологии для безопасности порта

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 1/1
Switch(config-if-ethernet1/1)#switchport port-security
Switch(config-if- ethernet1/1)#switchport port-security maximum 10
Switch(config-if- ethernet1/1)#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 предоставдяет 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 потенциаотных проблем по мониторингу напряжения и температуры модуля.

1.1. Высокое напряжение Vcc приведет к поломке CMOS, низкое – к неправильной работе.

1.2. Высокая RX-мощность пориведет к повреждению принимающего модуля, из-за низкой RX-мощности модуль не сможет нормально работать.

1.3. Высокая температура приведет к быстрому старению аппаратных средств.

1.4. 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:

3.1. Напряжение превышает установленный диапазон.

3.2. Rx power приводит к перезагрузке или к меньшей чувствительности приемопередатчика.

3.3. 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, состоние в реальном масштабе времени и т.д.). Кроме того, проверка информации о неисправностях оптических модулей помогает администратору быстро обаружить 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 значеня порогов. Потому, что пользовательское окружение различно, пользователь может определить значение порога (вдодящая 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 оповещени 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 состония 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.
   3.1. Настройка интервала мониторинга трансивера.
   3.2. Настройка состояния включения мониторинга трансивера.
   3.3. Просмотр информации мониторинга трансивера.
   3.4. 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.
   3.1. 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

3.2. 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 состояние неисправности. После отключения функции на порте, информация о неисправности будет стерта

3.3. 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

3.4. 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:

Ethernet 21 и Ethernet 23 включены в оптический модуль с DDM, Ethernet 24 включен в оптический модуль без DDM, Ethernet 22 не включен в какой-либо оптический модуль, просмотр информации о DDM на оптическом модуле.

1. 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)
1/21		333,31	6,11	−30,54 (A−)	−6,01

Interface Temp (°C)	Voltage (V)	Bias (mA)	RX Power (dBM)	TX Power (dBM)
1/23	335,00 (W+)	6,11	−20,54 (W−)	−6,02

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

   Switch#show transceiver interface ethernet 1/21-22;23 \

Interface Temp (°C)	Voltage (V)	Bias (mA)	RX Power (dBM)	TX Power (dBM)
1/21	333,31	6,11	−30,54 (A−)	−6,01
1/22	N/A	N/A	N/A	N/A
1/23	335,00 (W+)	6,11	−20,54 (W−)	−6,02

3. 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 1/21-22;24 detail

   Ethernet 1/21 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

	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn
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 1/22 transceiver detail information: N/A

Ethernet 1/24 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:

Ethernet 21 включен в оптический модуль с DDM. Настройка порогового значения на оптическом модуле после просмотра информаци о DDM.

Шаг 1. Просмотр подробной информации о DDM.

Switch#show transceiver interface ethernet 1/21 detail

Ethernet 1/21 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

	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn
RX Power (dBM)	−30,54 (A−)	9,00	−25,00	9,00	−25,00
TX Power (dBM)	−13,01	9,00	−25,00	9,00	−25,00

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 1/21
Switch(config-if-ethernet1/21)#transceiver threshold tx-power low-warning -12
Switch(config-if-ethernet1/21)#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 1/21 detail
Ethernet 1/21 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

	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn
TX Power (dBM)	−13,01 (A-)	9,00	−12,00 (−25,00)	9,00	−10,00 (−25,00)

Пример 3:

Ethernet 21 включен в 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 1/21-22
Ethernet 1/21 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn't exist.
Ethernet 1/22 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 1/21
Switch(config-if-ethernet1/21)#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 информаци о DDM, превышающая пороговое значение также показана:

```
Switch(config-if-ethernet1/21)#quit
Switch(config)#show transceiver threshold-violation interface ethernet 1/21-22
Ethernet 1/21 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 1/22 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 отправлять LLDP-MED Inventory Management TLVs. Команда no отменяет функцию

Команда	Описание
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 ECS ELIN	Настройка конфигурацию расположения с форматом на порте. Команда no отменяет
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

Команда	Описание
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

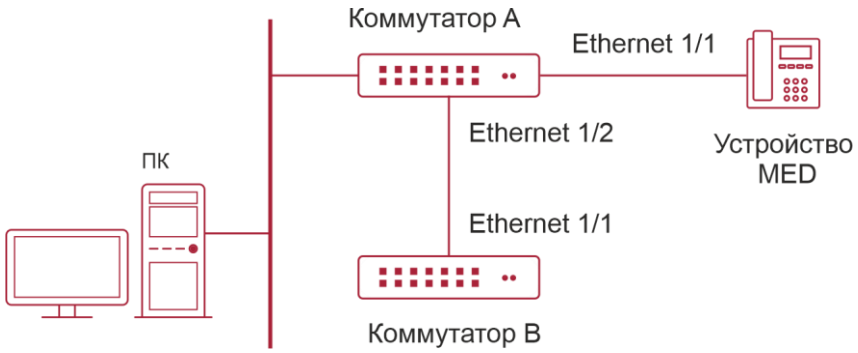


Рисунок 13-1. Топология базовой конфигурации LLDP-MED

1. Настройка Switch A.

SwitchA(config)#interface ethernet1/1

SwitchA (Config-If-Ethernet1/1)# lldp enable

SwitchA (Config-If-Ethernet1/1)# lldp mode both（this configuration can be omitted, the default mode is RxTx）

SwitchA (Config-If-Ethernet1/1)# lldp transmit med tlv capability

SwitchA (Config-If-Ethernet1/1)# lldp transmit med tlv network policy

SwitchA (Config-If-Ethernet1/1)# lldp transmit med tlv inventory

SwitchB (Config-If-Ethernet1/1)# network policy voice tag tagged vid 10 cos 5 dscp 15

SwitchA (Config-If-Ethernet1/1)# exit

SwitchA (config)#interface ethernet1/2

SwitchA (Config-If-Ethernet1/2)# lldp enable

SwitchA (Config-If-Ethernet1/2)# lldp mode both

2. Настройка Switch B.

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

3. Проверьте конфигурацию.

Просмотр глобального статуса и статуса интерфейса на SwitchA.

```
SwitchA# show lldp neighbors interface ethernet 1/1
Port name : Ethernet1/1 Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :00-1f-ce-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 1/2

Port name : interface ethernet 1/2

Port Remote Counter : 1

Neighbor Index: 1

Port name : Ethernet1/2

Port Remote Counter : 1

TimeMark :20

ChassisIdSubtype :4

ChassisId :00-1f-ce-00-00-02

PortIdSubtype :Local

PortId :1

PortDesc :Ethernet1/1

SysName :****

SysDesc :*****

SysCapSupported :4

SysCapEnabled :4

Пояснение:

1. Ethernet 2 коммутатора A и Ethernet 1 коммутатора B являются портами устройства сетевого соединения, они не пересылают пакеты с информацией MED TLV. Хотя Ethernet 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 2 коммутатора A.
2. Устройство LLDP-MED может посылать пакеты LLDP с MED TLV, поэтому в соответствующей удаленной таблице будет информация об Ethernet 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 отправляеемая 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 информационных данных, поступающих от пользовательской сети и передачи их друго сети некоторой корпорации через сеть оператора. Для поддержания локальной концепции, необходима не только передача данных от пользовательских частных сетей через туннель, но также передача пекетов 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 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.

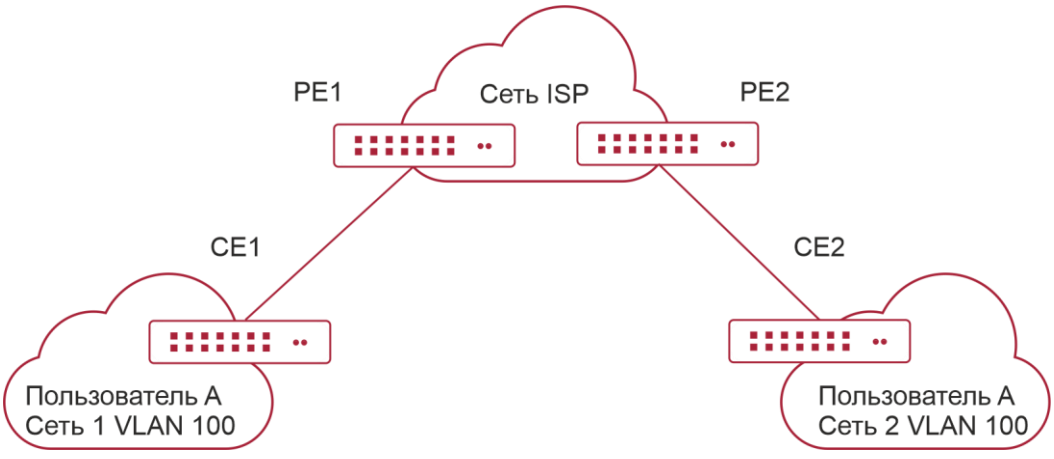


Рисунок 14-1. Применение BPDU-туннеля

14.2. Конфигурация BPDU-tunnel

Настройка порта для поддержки туннеля.

Команда	Описание
Режим конфигурирования порта	
bpdu-tunnel {stp|gvrp | dot1x | user-defined-protocol} no bpdu-tunnel {stp|gvrp | dot1x | user-defined-protocol}	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.

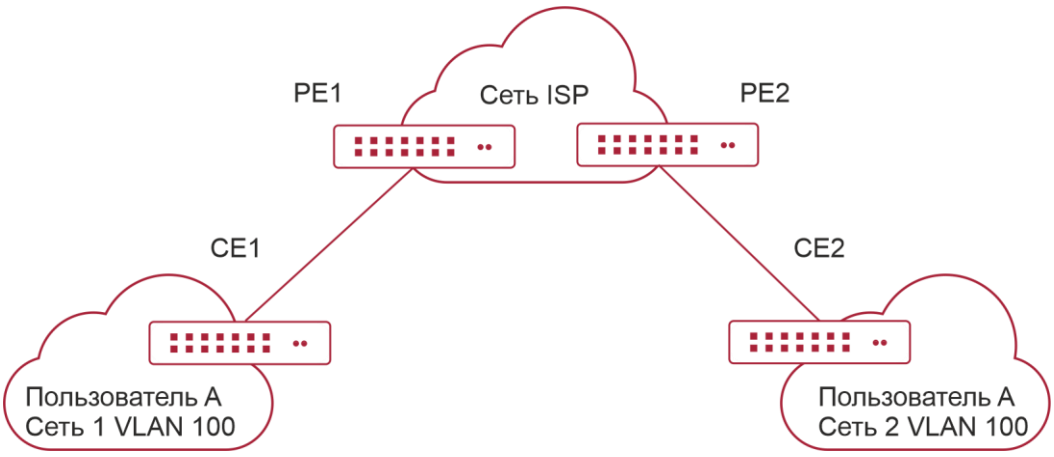


Рисунок 14-2. Применение BPDU-туннеля

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.

Настройка BPDU-tunnel на коммутаторах PE1 и PE2:

Настройка PE 1:

```
PE1(config-if-ethernet1/1)# bpdu-tunnel stp
PE1(config-if-etherne1/1)# bpdu-tunnel lacp
PE1(config-if-ethernet1/1)# bpdu-tunnel uldp
PE1(config-if-ethernet1/1)# bpdu-tunnel gvrp
PE1(config-if-ethernet1/1)# bpdu-tunnel dot1x
```

Настройка PE 2:

```
PE2(config-if-ethernet1/1)# bpdu-tunnel stp
PE2(config-if-ethernet1/1)# bpdu-tunnel lacp
PE2(config-if-ethernet1/1)# bpdu-tunnel uldp
PE2(config-if-ethernet1/1)# bpdu-tunnel gvrp
PE2(config-if-ethernet1/1)# bpdu-tunnel dot1x
```

14.4. Устранение неисправностей BPDU-tunnel

После отключения функций stp, gvrp, uldp, lacp and 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.

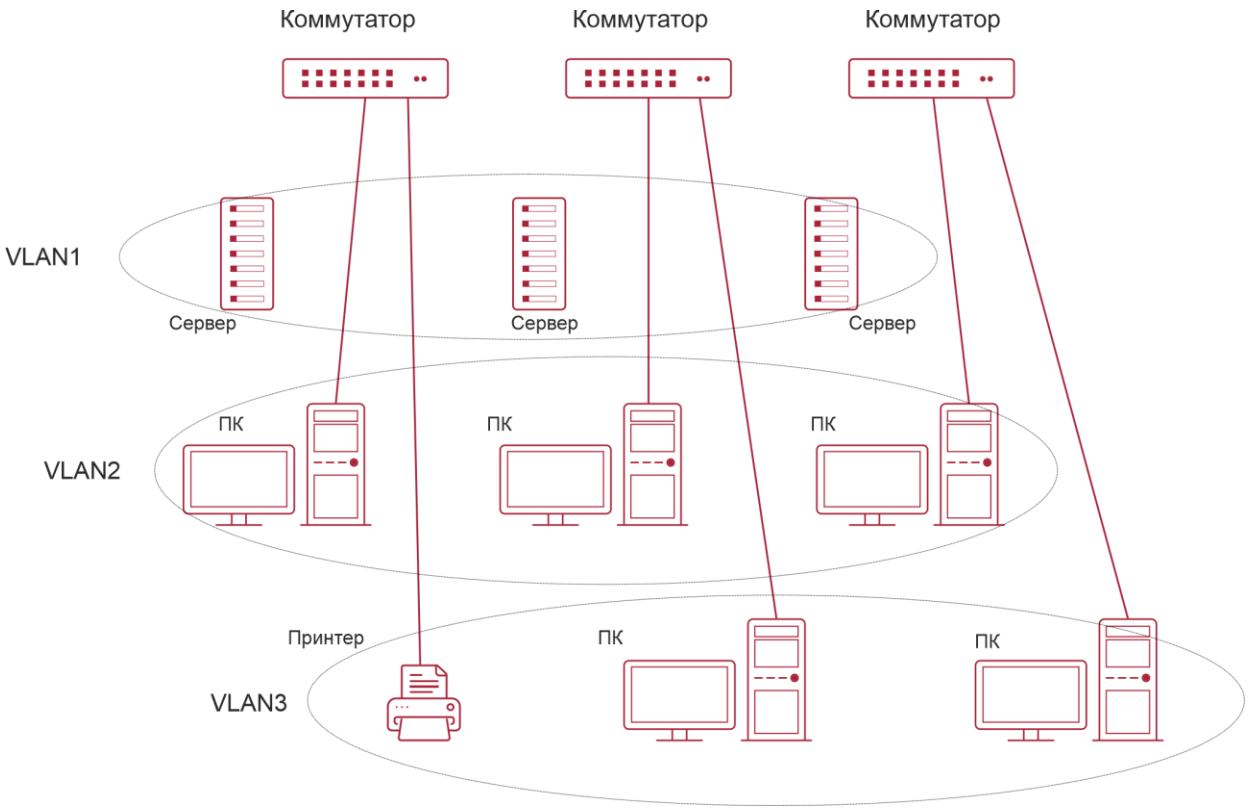


Рисунок 15-1. Логическое определение сети VLAN

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. 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

Команда	Описание
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 VLAN'е

9. Конфигурация приватного VLAN’a.

Команда	Описание
VLAN mode	
private-vlan {primary | isolated | community} no private-vlan	Конфигурация текущего VLAN’a 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

Сценарий:

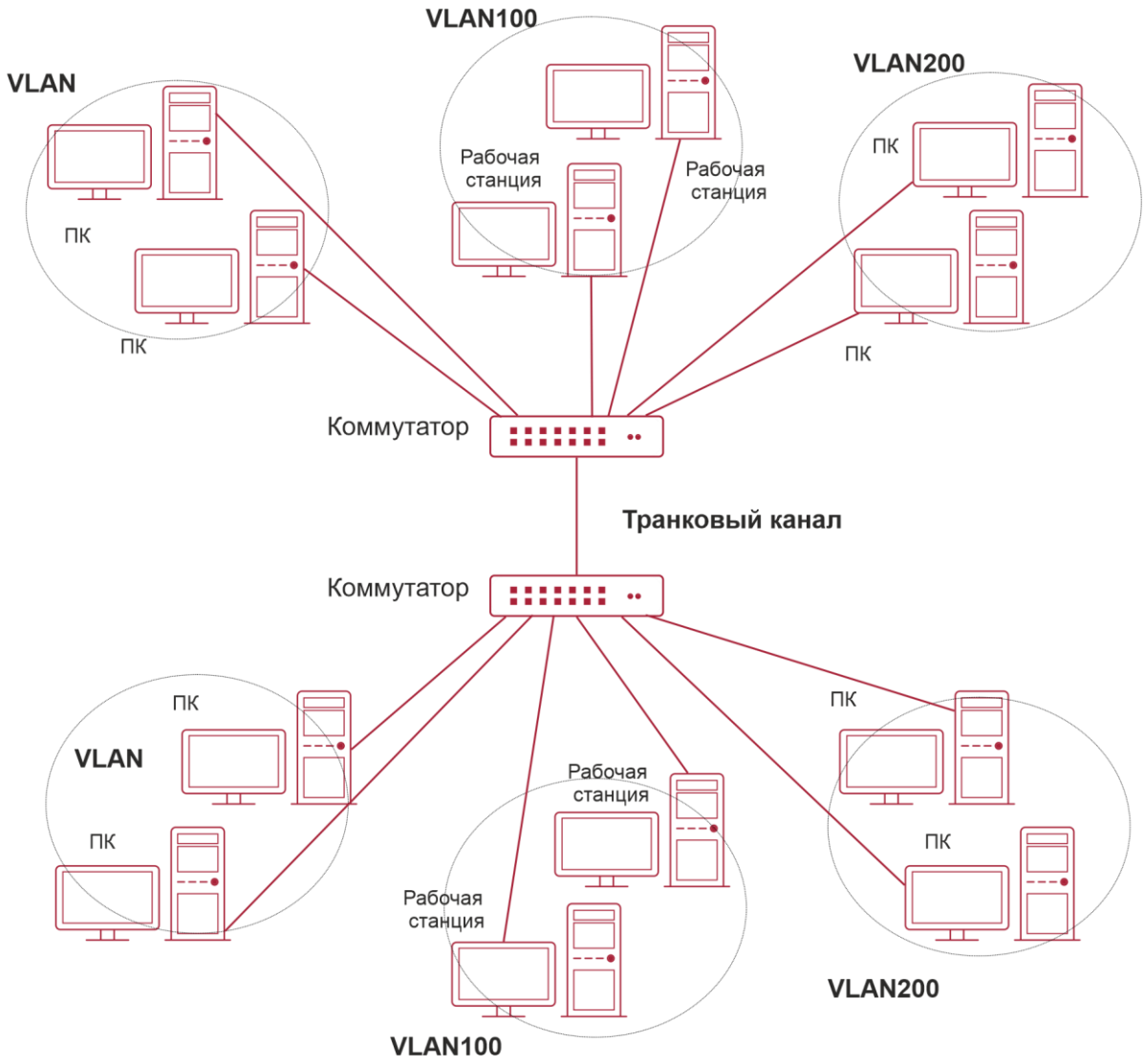


Рисунок 15-2. Типичная топология применения VLAN’a

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 -4

Объект конфигурации	Описание конфигурации
VLAN100	Site A and site B switch port 5 -7
VLAN200	Site A and site B switch port 8 -10
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.

Шаги конфигурации описаны ниже:

Коммутатор A:

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

Коммутатор B:

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

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

15.1.4. Типичное применение гибридных портов

Сценарий:

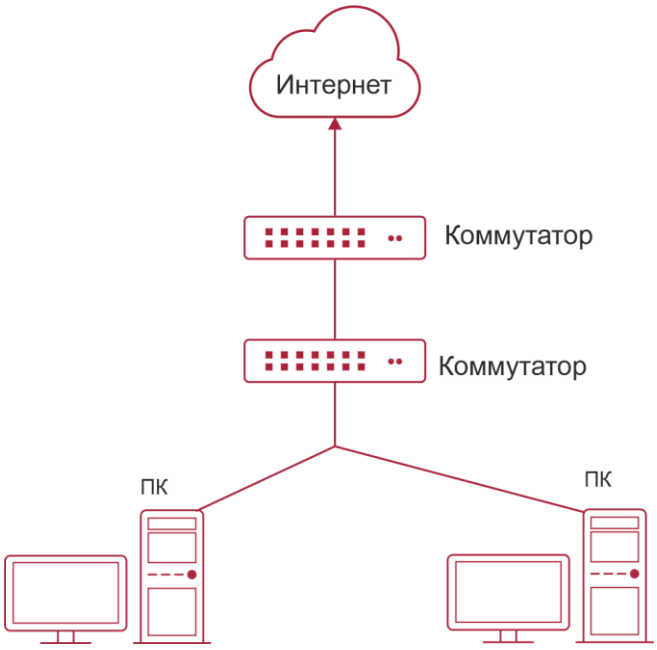


Рисунок 15-3. Типичное применение гибридного порта

PC1 подключен к интерфейсу Ethernet 1/7 коммутатора B, PC2 подключен к интерфейсу Ethernet 1/9 коммутатора B. Порт Ethernet 1/10 коммутатора A к порту Ethernet 1/10 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 1/10 of Switch A	Access	10	Пропускает пакеты VLAN’а 10 без меток
Port 1/10 of Switch B	Hybrid	10	Пропускает пакеты VLAN’ов 7,9, 10 без меток
Port 1/7 of Switch B	Hybrid	7	Пропускает пакеты VLAN’ов 7, 10 без меток
Port 1/9 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 1/10
```

Коммутатор B:

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

Рисунок 15-4. Межсетевое взаимодействие на основе Dot1q-туннеля

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.

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	Порт1 узлов PE1 и PE2
dot1q-tunnel	Порт1 узлов PE1 и PE2
tpid	9100

Процедура конфигурации описана ниже:

PE1:

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/1
Switch(Config-Vlan3)#exit
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)# dot1q-tunnel enable
```

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

PE2:

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

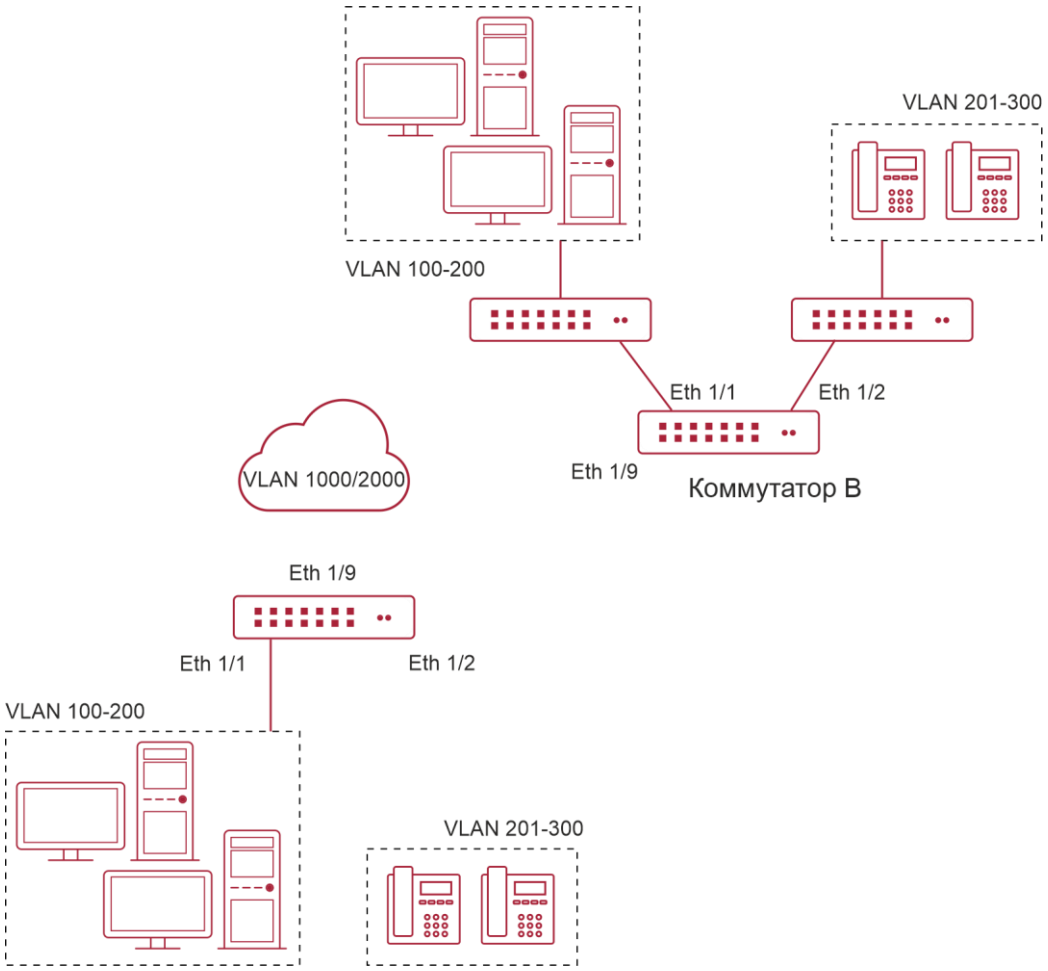


Рисунок 15-5. Применение Selective QinQ

1. Ethernet1/1 коммутатора A предоставляет доступ к сети общего пользования для пользователей PC и Ethernet1/2 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 1/9 коммутатора A соединена с сетью общего пользования.
2. Ethernet1/1 и Ethernet1/2 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 1/9 соединена с сетью общего пользования.
3. Сеть общего пользования разрешает пересылать пакеты в VLAN 1000 и VLAN 2000.
4. Включен selective QinQ на портах Ethernet1/1 и Ethernet1/2 на коммутаторах A и B соответственно. Пакеты VLAN 100- VLAN 200 отмечены тегом VLAN 1000 как выходящий тег VLAN на Ethernet1/1, и пакеты VLAN 201- VLAN 300 отмечены тегом VLAN 2000 как выходящий тег VLAN на Ethernet1/2.

Конфигурирование:

Создание VLAN 1000 and VLAN 2000 on SwitchA.

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

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

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

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

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

Включение selective QinQ на Ethernet1/1.

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

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

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

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

```
switch(config-if-ethernet1/2)#dot1q-tunnel selective s-vlan 2000 c-vlan 201-300
```

Включение selective QinQ на Ethernet 1/2.

```
switch(config-if-ethernet1/2)#dot1q-tunnel selective enable
```

Настройка порта Ethernet 1/9 как гибридного порта и настройка сохранения тега VLAN при пересылке пакетов в VLAN 1000 и VLAN 2000.

```
switch(config-if-ethernet1/2)#interface ethernet 1/9
switch(config-if-ethernet1/9)#switchport mode hybrid
switch(config-if-ethernet1/9)#switchport hybrid allowed vlan 1000;2000 tag
```

После проведения конфигурации, пакеты VLAN 100-VLAN 200 от Ethernet1/1 автоматически отмечаются тегом с VLAN 1000 как выходящим тегом VLAN, и пакеты VLAN 201- VLAN 300 от Ethernet1/2 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 1/1
switch(config-if-ethernet1/1)#switchport mode hybrid
switch(config-if-ethernet1/1)#switchport hybrid allowed vlan 1000 untag
switch(config-if-ethernet1/1)#dot1q-tunnel selective s-vlan 1000 c-vlan 100-200
switch(config-if-ethernet1/1)#dot1q-tunnel selective enable
switch(config-if-ethernet1/1)#interface ethernet 1/2
switch(config-if-ethernet1/2)#switchport hybrid allowed vlan 2000 untag
switch(config-if-ethernet1/2)#dot1q-tunnel selective s-vlan 2000 c-vlan 201-300
switch(config-if-ethernet1/2)#dot1q-tunnel selective enable
switch(config-if-ethernet1/9)#switchport mode hybrid
switch(config-if-ethernet1/9)#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 трансляции соответствий 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 PE1 Подключен к CE1, порт 10 подключен к публичной сети, порт 1 PE2 подключен к CE2, порт 10 подключен к публичной сети.

Рисунок 15-6. Топология сети с трансляцией VLAN'ов

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

Процедура конфигурирования указана ниже:

PE1, PE2:

```
switch(Config)#interface ethernet 1/1
```

```
switch(Config-Ethernet1/1)#switchport mode trunk
switch(Config-Ethernet1/1)# vlan-translation enable
switch(Config-Ethernet1/1)# vlan-translation 20 to 3 in
switch(Config-Ethernet1/1)# vlan-translation 3 to 20 out
switch(Config-Ethernet1/1)# exit
switch(Config)#interface ethernet 1/1
switch(Config-Ethernet1/1)#switchport mode trunk
switch(Config-Ethernet1/1)#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 A, B и C принаддлежат VLAN 1, 2 и 3 соответственно. На входящем сетевом уровне, траффик данных пользователей A, B и C будет переведен в VLAN100 на Ethernet1/1 со стороны Switch 1. Обратно траффик данных пользователей A, B и C будет переведен в VLAN 1, 2 и 3 на Ethernet1/1 со стороны Switch 1от сетевого уровня соответственно. Таким же образом реализуется аналогичнвй перевод трансляции multi-to-one между пользователями D, E и F на Ethernet1/1 и Switch 2.

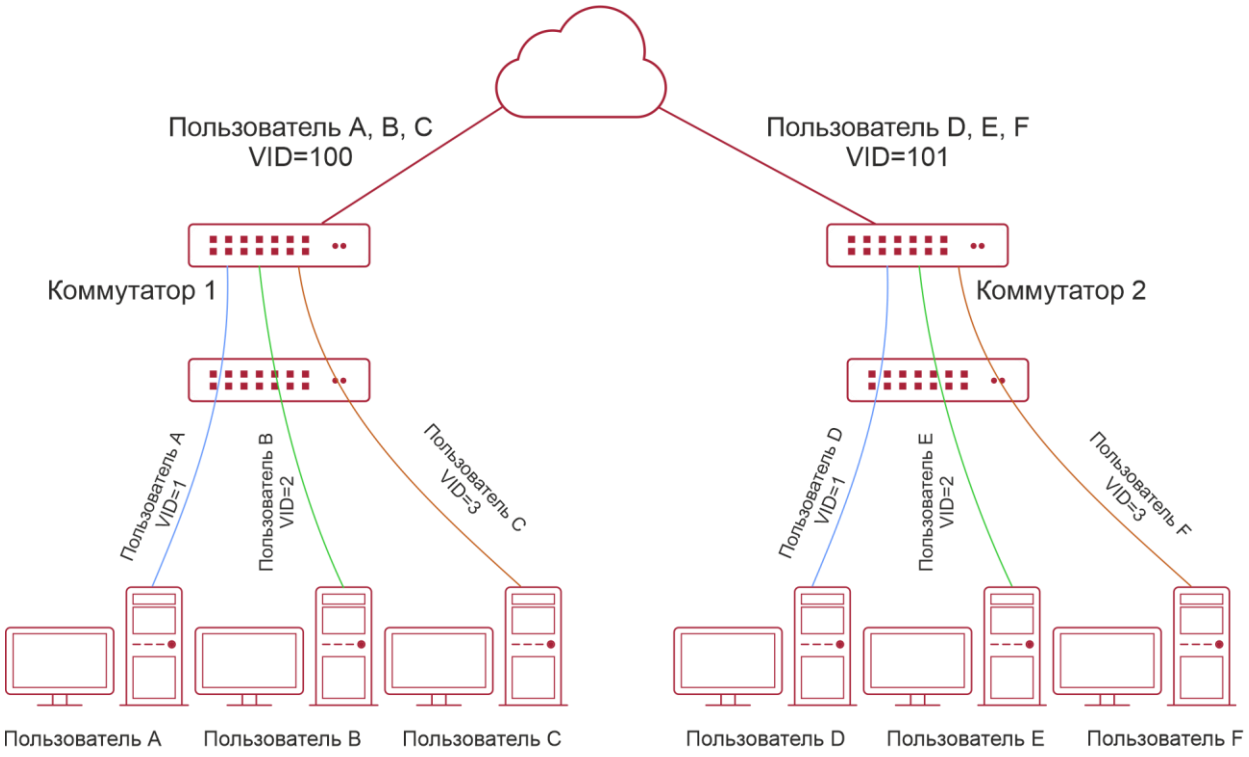


Рисунок 15-7.

Элемент конфигурации	Описание
VLAN	Switch1, Switch2

Элемент конфигурации	Описание
Trunk Port	Нисходящий порт 1/1 и восходящий порт 1/5 на Switch1 и Switch 2
Multi-to-One VLAN-трансляция	Нисходящий порт 1/1 на Switch1 и Switch2

Процедура настройки:

Switch1, Switch2:

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

15.5.4. Устранение неисправностей Multi-to-One VLAN-трансляции

- Нельзя одновременно использовать с Dot1q-tunnel.
- Нельзя одновременно использовать с VLAN-translation.
- MAC-адрес 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 VLAN'е при перемещении из одного места в другое. Как мы 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 VLAN'е

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 etype <etype-id> vlan <vlan-id> no protocol-vlan {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 – М. MAC-адрес его компьютера – 00-1f-ce-11-22-33, когда М переключается в VLAN200 или VLAN300, порт, к которому подключается М, конфигурируется как гибридный и подключается к VLAN100 в режиме «без меток». В этом случае данные VLAN100 будут передаваться на порт, к которому подключен М, и обеспечивать требования связности в VLAN100.

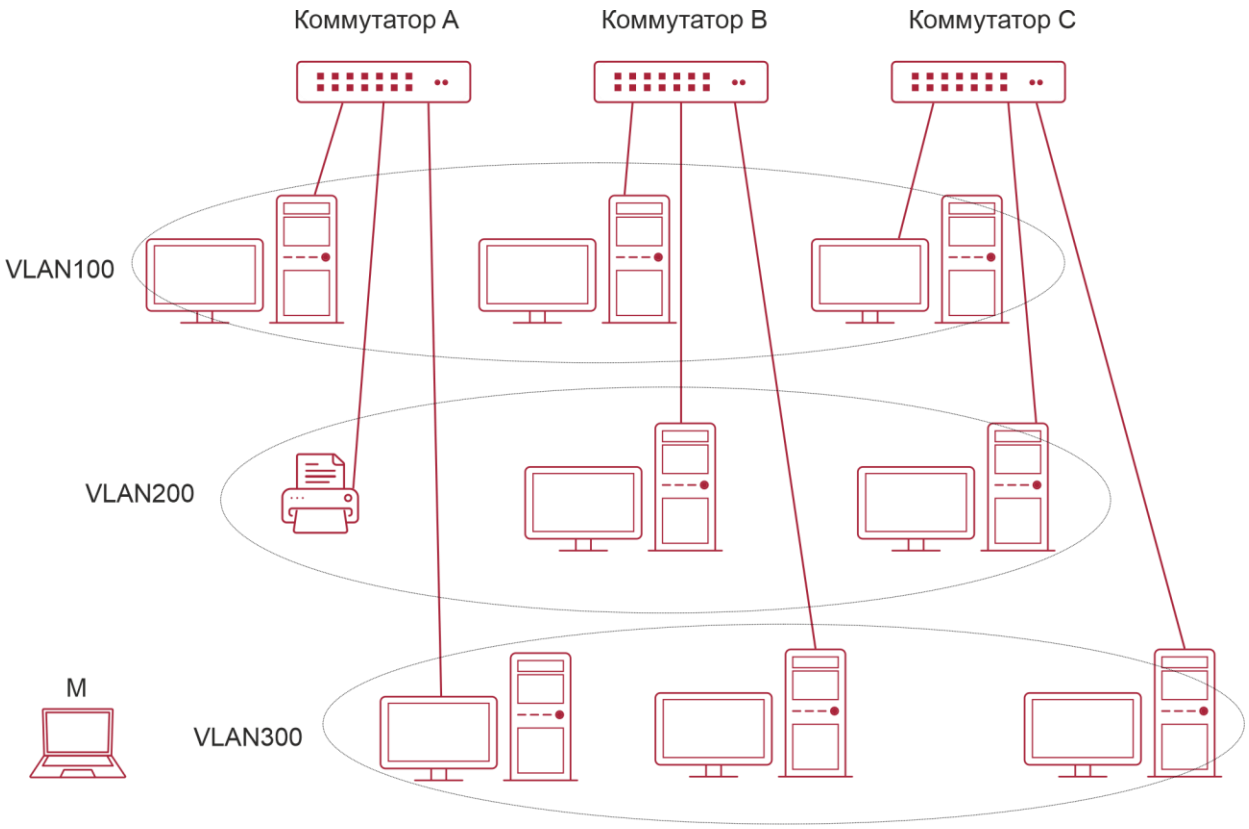


Рисунок 15-8. Типовая топология применения динамического VLAN'а

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 00-1f-ce-11-22-33 vlan 100 priority 0
switch(Config)#exit
switch#
```

15.6.4. Устранение неисправностей динамического VLAN'а

На коммутаторах со сконфигурированным динамическим VLAN'ом, 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.

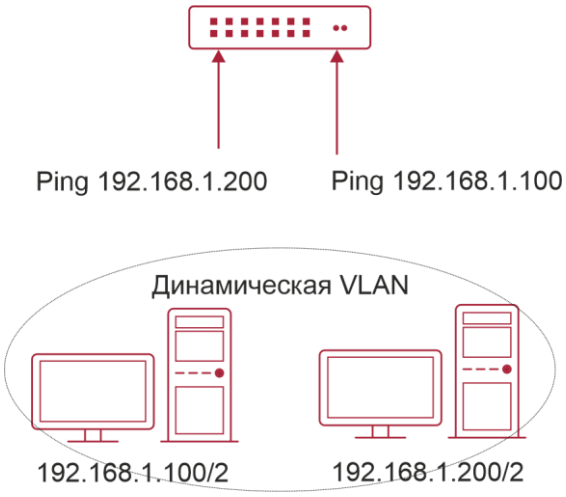


Рисунок 15-9. Устранение неисправностей динамического VLAN'а

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-членами 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.

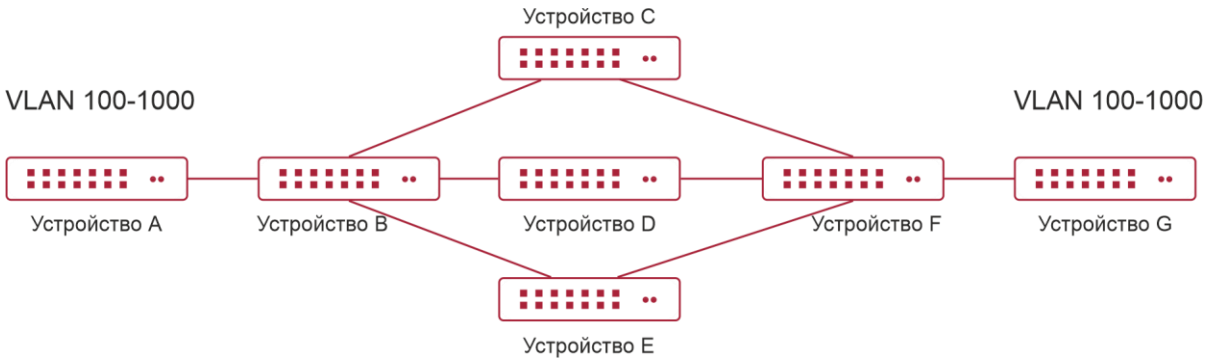


Рисунок 15-10. Типичная схема применения

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:

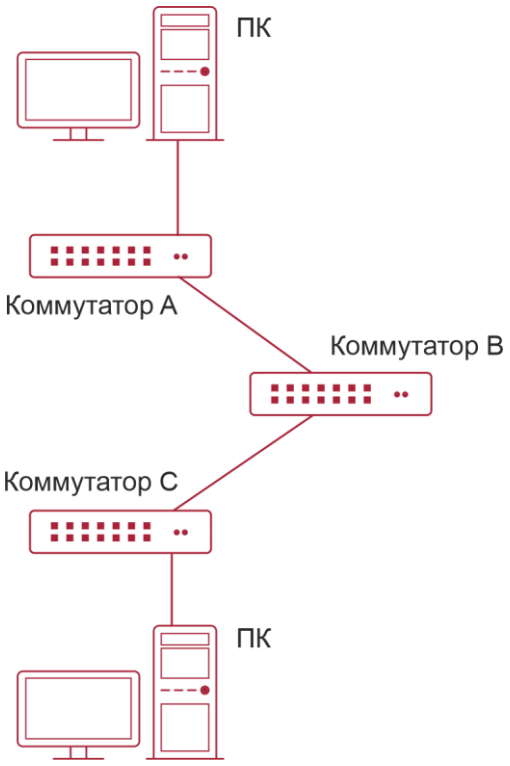


Рисунок 15-11. Типичная топология применения GVRP

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

Объект настройки	Описание объекта настройки
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 1/2-6
Switch(Config-Vlan100)#exit
Switch(config)#interface ethernet 1/11
Switch(Config-If-Ethernet1/11)#switchport mode trunk
Switch(Config-If-Ethernet1/11)# gvrp
Switch(Config-If-Ethernet1/11)#exit
```

Коммутатор B:

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

Коммутатор C:

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

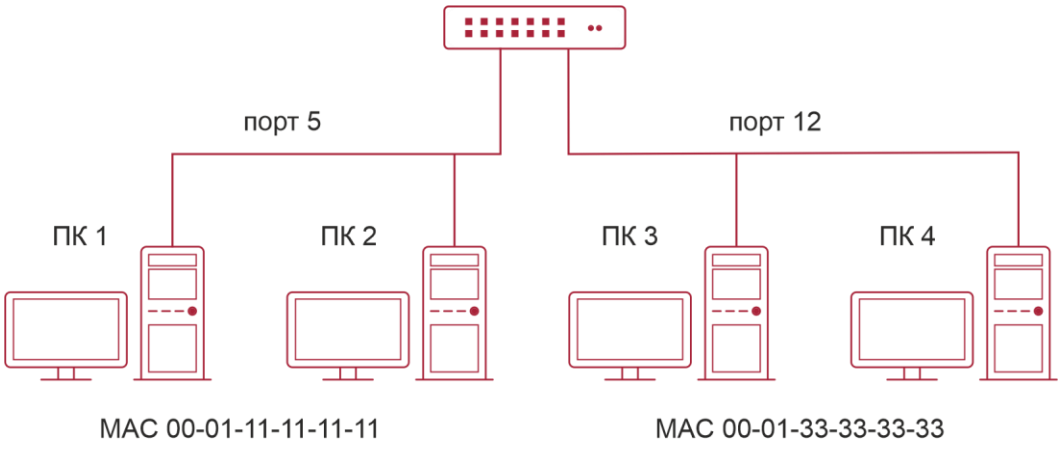


Рисунок 16-1. Динамическое построение таблицы MAC-адресов

Топология на рисунке выше: 4 компьютера подключены к коммутатору, где PC1 и PC2 принадлежат одному физическому сегменту (домену коллизий), физический сегмент подключен к порту 1/5 коммутатора, PC3 и PC4 принадлежат к другому физическому сегменту, подключенному к порту 1/12 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 00-01-11-11-11-11 и порт 1/5 из этого сообщения заносятся в таблицу MAC-адресов коммутатора.
2. В то же время коммутатору надо понять, как доставить сообщение на адрес 00-01-33-33- 33-33. Так как таблица содержит запись только для адреса 00-01-11-11-11-11 и порта 1/5, а для адреса 00-01-33-33-33-33 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 00-01-33-33-33-33, и отвечать на него будет только PC3. Когда порт 1/12 получает сообщение, отправленное PC3, в таблицу MAC-адресов добавляется запись о MAC-адресе 00-01-33-33-33-33 и соответствующем ему порте 1/12.
4. Теперь таблица MAC-адресов имеет две динамические записи: MAC-адрес 00-01-11-11-11- 11 – порт 1/5 и 00-01-33-33-33-33 – порт 1/12.
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.

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
00-01-11-11-11-11	1/5	Динамическое обучение
00-01-22-22-22-22	1/5	Статическая конфигурация
00-01-33-33-33-33	1/12	Динамическое обучение
00-01-44-44-44-44	1/12	Статическая конфигурация

1. Отправка пакетов в соответствии с таблицей MAC-адресов.

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

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 фреймов:

- широковещательные фреймы;

- многопользовательские фреймы;
- однопользовательские фреймы.

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

1. Широковещательный фрейм: 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 широковещательный фрейм, 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 VLAN'е.
2. Многопользовательский фрейм: если многопользовательский домен неизвестен, коммутатор рассылает фрейм в том же VLAN'е, но, если включена функция IGMP snooping или сконфигурирована статическая многопользовательская группа, коммутатор будет посылать этот фрейм в порты многопользовательской группы.
3. Однопользовательский фрейм: 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 однопользовательский фрейм только внутри одного VLAN'а. Если MAC-адрес найден в таблице, но принадлежит другому VLAN'у, коммутатор делает широковещательную рассылку фрейма в том VLAN'е, 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. 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

3. 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

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
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

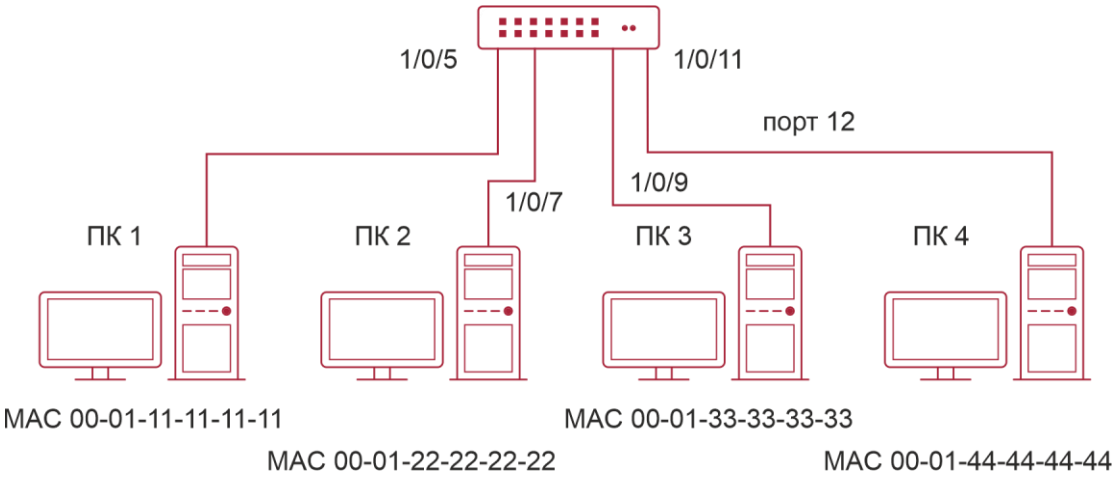


Рисунок 16-2. Типичный пример конфигурации таблицы MAC-адресов

Четыре компьютера, как показано на рисунке, подключены к портам 1/5, 1/7,1/9, 1/11 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.

Этапы конфигурации показаны ниже:

1. Установка MAC-адреса 00-01-11-11-11-11 PC1 как фильтруемого.

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

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

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

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

16.4. Устранение неисправностей с таблицей MAC-адресов

Если при использовании команды show mac-address-table, было выяснено, что на порту произошел сбой оучения 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, 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
switchport port-security mac-address <mac- address> no switchport port-security mac-address <mac- address>	Добавляет статические безопасные MAC-адреса; Команда “no switchport port-security mac-address” удаляет статические безопасные MAC-адреса

Команда	Описание
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 | shutdown | restrict } [recovery <30-3600>] 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 объединение портов 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 уведомлений о MAC-адресах

16.6.1. Введение в уведомления о MAC-адресах

Функция MAC-уведомления зависит от уведомления. Добавляя или удаляя MAC-адреса, а именно, когда добавляются или удаляются устройства, администратор будет уведомлен о смене функции ловушки snmp.

16.6.2. Конфигурация уведомлений о MAC-адресах

1. Настройка глобально snmp MAC-уведомления.
2. Настройка глобального MAC-уведомления.
3. Настройка интервала для отправки MAC-уведомлений.
4. Настройка размера таблицы истории.

5. Настройка типа ловушки MAC-уведомлений, поддерживаемых портом.
6. Просмотр конфигурации и данных MAC-уведомлений.
7. Очистка статистики ловушки MAC-уведомлений.

1. Настройка глобального snmp MAC-уведомления.

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

2. Настройка глобального MAC-уведомления.

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

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 | moved | 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-уведомления

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-Ethernet1/4)# mac-notification all
```

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:

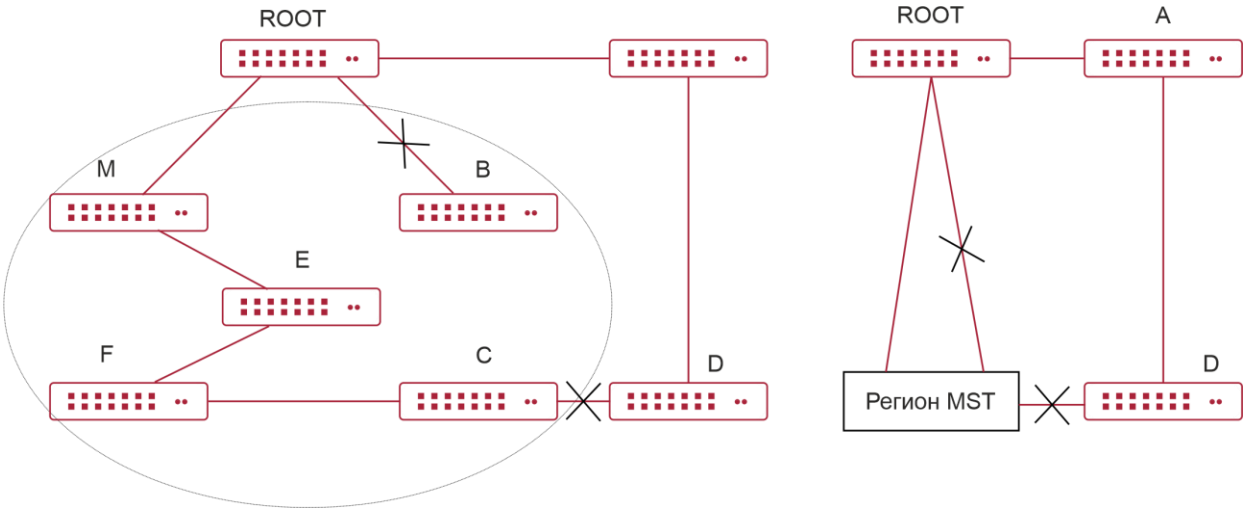


Рисунок 17-1. Пример CIST и региона MST

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

Команда	Описание
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

Команда	Описание
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 региона MSTP
abort	Выход из режима конфигурирования региона MSTP и возврат в режим глобального конфигурирования без сохранения конфигурации региона MSTP
exit	Позволяет сохранить сделанные настройки региона MSTP, выйти из режима настройки регионов MSTP и вернуться в глобальный режим конфигурирования

Команда	Описание
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 spanning-tree portfast 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 spanning-tree format auto no spanning-tree format	Позволяет настроить формат пакета связующего дерева порта. При выборе опции standard пакет соответствует стандартам IEEE, при опции privacy 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

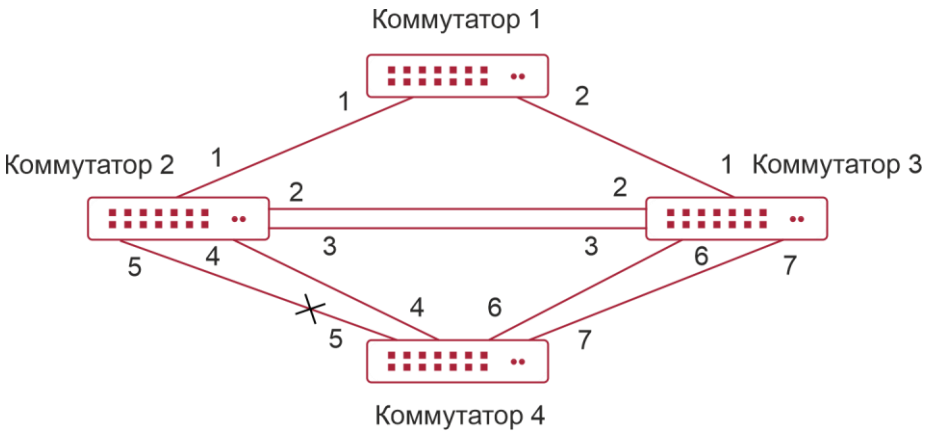


Рисунок 17-2. Типичный сценарий применения MSTP

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		Switch1	Switch2	Switch3	Switch4
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 Switch2, Switch3 и Switch4;
- настроить порты 1-7 как транковые на Switch2, Switch3 и Switch4.

Шаг 2. Установить Switch2, Switch3 и Switch4 как принадлежащих одному дереву MSTP:

- установить на Switch2, Switch3 и Switch4 одно и то же имя региона, совпадающее с именем дерева MSTP;

- привязать VLAN 20 и VLAN 30 на Switch2, Switch3 и Switch4 к экземпляру связующего дерева 3;
- приписать VLAN 40 и VLAN 50 на Switch2, Switch3 и Switch4 к экземпляру связующего дерева 4.

Шаг 3. Настроить Switch3 как корневой коммутатор для экземпляра связующего дерева 3. Настроить Switch4 как корневой коммутатор для экземпляра связующего дерева 4:

- настроить приоритет коммутатора для экземпляра связующего дерева 3 на Switch3 как 0;
- настроить приоритет коммутатора для экземпляра связующего дерева 4 на Switch4 как 0.

Детальная конфигурация приведена ниже:

Switch2:

```
Switch2(config)#vlan 20
Switch2(Config-Vlan20)#exit
Switch2(config)#vlan 30
Switch2(Config-Vlan30)#exit
Switch2(config)#vlan 40
Switch2(Config-Vlan40)#exit
Switch2(config)#vlan 50
Switch2(Config-Vlan50)#exit
Switch2(config)#spanning-tree mst configuration
Switch2(Config-Mstp-Region)#name mstp
Switch2(Config-Mstp-Region)#instance 3 vlan 20;30
Switch2(Config-Mstp-Region)#instance 4 vlan 40;50
Switch2(Config-Mstp-Region)#exit
Switch2(config)#interface e1/0/1-7
Switch2(Config-Port-Range)#switchport mode trunk
Switch2(Config-Port-Range)#exit
Switch2(config)#spanning-tree
```

Switch3:

```
Switch3(config)#vlan 20
Switch3(Config-Vlan20)#exit
Switch3(config)#vlan 30
Switch3(Config-Vlan30)#exit
Switch3(config)#vlan 40
Switch3(Config-Vlan40)#exit
Switch3(config)#vlan 50
Switch3(Config-Vlan50)#exit
Switch3(config)#spanning-tree mst configuration
```

```
Switch3(Config-Mstp-Region)#name mstp
Switch3(Config-Mstp-Region)#instance 3 vlan 20;30
Switch3(Config-Mstp-Region)#instance 4 vlan 40;50
Switch3(Config-Mstp-Region)#exit
Switch3(config)#interface e1/0/1-7
Switch3(Config-Port-Range)#switchport mode trunk
Switch3(Config-Port-Range)#exit
Switch3(config)#spanning-tree
Switch3(config)#spanning-tree mst 3 priority 0
```

Switch4:

```
Switch4(config)#vlan 20
Switch4(Config-Vlan20)#exit
Switch4(config)#vlan 30
Switch4(Config-Vlan30)#exit
Switch4(config)#vlan 40
Switch4(Config-Vlan40)#exit
Switch4(config)#vlan 50
Switch4(Config-Vlan50)#exit
Switch4(config)#spanning-tree mst configuration
Switch4(Config-Mstp-Region)#name mstp
Switch4(Config-Mstp-Region)#instance 3 vlan 20;30
Switch4(Config-Mstp-Region)#instance 4 vlan 40;50
Switch4(Config-Mstp-Region)#exit
Switch4(config)#interface e1/0/1-7
Switch4(Config-Port-Range)#switchport mode trunk
Switch4(Config-Port-Range)#exit
Switch4(config)#spanning-tree
Switch4(config)#spanning-tree mst 4 priority 0
```

После настройки, описанной выше, Switch1 будет корневым коммутатором экземпляра связующего дерева 0 всей сети. В регионе MSTP, к которому относятся Switch2, Switch3 и Switch4, Switch 2 является корневым коммутатором региона для экземпляра связующего дерева 0, Switch3 является корневым коммутатором региона для экземпляра связующего дерева 3 и Switch4 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 Switch2 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.

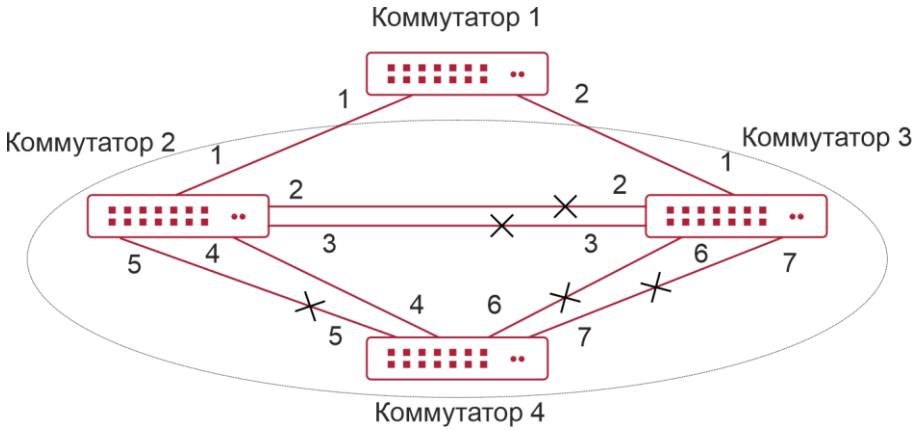


Рисунок 17-3. Топология экземпляра связующего дерева 0 после вычисления MSTP

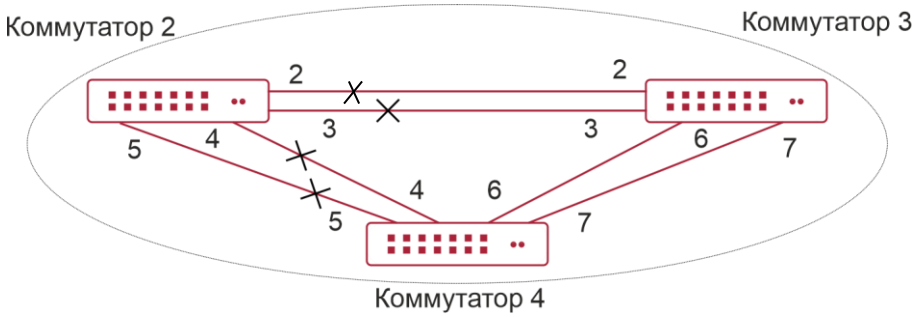


Рисунок 17-4. Топология экземпляра связующего дерева 3 после вычисления MSTP

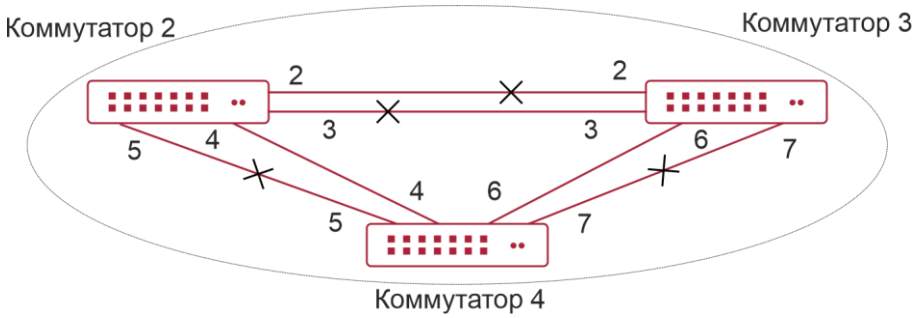


Рисунок 17-5. Топология экземпляра связующего дерева 4 после вычисления MSTP

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.

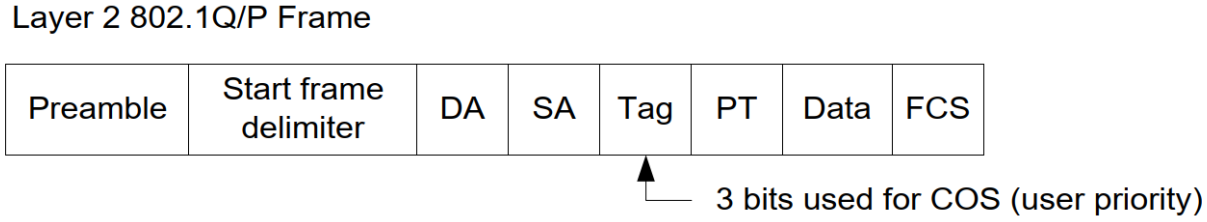


Рисунок 18-1. Приоритеты Класса сервиса

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.

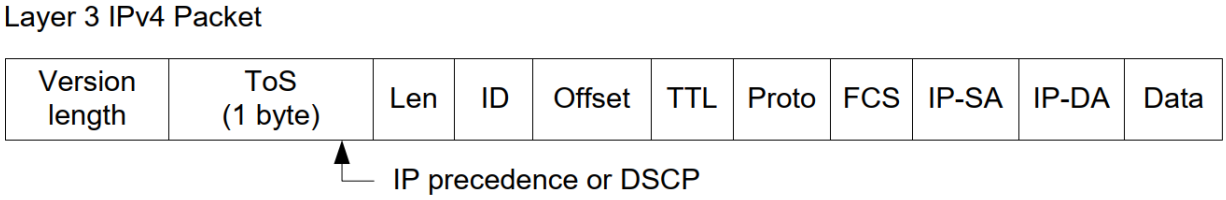


Рисунок 18-2. Приоритет ToS

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

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 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, и 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.

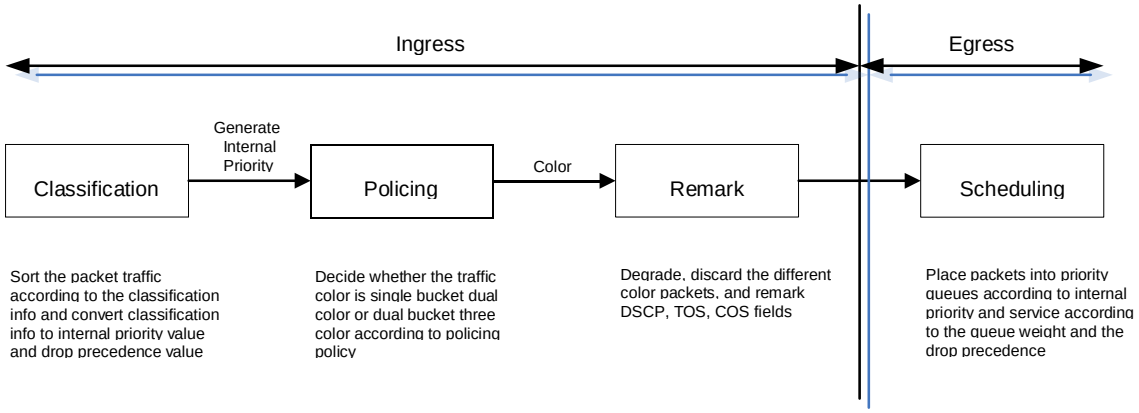


Рисунок 18-3. Базовая модель QoS

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.

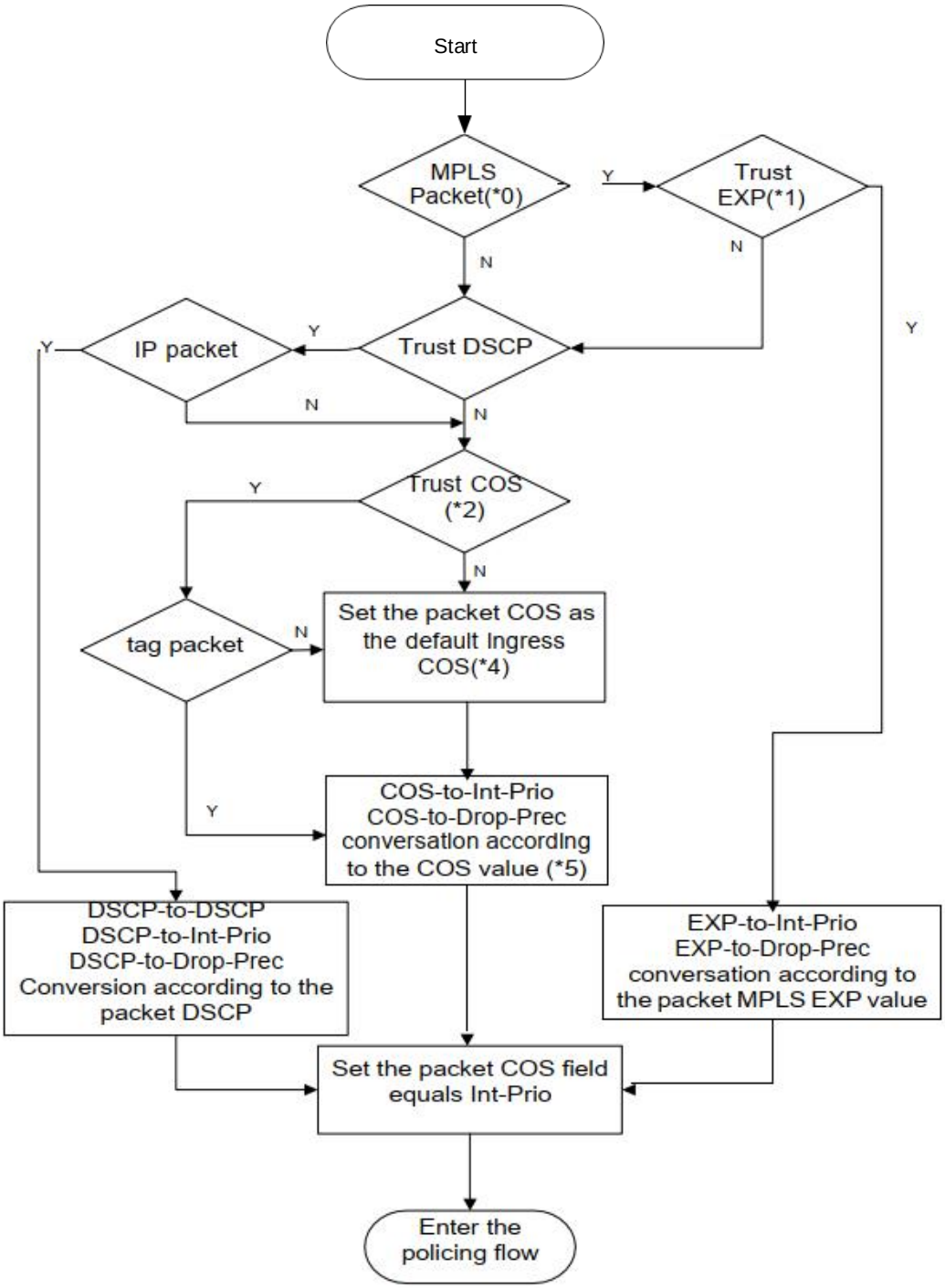


Рисунок 18-4. Процесс классификации

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.

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.

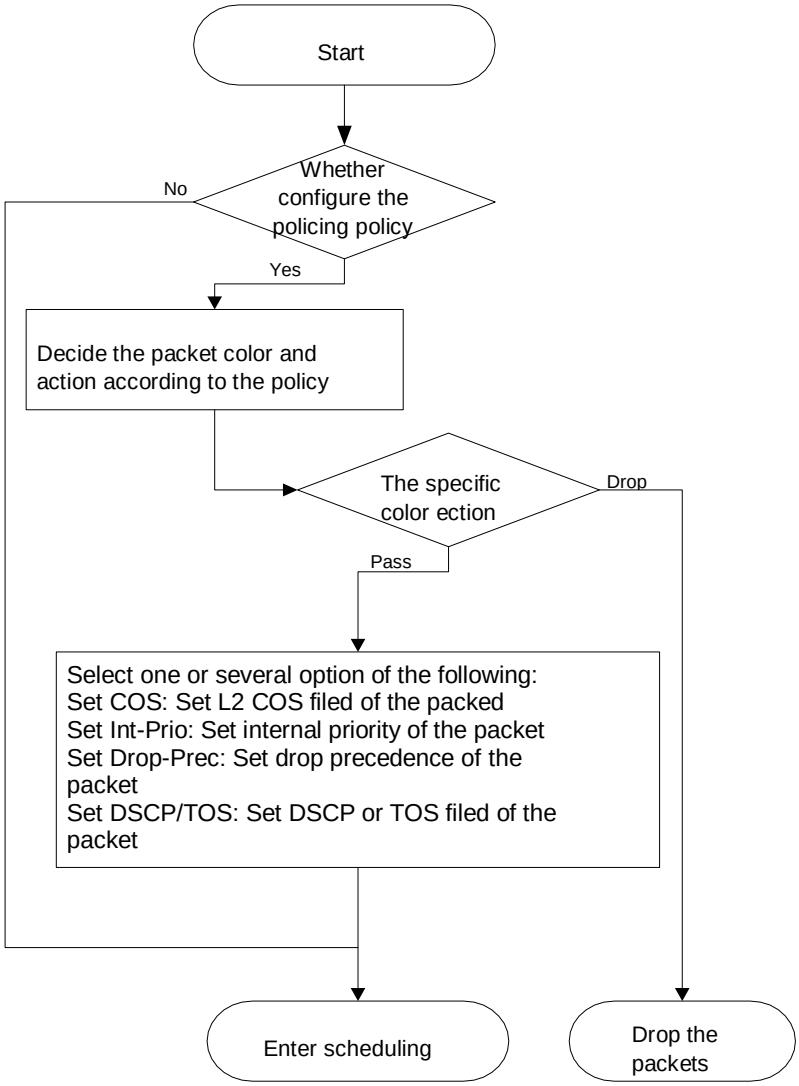


Рисунок 18-5. Процессы Регулирования и пометки

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.

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.

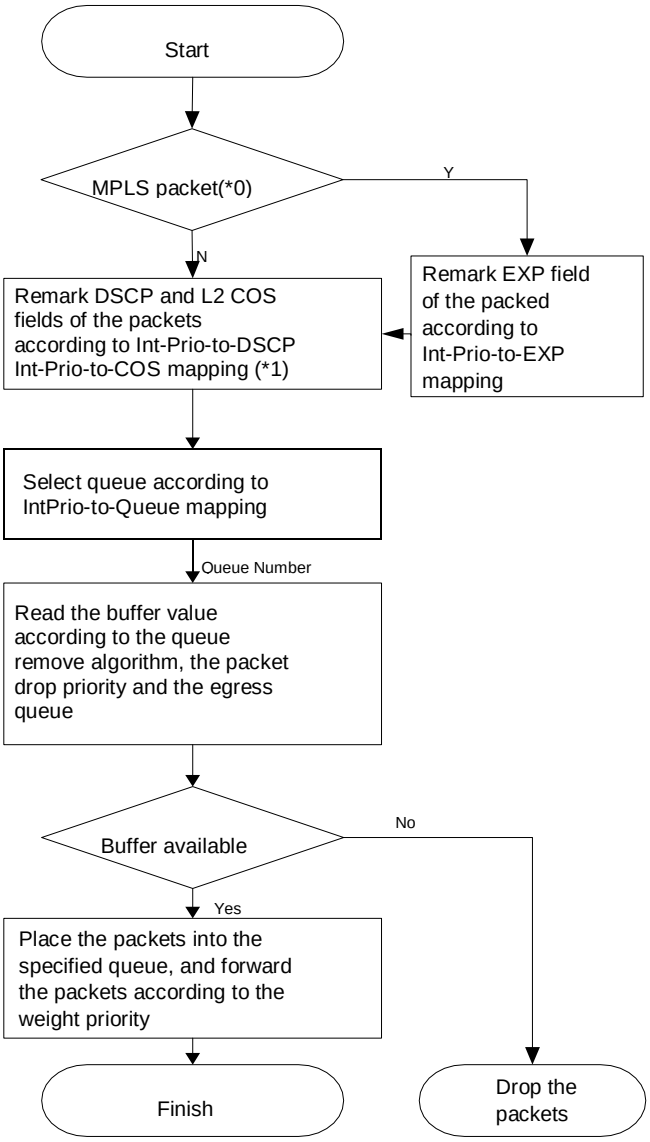


Рисунок 18-6. Процессы планировки и управления очередями

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.

классов, созданной ранее и входом в режим класса. Тогда различные политики (такие как ограничение полосы, понижение приоритета назначением нового значения DSCP) могут применяться для различных 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-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

Команда	Описание
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 <bits_per_second> <normal_burst_bytes> ({conform-action ACTION | exceed-action ACTION}) ACTION definition: drop | transmit | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | set-cos-transmit <cos_value> | set-internal-priority <inp_value> | set-Drop-Precedence <dp_value> 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

Команда	Описание
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 | wdrr} no mls qos queue algorithm	Установка алгоритма управления очередями. По умолчанию алгоритм — wdrr
Общий режим	
mls qos queue 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 VLAN'e.

Команда	Описание
Режим администратора	
clear mls qos statistics [interface <interface-name> | vlan <vlan-id>]	Очистка счетчиков данных в карте политик на определенном порту или VLAN'e. 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 1/1 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 weight 1 1 2 2 4 4 8 8
Switch(Config-If-Ethernet 1/1)#mls qos trust cos
Switch(Config-If-Ethernet1/1)#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 1/1 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 1/2 необходимо установить полосу для пакетов из сегмента 192.168.1.0 в 10 Мбит/с с дополнительной полосой в 4 Мбит. 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-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#policy 10000 4000 exceed-action drop
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#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 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 1/2. После того, как вышеуказанные настройки сделаны, полоса для пакетов из сегмента 192.168.1.0, проходящих через порт Ethernet 1/2, установлена в 10 Мбит/с с дополнительным расширением в 4 Мбит. Все пакеты, превышающие данные установки в данном сегменте, будут сброшены.

Пример 3:

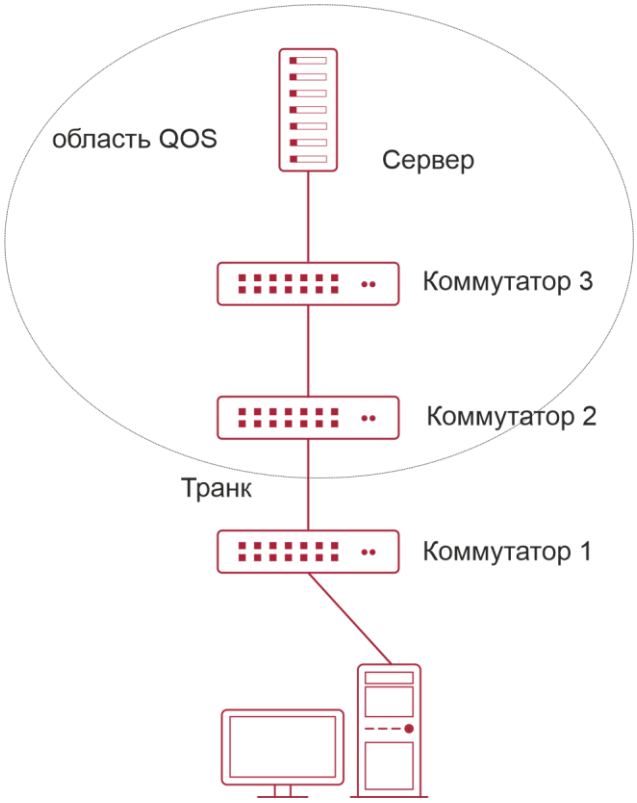


Рисунок 18-7. Типовая топология QoS

Как показано на рисунке, внутри области, отмеченной пунктиром находится QoS домен, Switch1 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 ethernet1/1 (установим внутренний приоритет равным 40 и по умолчанию трансляцию внутреннего приоритета в dcsp как 40-40, соответствующий IP-приоритет равным 5). Порт, подключенный к Switch2 – транковый. На Switch2 порт Ethernet 1/1, подключенный к Switch1 настроен как доверительный dscp. Таким образом внутри области QoS пакеты с различными приоритетами будут распределяться в различные очереди и получат различную полосу передачи.

Этапы конфигурации описаны ниже:

Конфигурация QoS на Switch1:

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)#exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 40
```

```
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#service-policy input p1
```

Конфигурация QoS на Switch2:

```
Switch#config
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#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 настояшее 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

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 1/1
Switch(Config-If-Ethernet1/1)# access-group 1 redirect to interface ethernet 1/6
```

19.3. 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 1000 МБ.

20. КОНФИГУРИРОВАНИЕ ГИБКОГО QINQ

20.1. Общие сведения о гибком 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 обеспечения простого туннеля 2-го уровня пользователям. 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: базовый QinQ и гибкий QinQ. Приоритет гибкого QinQ выше, чем базового.

20.1.2. Базовый QinQ

Базовый 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 гибкий.

20.1.3. Гибкий QinQ

Гибкий 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 гибкого 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 гибкого QinQ

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

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

1. Создать карту классов для классификации различных потоков данных.

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

Команда	Описание
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 гибкого 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-mapname>] 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
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

3. Показывает привязку карты политик гибкого QinQ к порту.

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

20.3. Пример применения гибкого QinQ

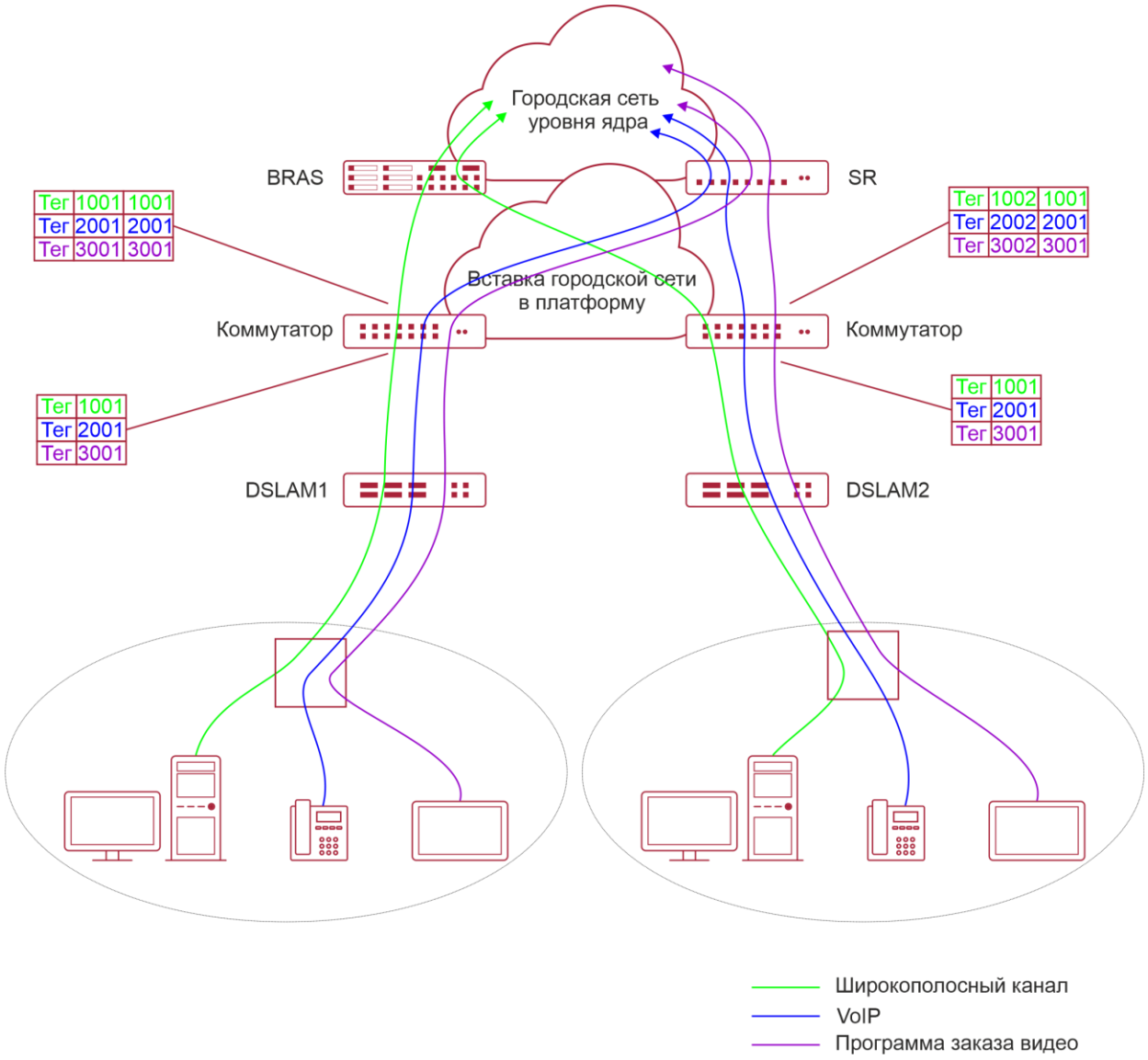


Рисунок 20-1. Топология применения гибкого QinQ

Как показано на рисунке, первый пользователь использует три VLAN'а с метками 1001, 2001, 3001 соответственно на DSLAM1. VLAN1001 соответствует широковещательной сети, VLAN2001 соответствует VOIP, VLAN3001 соответствует VOD. На соответствующем порту сети, имеющем функцию QinQ, пакеты будут формироваться с разными внешними метками в соответствии с VLAN ID пользователя. Пакет с меткой 1001 будет паковаться во внешнюю метку 1001 непосредственно (эта метка уникальна на данной сети), получит метку «широковещательная сеть – VLAN1001» и классифицирована на устройстве BRAS (центр хранения конфигурации). Пакеты с метками 2001 (или 3001) будут паковаться с 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.

Конфигурация следующая:

Если поток данных DSLAM1 идет через порт1 коммутатора, 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 коммутатора, 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-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 гибкого QinQ

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

- Проверьте, поддерживается ли гибкий 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 состоянии UP) – 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 Интернета. Однако по мере роста инфраструктуры Интернета 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 версии4 (IPv4). IPv6 был разработан специально для того, чтобы ликвидировать нехватку адресов IPv4, препятствующую дальнейшему развитию Интернета.

Наиболее важная проблема, которая решена вIPv6 – это добавление достаточного количества IP-адресов. Запас адресов IPv4 почти исчерпан, в то время как число пользователей Интернета 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 внутреннего шлюза (Internal Gateway Protocols — IGP) и протоколов внешнего шлюза (Exterior Gateway Protocols – EGP). 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 default-gateway <A.B.C.D> no ip default-gateway <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.
   1.1. Настройка адреса IPv6-интерфейса.
   1.2. Настройка статической маршрутизации IPv6.
2. Настройка IPv6 Neighbor Discovery.
   2.1. Настройка количества сообщений DAD neighbor solicitation.
   2.2. Настройка интервала отправки сообщений neighbor solicitation.
   2.3. Настройка статических записей IPv6-соседей (neighbor).
   2.4. Удаление всех записей в таблице соседей IPv6.

1. Базовая настройка IPv6.
   1.1. 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

1.2. 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.

2.1. 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)

2.2. 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).

2.3. Настройка статических записей IPv6-соседей (neighbor).

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

2.4. 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

ARARP (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:

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

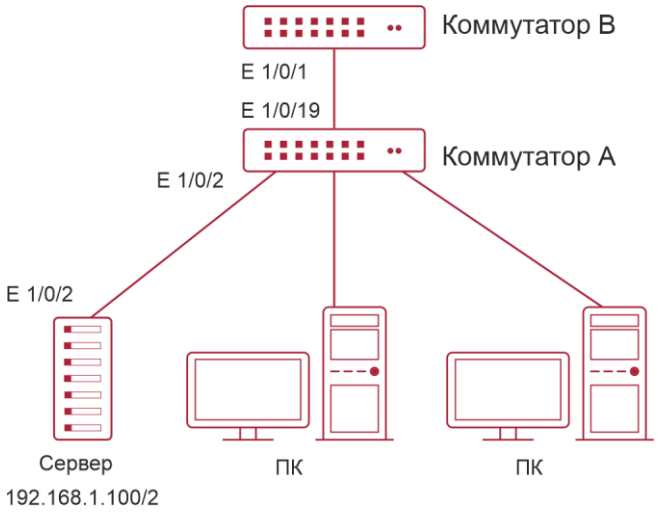


Рисунок 22-1. Типовой пример конфигурации предотвращения ARP-сканирования

В сети, топология которой показана выше, порт E1/1 коммутатора B подключен к порту E1/19 коммутатора A, порт E1/2 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 ethernet1/2
SwitchA (Config-If-Ethernet1/2)#anti-arpscan trust port
SwitchA (Config-If-Ethernet1/2)#exit
SwitchA(config)#interface ethernet1/19
SwitchA (Config-If-Ethernet1/19)#anti-arpscan trust supertrust-port
Switch A(Config-If-Ethernet1/19)#exit
```

Последовательность настройки коммутатора B:

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

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 00-1F-CE-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 динамические ARP на статические

23.3. Пример предотвращения подмены ARP, ND

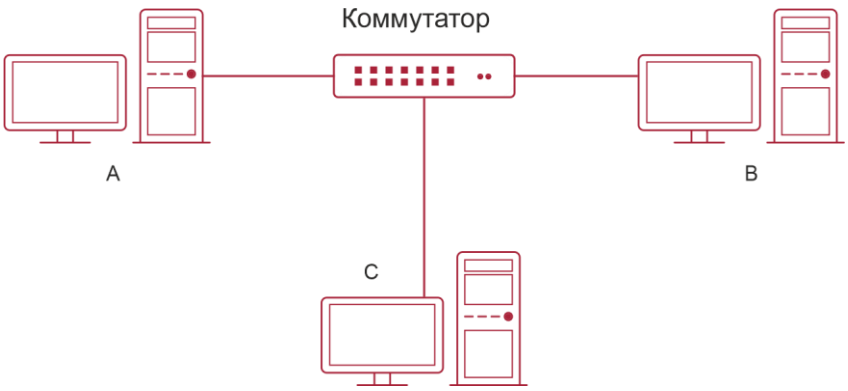


Рисунок 23-1. Описание оборудования

Оборудование	Конфигурация	Кол-во
switch	IP:192.168.2.4;mac: 00-00-00-00-00-04	1
A	IP:192.168.2.1;mac: 00-00-00-00-00-01	1
B	IP:192.168.1.2;mac: 00-00-00-00-00-02	1
C	IP:192.168.2.3;mac: 00-00-00-00-00-03	несколько

На диаграмме показана нормальная связь между B и C. Хост A хочет, чтобы коммутатор направлял ему пакеты, отправленные хостом B. В первую очередь A отправляет пакет ARP-ответа на коммутатор в формате: 192.168.2.3, 00-00-00-00-00-01, сопоставляя его MAC-адрес с IP-адресом хоста C, коммутатор обновляет ARP-список и начинает отправлять пакеты для 192.168.2.3 на MAC-адрес 00-00-00-00-00-01 address (адрес хоста A).

В дальнейшем хост A пересылает принятые пакеты хосту C, 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 00-00-00-00-00-01 interface eth 1/2
Switch(Config-If-Vlan1)#interface vlan 2
Switch(Config-If-Vlan2)#arp 192.168.1.2 00-00-00-00-00-02 interface eth 1/2
Switch(Config-If-Vlan2#interface vlan 3
Switch(Config-If-Vlan3)#arp 192.168.2.3 00-00-00-00-00-03 interface eth 1/2
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.

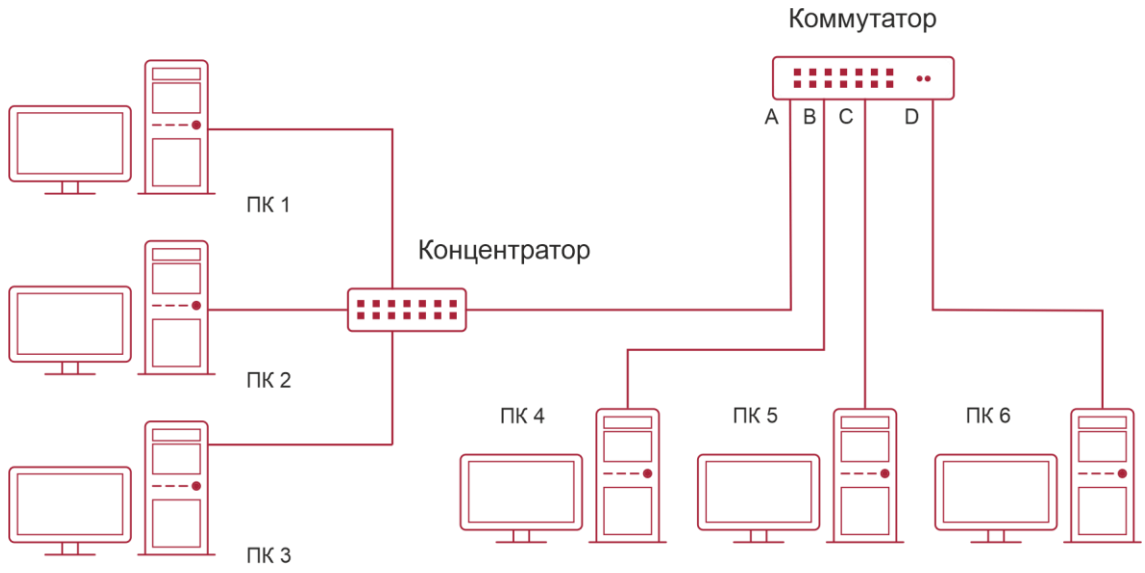


Рисунок 24-1. Схематичная диаграмма ARP GUARD

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 схемы 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.

Базовый режим работы коммутаторов QTECH 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

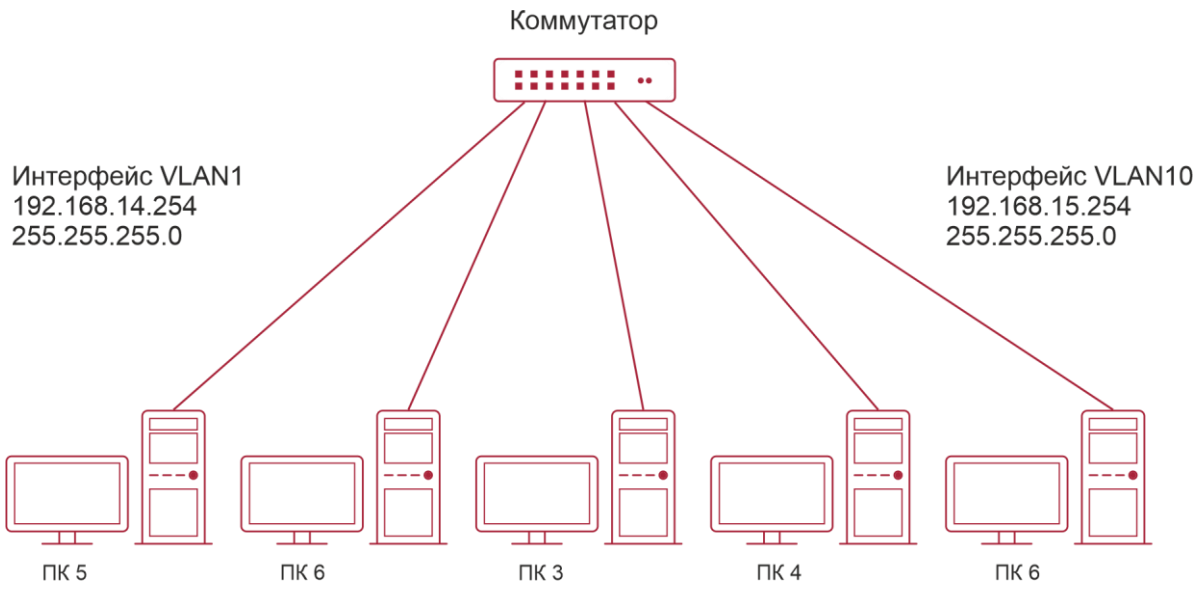


Рисунок 25-1. Пример настройки самообращенного ARP

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 также 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:

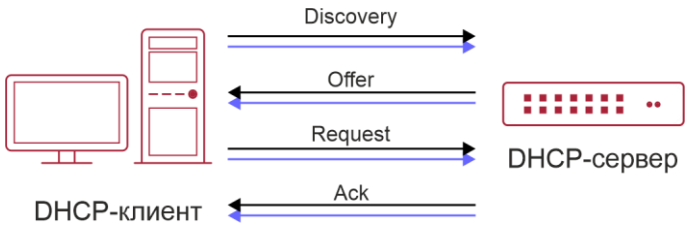


Рисунок 26-1. Взаимодействие протокола DHCP

Разъяснение:

DHCP-клиент рассылает в локальную подсеть широковещательные пакты DHCPDISCOVER.

DHCP-сервер при получении пакета DHCPDISCOVER отправляет DHCP-клиент 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 также 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.
   2.1. Создать/удалить адресный пул DHCP.
   2.2. Настроить параметры адресного пула DHCP.
   2.3. 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.
   2.1. 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

2.2. 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 [<address1>[<address2>[…<address8>]]] no default-router	Настройка шлюза по умолчанию для DHCP-клиентов. Команда no отменяет шлюз по умолчанию
dns-server [<address1>[<address2>[…<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 [<address1>[<address2>[…<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 [<address1>[<address2>[…<address8>]]] no next-server [<address1>[<address2>[…<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

Команда	Описание
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

2.3. 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.

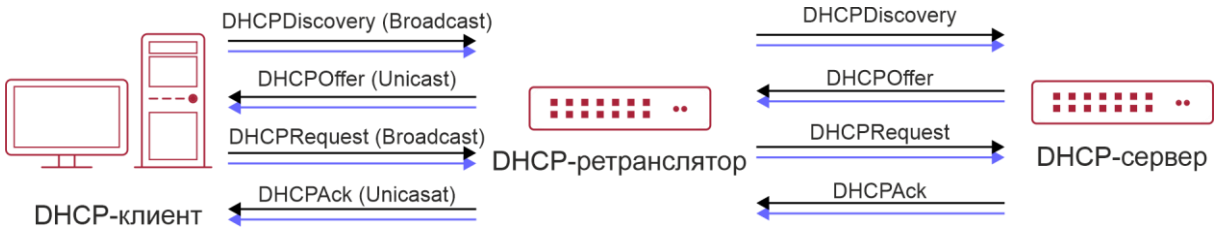


Рисунок 26-2. DHCP-ретранслятор

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

Пул A (сеть 10.16.1.0)		Пул B (сеть 10.16.2.0)	
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 00-03-22-23-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 00-03-22-23-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:

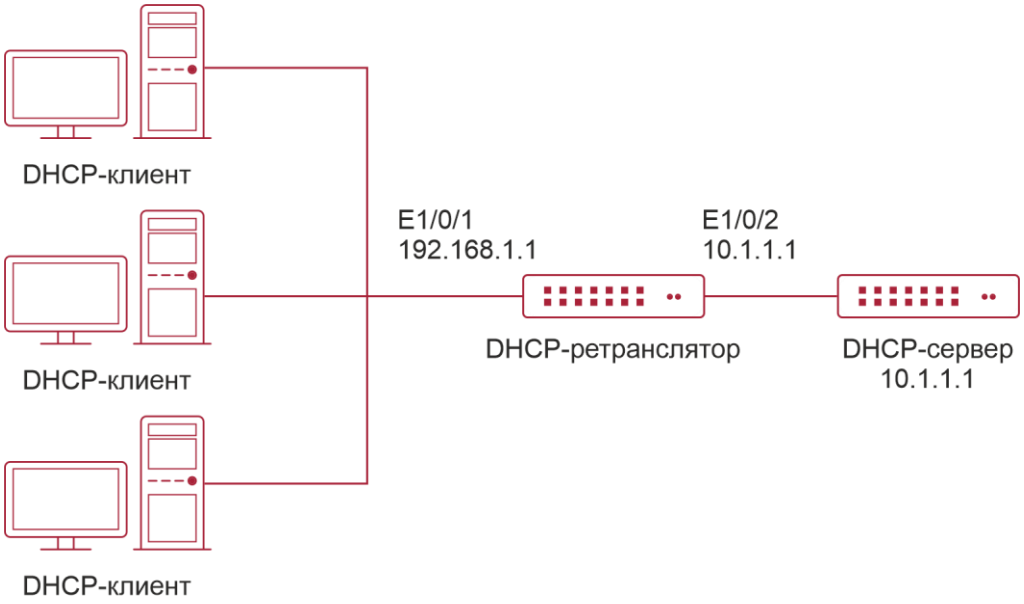


Рисунок 26-3. Конфигурация DHCP-ретранслятора

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 1/2
Switch(Config-Erthernet1/2)#switchport access vlan 2
Switch(Config-Erthernet1/2)#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.

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. Ethernet1/2 является портом доступа, включенным в VLAN3, Ethernet1/3 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 1/2
Switch(Config-If-Ethernet1/2)#switchport access vlan 3
switch(config)#interface ethernet 1/3
Switch(Config-If-Ethernet1/2)#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.

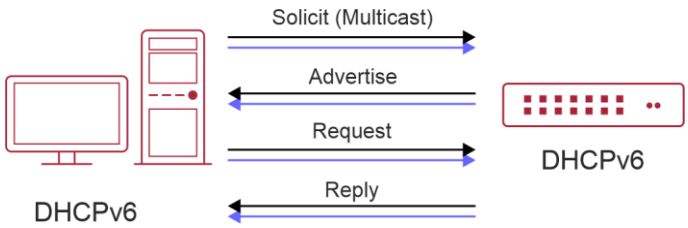


Рисунок 27-1. Согласование DHCPv6

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.
   2.1. Создать/удалить адресный пул DHCPv6.
   2.2. 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.
   2.1. Создать/удалить адресный пул DHCPv6.

Команда	Описание
Общий режим	
ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>	Создать/удалить адресный пул DHCPv6

2.2. 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

Список задач конфигурации DHCPv6-ретранслятора:

1. Включить/выключить сервис DHCPv6.
2. 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.
   3.1. Создать/удалить адресный пул DHCPv6.
   3.2. Настроить пул делегации префиксов, используемый адресным пулом.
   3.3. Настроить статическую привязку делегации префиксов.
   3.4. 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.

3.1. Создать/удалить адресный пул DHCPv6.

Команда	Описание
Общий режим	
ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>	Создать/удалить адресный пул DHCPv6

3.2. 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

3.3. 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

3.4. 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 QTECH 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 Windows Vista, в которой есть DHCPv6-клиент.

Конфигурация коммутатора 3:

```
Switch3>enable Switch3#config
Switch3(config)#service dhcpv6
Switch3(config)#ipv6 dhcp pool EastDormPool
Switch3(dhcpv6-EastDormPool-config)#network-address 2001:da8:100:1::1
2001:da8:100:1::100
Switch3(dhcpv6-EastDormPool-config)#excluded-address 2001:da8:100:1::1
Switch3(dhcpv6-EastDormPool-config)#dns-server 2001:da8::20
Switch3(dhcpv6-EastDormPool-config)#dns-server 2001:da8::21
Switch3(dhcpv6-EastDormPool-config)#domain-name dhcpv6.com
Switch3(dhcpv6-EastDormPool-config)#lifetime 1000 600
Switch3(dhcpv6-EastDormPool-config)#exit
Switch3(config)#interface vlan 1
Switch3(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::1/64
Switch3(Config-if-Vlan1)#exit
Switch3(config)#interface vlan 10
Switch3(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::1/64
Switch3(Config-if-Vlan10)#ipv6 dhcp server EastDormPool preference 80
Switch3(Config-if-Vlan10)#exit
```

```
Switch3(config)#
```

Конфигурация коммутатора 3:

```
Switch2>enable Switch2#config
Switch2(config)#service dhcpv6
Switch2(config)#interface vlan 1
Switch2(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::2/64
Switch2(Config-if-Vlan1)#exit
Switch2(config)#interface vlan 10
Switch2(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::2/64
Switch2(Config-if-Vlan10)#exit
Switch2(config)#interface vlan 100
Switch2(Config-if-Vlan100)#ipv6 address 2001:da8:100:1::1/64
Switch2(Config-if-Vlan100)#no ipv6 nd suppress-ra
Switch2(Config-if-Vlan100)#ipv6 nd managed-config-flag
Switch2(Config-if-Vlan100)#ipv6 nd other-config-flag
Switch2(Config-if-Vlan100)#ipv6 dhcp relay destination 2001:da8:10:1::1
Switch2(Config-if-Vlan100)#exit
Switch2(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'a, 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.

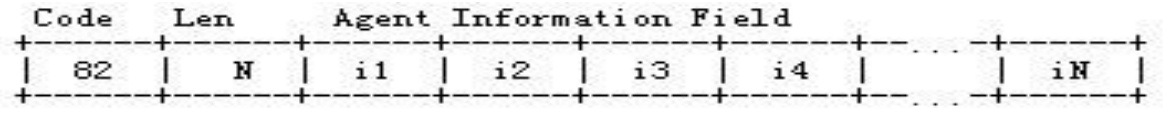
28. КОНФИГУРАЦИЯ ОПЦИИ 82 DHCP

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

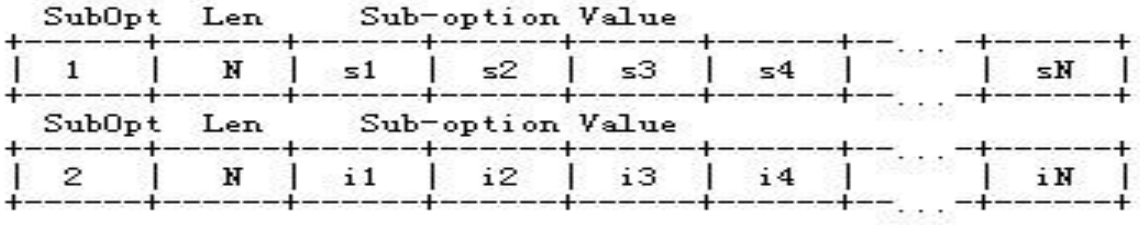
Сообщение DHCP может иметь несколько сегментов опций, опция 82 один из них. Она должна быть после других опций, но до опции 255. Вот ее формат:



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

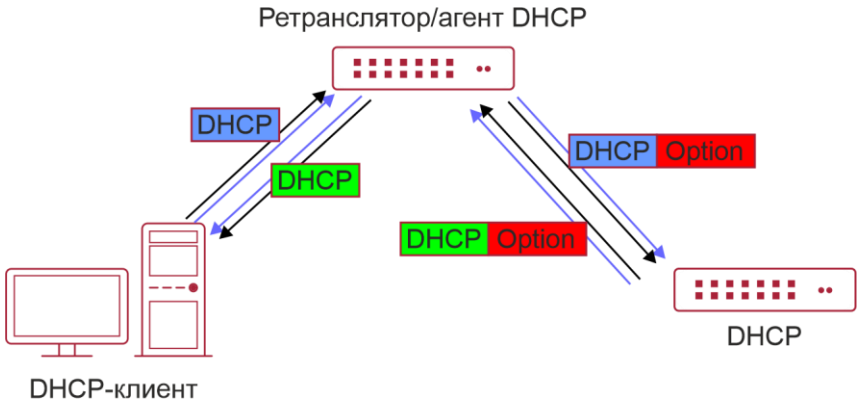


Рисунок 28-1. Диаграмма потоков опции 82 DHCP

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} no ip dhcp relay information option self-defined remote-id	Устанавливает медот создания опции 82, пользователи могут 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

Команда	Описание
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

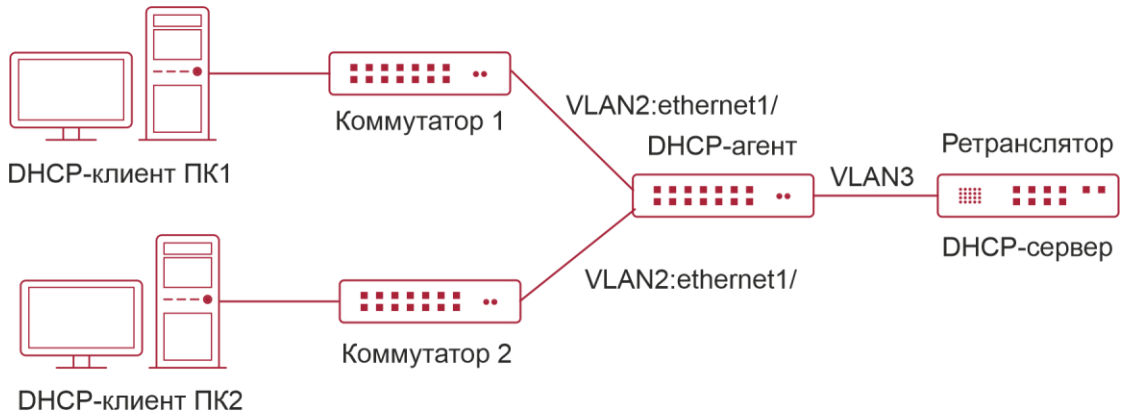


Рисунок 28-2. Типовой пример применения опции 82 DHCP

В данной схеме оба коммутатора второго уровня (1 и 2) подключены к коммутатору третьего уровня (3), 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 коммутаторам 1 и 2, 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 (коммутатор 1 или коммутатор 2) и, таким образом, сможет выделять разное адресное пространство двум подсетям, чтобы упростить управление сетью.

Конфигурация комутатора 3 (MAC-адрес 00:1f:ce:02:33:01):

```
Switch3(Config)#service dhcp
Switch3(Config)#ip dhcp relay information option
Switch3(Config)#ip forward-protocol udp bootps
Switch3(Config)#interface vlan 3
Switch3(Config-if-vlan3)#ip address 192.168.10.222 255.255.255.0
Switch3(Config-if-vlan2)#ip address 192.168.102.2 255.255.255.0
Switch3(Config-if-vlan2)#ip helper 192.168.10.88
```

Linux ISC DHCP-сервер поддерживает опцию 82, его конфигурационный файл /etc/dhcpd.conf:

```
ddns-update-style interim;
ignore client-updates;

class "Switch3Vlan2Class1" {
match if option agent.circuit-id = "Vlan2+Ethernet1/0/2" and option agent.remote-id=00:1f:ce:02:33:01;
}
class "Switch3Vlan2Class2" {
match if option agent.circuit-id = "Vlan2+Ethernet1/0/3" and option agent.remote-id=00:1f:ce:02:33:01;
}
subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name "example.com.cn";
option domain-name-servers 192.168.10.3;
authoritative;

pool {
range 192.168.102.21 192.168.102.50;
default-lease-time 86400; #24 Hours
max-lease-time 172800; #48 Hours
allow members of "Switch3Vlan2Class1";
}
pool {
range 192.168.102.51 192.168.102.80;
```

```
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch3Vlan2Class2";
}
}
```

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

Команда	Описание
no option 43	Удаление настроек опции 43 в режиме адресного пространства

29.3. Пример настройки опций 60 и 43 DHCPv6

Рисунок 29-1.

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	Описание
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

Команда	Описание
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 |) no ipv6 dhcp snooping 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 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

Команда	Описание
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+Ethernet1/2"

2. Конфигурация базовых опций DHCPv6-ретранслятора.

Команда	Описание
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-го 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

Команда	Описание
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+Ethernet1/2"

3. Конфигурация базовых опций DHCPv6-сервера.

Команда	Описание
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-forw no ipv6 dhcp server select relay-forw	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

Команда	Описание
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
Режти конфигурации пула адресов DHCPv6	
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 опиций 37, 38 DHCPv6

30.3.1. Пример опций 37, 38 в DHCPv6 Snooping

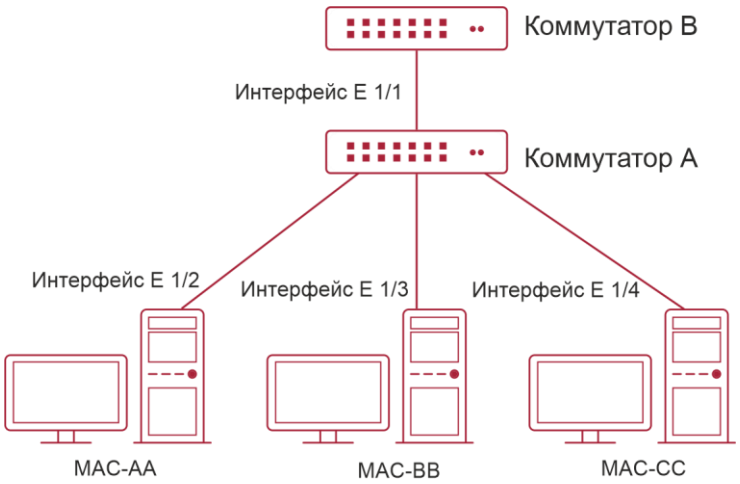


Рисунок 30-1. Схема опций в DHCPv6 Snooping

Согласно схеме Mac-AA, Mac-BB и Mac-CC – обычные пользователи, подключенные к недоверенным интерфейсам 1/2, 1/3 и ¼ соответственно. Они получают IP-адреса 2010:2, 2010:3 и 2010:4 по DHCPv6; DHCPv6-сервер подключен к доверенному интерфейсу 1/1. Настроено три политики выделения адресов (классов), CLASS1 соответствует опции 38, CLASS2 соответствует опции 37, а CLASS3 – опциям 37 и 38. В пуле адресов EastDormPool запросам, соответствующим классам CLASS1, CLASS2 и CLASS3 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 коммутатора A:

```
SwitchA(config)#ipv6 dhcp snooping remote-id option
SwitchA(config)#ipv6 dhcp snooping subscriber-id option
SwitchA(config)#int e 1/1
SwitchA(config-if-ethernet1/1)#ipv6 dhcp snooping trust
SwitchA(config-if-ethernet1/1)#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 1/1-4
SwitchA(config-if-port-range)#switchport access vlan 1
SwitchA(config-if-port-range)#exit
SwitchA(config)#
```

Конфигурация коммутатора B:

```
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 CLASS1
SwitchB(dhcpv6-class-class1-config)#remote-id 00-1f-ce-00-00-01 subscriber-id
vlan1+Ethernet1/1
SwitchB(dhcpv6-class-class1-config)#exit
SwitchB(config)#ipv6 dhcp class CLASS2
SwitchB(dhcpv6-class-class2-config)#remote-id 00-1f-ce-00-00-01 subscriber-id
vlan1+Ethernet1/2
SwitchB(dhcpv6-class-class2-config)#exit
SwitchB(config)#ipv6 dhcp class CLASS3
```

```
SwitchB(dhcpv6-class-class3-config)#remote-id 00-1f-ce-00-00-01 subscriber-id
vlan1+Ethernet1/3
SwitchB(dhcpv6-class-class3-config)#exit
SwitchB(config)#ipv6 dhcp pool EastDormPool
SwitchB(dhcpv6-eastdormpool-config)#class CLASS1
SwitchB(dhcpv6-pool-eastdormpool-class-class1-config)#address range
2001:da8:100:1::3 2001:da8:100:1::30
SwitchB(dhcpv6-pool-eastdormpool-class-class1-config)#exit
SwitchB(dhcpv6-eastdormpool-config)#class CLASS2
SwitchB(dhcpv6-pool-eastdormpool-class-class2-config)#address range
2001:da8:100:1::31 2001:da8:100:1::60
SwitchB(dhcpv6-eastdormpool-config)#class CLASS3
SwitchB(dhcpv6-pool-eastdormpool-class-class3-config)#address range
2001:da8:100:1::61 2001:da8:100:1::100
SwitchB(dhcpv6-pool-eastdormpool-class-class3-config)#exit
SwitchB(dhcpv6-eastdormpool-config)#exit
SwitchB(config)#interface vlan 1
SwitchB(config-if-vlan1)#ipv6 address 2001:da8:100:1::2/64
SwitchB(config-if-vlan1)#ipv6 dhcp server 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).

Топология сети:

На уровне доступа используется коммутатор 1 для подключения пользователей общежития; на первом уровне аггрегации коммутатор 2 настроен как DHCPv6-ретранслятор; на втором уровне аггрегации коммутатор 3 настроен как DHCPv6-сервер и соединен с магистральной сетью. На компьютерах должна быть установлена ОС Windows Vista, в которой есть DHCPv6-клиент.

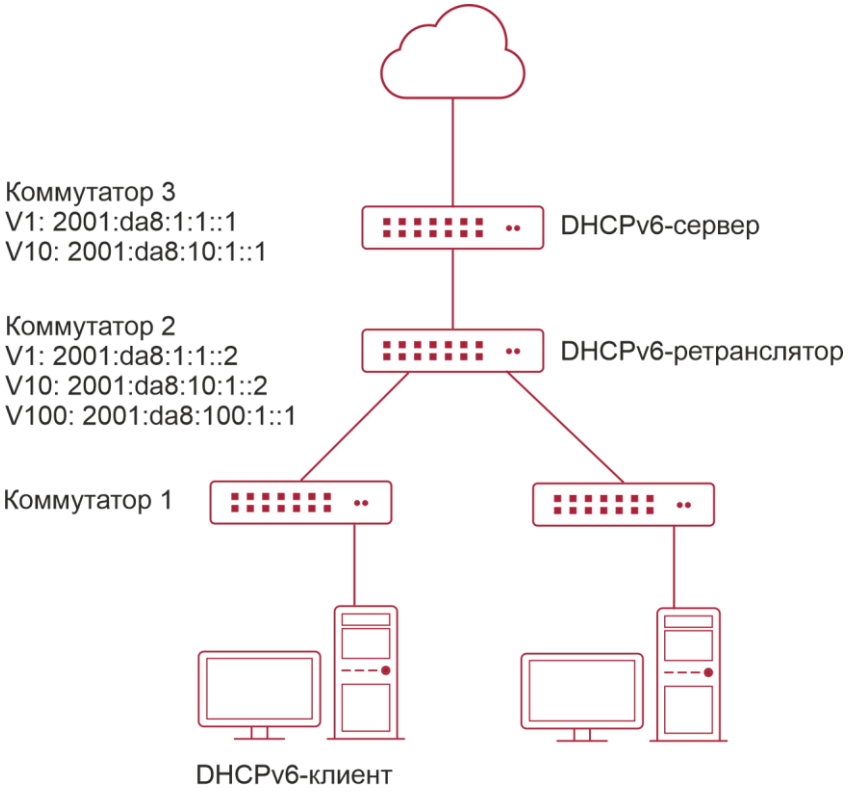


Рисунок 30-2. Схема применения опций в DHCPv6-ретрансляторе

Конфигурация коммутатора 2:

```
S2(config)#service dhcpv6
S2(config)#ipv6 dhcp relay remote-id option
S2(config)#ipv6 dhcp relay subscriber-id option
S2(config)#vlan 10
S2(config-vlan10)#int vlan 10
S2(config-if-vlan10)#ipv6 address 2001:da8:1:::2/64
S2(config-if-vlan10)#ipv6 dhcp relay destination 2001:da8:10:1::1
S2(config-if-vlan10)#exit
S2(config)#
```

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 «черной дыры».

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 «черной дыры»).

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 связующих данных DHCP: DHCP snooping при пересылке DHCP-пакетов будет записывать связующие данные, выделенные DHCP-сервером. Можно так же загрузить эти данные на сервер в целях восстановления утерянной информации. Связующие данные, 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 «черной дыры», 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 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 no ip dhcp snooping trust	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> <mask> 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}	Устанавливает формат subscriber-id опции 82 DHCP snooping
ip dhcp snooping information option remote- id {standard | <remote-id>} 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

Команда	Описание
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

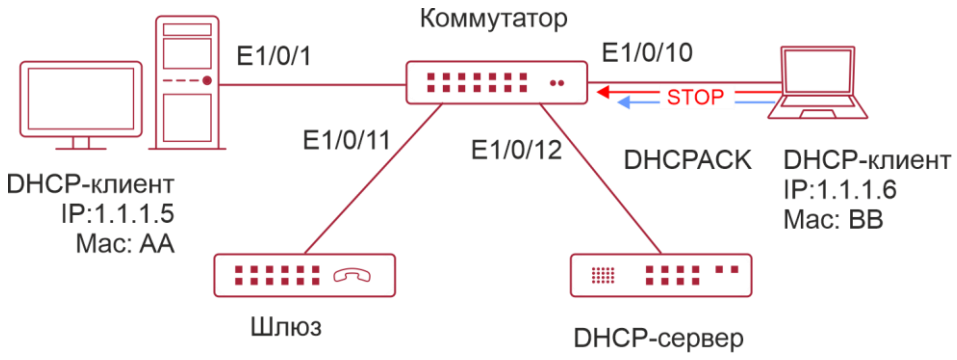


Рисунок 31-1. Типовой применение

Как показано на рисунке, устройство Mac-AA – обычный пользователь, подключенный к недоверенному порту 1/1 коммутатора, получает IP-настройки через DHCP, IP-адрес клиента 1.1.1.5. DHCP-сервер и шлюз подключены к доверенным портам коммутатора, 1/11 и 1/12 соответственно. Злоумышленник Mac-BB, подключенный к недоверенному

порту 1/1 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 1/11
switch(Config-If-Ethernet1/11)#ip dhcp snooping trust
switch(Config-If-Ethernet1/11)#exit
switch(config)#interface ethernet 1/12
switch(Config-If-Ethernet1/12)#ip dhcp snooping trust
switch(Config-If-Ethernet1/12)#exit
switch(config)#interface ethernet 1/1-10
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.

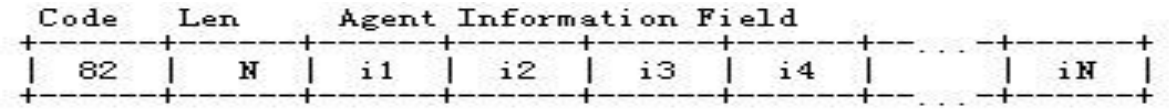
32. КОНФИГУРАЦИЯ ОПЦИИ 82 DHCP

32.1. 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.

32.1.1. Структура сообщения опции 82 DHCP

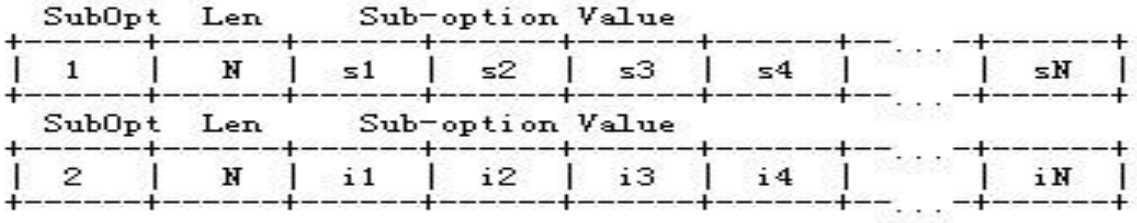
Сообщение DHCP может иметь несколько сегментов опций, опция 82 один из них. Она должна быть после других опций, но до опции 255. Вот ее формат:



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.

32.1.2. Механизм работы опции 82

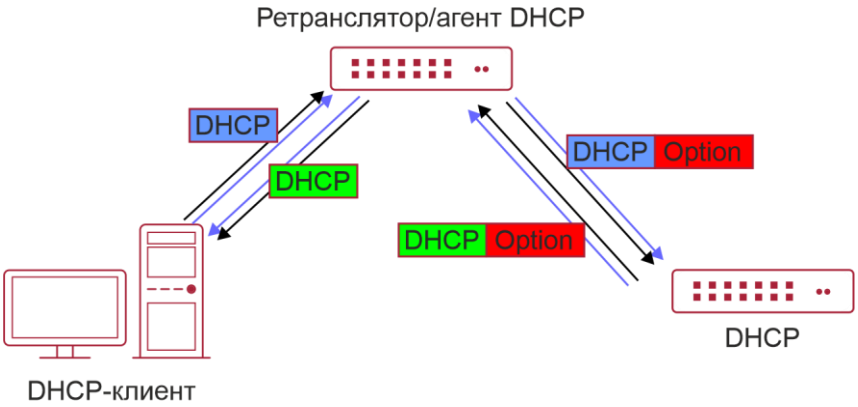


Рисунок 32-1. Диаграмма потоков опции 82 DHCP

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.

32.2. Список задач конфигурации опции 82 DHCP

1. Включить DHCP Snooping.
2. Включить функцию привязки DHCP Snooping.
3. Включить функцию опции 82 DHCP Snooping.
4. Настроить доверенные порты.

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 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

4. Настроить доверенные порты.

Команда	Описание
Режим порта	
ip dhcp snooping trust no ip dhcp snooping trust	Сделать порт доверенным. Команда no отменяет настройку

32.3. Примеры применения опции 82 DHCP

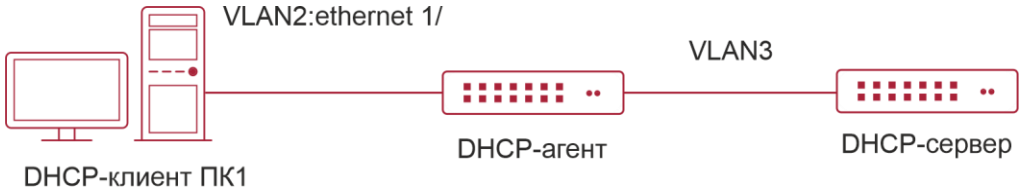


Рисунок 32-2. Типовой пример применения опции 82 DHCP

В данной схеме комутатор второго уровня передает сообщение запроса от DHCP-клиента к серверу через включенный DHCP Snooping. Он так же передаст сообщение ответа от сервера к клиенту для завершения процедуры DHCP-протокола. После включения 82 опции DHCP Snooping, коммутатор добавляет информацию о порте доступа в сообщение запроса от клиента с опцией 82.

Конфигурация комутатора 3 (MAC-адрес 00:1f:ce:02:33:01):

```
Switch3(Config)#service dhcp
Switch3(Config)#ip dhcp relay information option
Switch3(Config)#ip forward-protocol udp bootps
Switch3(Config)#interface vlan 3
Switch3(Config-if-vlan3)#ip address 192.168.10.222 255.255.255.0
Switch3(Config-if-vlan2)#ip address 192.168.102.2 255.255.255.0
Switch3(Config-if-vlan2)#ip helper 192.168.10.88
}
```

Linux ISC DHCP-сервер поддерживает опцию 82, его конфигурационный файл /etc/dhcpd.conf:

```
ddns-update-style interim;
ignore client-updates;

class "Switch3Vlan2Class1" {
match if option agent.circuit-id = "Vlan2+Ethernet1/2" and option
agent.remote-id=00:1f:ce:02:33:01;
}
class "Switch3Vlan2Class2" {
match if option agent.circuit-id = "Vlan2+Ethernet1/3" and option
agent.remote-id=00:1f:ce:02:33:01;
}
subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name "example.com.cn";
option domain-name-servers 192.168.10.3;
authoritative;

pool {
range 192.168.102.21 192.168.102.50;
default-lease-time 86400; #24 Hours
max-lease-time 172800; #48 Hours
allow members of "Switch3Vlan2Class1";
```

```
}
pool {
range 192.168.102.51 192.168.102.80;
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch3Vlan2Class2";
}
}
```

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.

32.4. 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.

33. НАСТРОЙКА ЭНЕРГОСБЕРЕЖЕНИЯ EEE

33.1. Введение в энергосбережение EEE

EEE означает «Энергоэффективная сеть Ethernet». После включения данной функции коммутатор будет автоматически определять состояние порта. Если порт свободен и передача данных отсутствует, этот порт перейдет в режим экономии электроэнергии и коммутатор ограничит его питание.

33.2. Список настроек энергосбережения EEE

33.2.1. Включить функцию энергосбережения EEE

Команда	Описание
Режим конфигурирования порта	
eee enable no eee enable	Включает функцию энергосбережения порта; команда «no» выключает функцию энергосбережения порта

33.3. Типичные примеры энергосбережения EEE

Пример. Перевести порт 1 коммутатора в режим экономии электроэнергии.

Ниже приведены этапы настройки:

```
Switch(config-if-ethernet1/0/1)# eee enable
```

34. ПРОТОКОЛ МНОГОАДРЕСНОЙ МАРШРУТИЗАЦИИ (MULTICAST) IPV4

34.1. Общая информация о протоколе многоадресной маршрутизации IPv4

В этой главе приводятся краткие сведения о настройке протокола многоадресной маршрутизации IPv4.

34.1.1. Введение в многоадресную рассылку

Когда пунктом назначения передачи пакетов (в т. ч. данных, звука и видео) является небольшая группа пользователей в сети, можно применять различные режимы передачи. Можно использовать одноадресный режим, т. е. настроить отдельный тракт передачи данных для каждого пользователя. Кроме того, можно использовать режим широковещания, который предполагает рассылку сообщений всем пользователям в сети, независимо от того, нужны им эти сообщения или нет. Например, если в сети находится 200 пользователей, которым нужно получить один и тот же пакет, традиционное решение – отправить этот пакет в одноадресном режиме 200 раз. Таким образом, все пользователи, которым требуются эти данные, их получают. Другое решение – отправить данные всему домену в режиме широковещания. При передаче данных по всей сети пользователи, которым нужны эти данные, могут получить их непосредственно из сети. В любом из этих режимов без меры тратится ценный ресурс пропускной способности, и, кроме того, при использовании режима широковещания нарушаются безопасность и конфиденциальность.

Эту проблему решило своевременное появление технологии многоадресной IP-маршрутизации. Многоадресный источник отправляет сообщение только один раз, а протокол многоадресной маршрутизации настраивает дерево маршрутизации для многоадресных пакетов данных, после чего начинается дублирование и распространение передаваемого пакета как можно дальше по разветвленной сети. Таким образом, становится возможной точная и эффективная отправка пакета всем пользователям, которым он нужен.

Следует отметить, что многоадресному источнику подключаться к многоадресной группе необязательно. Он отправляет данные некоторым многоадресным группам, но сам при этом необязательно является получателем. Отправлять пакеты многоадресной группе могут одновременно несколько источников. В сети могут находиться маршрутизаторы, не поддерживающие многоадресную передачу. Однако многоадресный маршрутизатор может инкапсулировать многоадресные пакеты в одноадресные IP-пакеты для передачи их в туннельном режиме соседнему многоадресному маршрутизатору, который удалит одноадресный заголовок и продолжит процесс многоадресной передачи. Таким образом, удается избежать глобальной модификации структуры сети. Ниже перечислены основные преимущества многоадресной рассылки:

1. Повышенная производительность: уменьшение сетевого трафика, снижение нагрузок на сервер и ЦПУ.
2. Оптимизация производительности: сокращение лишнего трафика.
3. Распределенное применение: возможность многоточечного применения.

34.1.2. Адрес групповой передачи

Пунктам назначения многоадресного сообщения присваиваются IP-адреса класса D в диапазоне от 224.0.0.0 до 239.255.255.255. Адрес класса D не может появиться в поле IP-адреса источника IP-сообщения. При одноадресной рассылке тракт передачи пакета

данных прокладывается от адреса источника к адресу пункта назначения, а передача данных осуществляется по принципу «от узла к узлу». Однако при многоадресной маршрутизации адреса пунктов назначения – это группа, а не отдельный адрес. Вместе они образуют групповой адрес. Каждый получатель сообщения подключается к группе. Сразу после этого поток данных, передаваемых на групповой адрес, рассылается получателям, и все участники группы принимают пакеты данных. Участники многоадресной группы являются динамическими, т. е. узлы могут в любое время присоединяться к многоадресной группе и выходить из нее.

Многоадресная группа может быть как постоянной, так и временной. Некоторые групповые адреса назначаются официально: они носят название постоянной многоадресной группы. IP-адрес такой группы зафиксирован, но ее внутренняя структура может изменяться. Число участников постоянной многоадресной группы произвольно, участников может не быть вообще. IP-адреса групповой передачи, не зарезервированные для постоянной многоадресной группы, могут использоваться временными многоадресными группами.

224.0.0.0 — 224.0.0.255 – зарезервированные адреса многоадресной рассылки (адрес постоянной группы); адрес 224.0.0.0 зарезервирован, но не назначается, остальные адреса используются протоколом маршрутизации. 224.0.1.0 — 238.255.255.255 – адреса групповой передачи, доступные пользователям (адрес временной группы), и действуют во всем сетевом домене. 239.0.0.0 — 239.255.255.255 – адреса групповой передачи локального управления, действующие только в конкретном локальном домене. Ниже приведен список часто используемых зарезервированных адресов групповой передачи:

Базовый адрес (зарезервирован)

224.0.0.1 Адрес всех узлов

224.0.0.2 Адрес всех многоадресных маршрутизаторов

224.0.0.3 Не назначен

224.0.0.4 Маршрутизатор DVMRP

224.0.0.5 Маршрутизатор OSPF

224.0.0.6 OSPF DR

224.0.0.7 Маршрутизатор ST

224.0.0.8 Узел ST

224.0.0.9 Маршрутизатор RIP-2

224.0.0.10 Маршрутизатор IGRP

224.0.0.11 Мобильный агент

224.0.0.12 Агент сервера/ретрансляции DHCP

224.0.0.13 Все PIM-маршрутизаторы

224.0.0.14 Протокол RSVP Encapsulation

224.0.0.15 Все CBT-маршрутизаторы

224.0.0.16 Выделенный экземпляр SBM

224.0.0.17 Все SBM

224.0.0.18 Протокол VRRP

224.0.0.22 Протокол IGMP

При передаче одноадресных IP-сообщений через Ethernet в качестве MAC-адреса пункта назначения используется MAC-адрес получателя. Однако при передаче многоадресных

пакетов пунктом назначения является не конкретный получатель, а группа неопределенных участников, поэтому используется MAC-адрес многоадресной рассылки. Этот адрес соответствует IP-адресу многоадресной рассылки. Согласно IANA (Администрация адресного пространства Интернет), старшие 25 бит в MAC-адресе групповой передачи – 0x01005e, а младшие 23 бита MAC-адреса формируются из младших 23 бит IP-адреса групповой передачи.

Поскольку для формирования MAC-адреса из младших 28 бит IP-адреса групповой передачи используется только 23 бита, одному MAC-адресу соответствует 32 IP-адреса.

34.1.3. Передача многоадресных IP-пакетов

При передаче данных в многоадресном режиме узел-источник отправляет пакеты группе узлов, адрес которой указан в поле адреса пункта назначения IP-пакета данных. Для того чтобы в многоадресном режиме разослать пакет всем получателям, необходимо сначала направить его ряду внешних интерфейсов, чего не требуется в одноадресном режиме. Таким образом, процедура многоадресной передачи сложнее одноадресной.

Для гарантии того, что многоадресные пакеты передаются маршрутизатору кратчайшим путем, необходимо определенным образом (на основе таблицы одноадресной маршрутизации) проверять интерфейс получателя многоадресного пакета. Этот механизм проверки лежит в основе большинства протоколов маршрутизации для передачи в многоадресном режиме – проверка RPF (переадресация в обратном направлении). Для того чтобы определить, является ли путь между получателем и источником, на котором находится входной интерфейс пакета, кратчайшим, многоадресный маршрутизатор выполняет запрос к таблице одноадресной маршрутизации с помощью адреса источника пакета или использует независимую таблицу многоадресной маршрутизации. Если используется дерево кратчайших маршрутов, то адресом источника является адрес узлаисточника, который отправляет многоадресные пакеты данных. Если используется общее дерево, то адресом источника является корень общего дерева. При поступлении на маршрутизатор многоадресный пакет данных направляется согласно правилу групповой передачи, если проверка RPF успешно пройдена, и утилизируется в противном случае.

34.1.4. Применение многоадресной IP-рассылки

С помощью технологии многоадресной IP-маршрутизации была успешно решена проблема передачи данных от одной точки ко многим. Применяя ее, удалось достичь эффективной передачи данных от одной точки ко многим, сэкономить пропускную способность сети и снизить нагрузки на сеть. Групповая передача упрощает выполнение некоторых новых дополнительных операций. Ниже перечислены варианты применения многоадресной рассылки в сфере информационных услуг, включая прямые онлайнтрансляции, сетевое ТВ, дистанционное обучение, дистанционная медицина, видео- и аудиоконференции в режиме реального времени:

1. Мультимедиа и потоковые мультимедиа.
2. Хранилище данных, финансы (фонды) и т. д.
3. Любое приложение по распределению данных «от одной точки ко многим».

В IP-сети выполняется все больше и больше мультимедийных операций, поэтому многоадресная рассылка обладает огромным рыночным потенциалом и будет широко распространяться.

34.2. DCSCM

34.2.1. Введение в технологию DCSCM

Технология DCSCM (многоадресное управление адресатами и источником) состоит из трех основных аспектов: управление источником многоадресного пакета, управление пользователем многоадресной рассылки и сервис-ориентированная стратегия многоадресной рассылки.

Технология управления источником многоадресного пакета, представляющая собой часть технологии управления безопасностью при многоадресной рассылке, как правило, работает следующим образом:

1. Для граничного коммутатора: если настроена многоадресная рассылка с контролируемым источником, пропускаются только многоадресные данные указанной группы от указанного источника.
2. Для RP-коммутатора в ядре протокола PIM-SM: с помощью сообщения REGISTER регистрируется информация от указанного источника и указанной группы, сообщение REGISTER_STOP передается напрямую и запрещает настраивать запись таблицы. (Эта задача встроена в модель PIM-SM.)

Технология управления пользователем многоадресной рассылки, представляющая собой часть технологии управления безопасностью при многоадресной рассылке, реализуется на основе управления сообщениями-отчетами IGMP, которые отправляют пользователи. Таким образом, управляемая модель представляет собой отслеживание IGMP-пакетов. Логика управления модели IGMP состоит из трех частей: получить управление на основе сети VLAN и MAC-адреса передаваемых пакетов, на основе IP-адреса передаваемых пакетов и на основе порта, в который поступают сообщения. Для отслеживания IGMP-пакетов можно одновременно применять все три вышеописанных метода, в то время как модель IGMP расположена на уровне 3 и может получить управление только IP-адресами передаваемых пакетов.

Сервис-ориентированная стратегия многоадресной рассылки, представляющая собой часть технологии управления безопасностью, работает следующим образом. Для многоадресных данных в ограниченном диапазоне устанавливается приоритет, указываемый пользователем на общем конце, благодаря чему данные, обладающие более высоким приоритетом, можно отправлять через магистральный порт. Это гарантирует передачу данных по всей сети в соответствии с указанным пользователем приоритетом.

34.2.2. Список задач по настройке DCSCM

1. Настройка управления источником.
2. Настройка управления пунктом назначения.
3. Настройка стратегии многоадресной рассылки.

34.2.2.1. Настройка управления источником.

Настройка управления источником состоит из трех частей. Первая часть — включить управление источником. Ниже приводится команда управления источником:

Команда	Описание
Режим общих настроек	
[no] ip multicast source-control (Required)	Глобально включает управление источником. Команда «no ip multicast source-control» глобально выключает управление источником. Следует отметить, что по умолчанию все многоадресные пакеты утилизируются после глобального включения управления источником. Настройки управления источником невозможно применить, пока управление источником не включено глобально. В то же время управление источником нельзя отключить, пока работают все заданные правила

Теперь необходимо задать правило управления источником. Оно задается так же, как и для ACL, и применяет номера ACL 5000–5099. Каждый номер можно использовать для настройки 10 правил. Следует отметить, что эти правила упорядочены: первым является правило, заданное раньше остальных. После определения заданных правил последующие правила не смогут вступить в силу, поэтому команды глобальных разрешений следует настраивать в конце. Команды приводятся ниже:

Команда	Описание
Режим общих настроек	
[no] access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}	Правило используется для настройки управления источником. Это правило вступает в силу только после применения его к конкретному порту. Для того чтобы удалить указанное правило, необходимо начать команду со слова «NO»

Осталось применить заданное правило к конкретному порту.

Примечание. Если задаваемых правил окажется слишком много, и они заполнят всю таблицу записей оборудования, произойдет отказ конфигурации, вызванный заполнением нижних записей в таблице. Поэтому по возможности рекомендуется использовать максимально простые правила. Ниже приводятся правила конфигурации:

Команда	Описание
Режим настроек порта	
[no] ip multicast source-control access-group <5000-5099>	Используется для настройки правил, применяемых управлением источником к порту. Если команда начинается со слова «NO», настройки отменяются

34.2.2.2. Настройка управления пунктом назначения

Как и в случае настройки управления источником, чтобы настроить управление пунктом назначения, необходимо выполнить три шага.

Во-первых, следует глобально включить управление пунктом назначения. Поскольку управление пунктом назначения используется для предотвращения отправки многоадресных данных неавторизованным пользователям, после включения данной функции коммутатор не будет рассылать данные в режиме широковещания. Следовательно, следует избегать подключения двух или более коммутаторов уровня 3 в одной и той же сети VLAN к коммутатору, на котором включено управление пунктом назначения. Ниже приводятся команды настройки:

Команда	Описание
Режим общих настроек	
[no] multicast destination-control (required)	Глобально включает управление пунктом назначения. Команда, начинающаяся со слова «no», глобально выключает управление. Все остальные настройки вступают в силу только после глобального включения управления. Теперь необходимо задать однотипные правила управления пунктом назначения

Следующая команда применяется, чтобы настроить список правил для профиля управления пунктом назначения многоадресной рассылки. В качестве идентификационного номера профиля используется число от 1 до 50.

Команда	Описание
Режим общих настроек	
profile-id <1-50> {deny|permit} {{<source/M>}|{host-source <source-host-ip> (range <265535>|)}|any-source} {{<destination/M>}|{hostdestination <destination-host-ip> (range <2-255>|)}|any-destination} no profile-id <1-50>	Задает правило для профиля управления пунктом назначения. Команда, начинающаяся с «no», удаляет его

Теперь следует задать правило управления пунктом назначения. Оно похоже на правило управления источником, но использует номера ACL 6000–7999.

Команда	Описание
Режим общих настроек	
[no] access-list <6000-7999> {{{add | delete} profile-id WORD} | {{deny|permit} (ip) {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|anydestination}}	Правило используется для настройки управления пунктом назначения. Это правило вступает в силу только после его применения к IP-адресу источника или к MAC-адресу сети VLAN и порту. Для того чтобы удалить указанное правило, необходимо начать команду со слова «NO»

Осталось применить правило к IP-адресу указанного источника, MAC-адресу сети VLAN источника или конкретному порту. Следует отметить, что с учетом вышеприведенных ситуаций глобально эти правила можно использовать только при включении отслеживания IGMP-пакетов. Если же отслеживание выключено, то в рамках протокола IGMP можно использовать только правило для IP-адреса источника. Ниже приводятся команды настройки:

Команда	Описание
Режим настроек порта	
[no] ip multicast destination-control access-group <6000-7999>	Используется для настройки правил, применяемых управлением пунктом назначения к порту. Если команда начинается со слова «NO», настройки отменяются
Режим общих настроек	
[no] ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999>	Используется для настройки правил, применяемых управлением пунктом назначения к указанному IP-адресу/маске сети. Если команда начинается со слова «NO», настройки отменяются
[no] ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>	Используется для настройки правил, применяемых управлением пунктом назначения к указанному IP-адресу/маске сети. Если команда начинается со слова «NO», настройки отменяются

34.2.2.3. Настройка стратегии многоадресной рассылки

Стратегия многоадресной рассылки предполагает назначение указанным многоадресным данным приоритета, благодаря чему достигается и гарантируется удовлетворение требований конкретного пользователя. Необходимо отметить, что для этого данные должны передаваться через магистральный порт. Настройка очень проста. Имеется всего

одна команда: назначение приоритета указанной многоадресной рассылке. Команда приводится ниже:

Команда	Описание
Режим общих настроек	
[no] ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>	Настраивает стратегию многоадресной рассылки. Назначает приоритет источникам и группам в указанном диапазоне (<0–7>)

34.2.3. Примеры настройки DCSCM

34.2.3.1. Управление источником

Для предотвращения передачи многоадресных данных произвольным образом мы настраиваем граничный коммутатор так, чтобы выполнять многоадресную рассылку мог только коммутатор с портом Ethernet 1/0/5. Группа данных должна быть 225.1.2.3. Кроме того, коммутатор, подключенный к порту Ethernet 1/0/10, может передавать многоадресные данные без каких-либо ограничений. Настройки выглядят следующим образом:

```
EC(config)#access-list 5000 permit ip any host 225.1.2.3
EC(config)#access-list 5001 permit ip any any
EC(config)#ip multicast source-control
EC(config)#interface ethernet1/0/5
EC(Config-If-Ethernet1/0/5)#ip multicast source-control accessgroup 5000
EC(config)#interface ethernet1/0/10
EC(Config-If-Ethernet1/0/10)#ip multicast source-control accessgroup 5001
```

34.2.3.2. Управление источником пунктом назначения

Необходимо ограничить доступ к группе 238.0.0.0/8 пользователям, адреса которых принадлежат сегменту сети 10.0.0.0/8. Мы выполняем следующие настройки.

Во-первых, следует включить отслеживание IGMP-пакетов в сети VLAN, в которой находится группа. (Здесь предполагается, что это VLAN2.)

```
EC(config)#ip igmp snooping
EC(config)#ip igmp snooping vlan 2
```

Теперь необходимо настроить список доступа к управлению пунктом назначения и задать IP-адрес для использования этого списка.

```
Switch(config)#access-list 6000 deny ip any 238.0.0.0 0.255.255.255
Switch(config)#access-list 6000 permit ip any any
Switch(config)#multicast destination-control
Switch(config)#ip multicast destination-control 10.0.0.0/8 access-group 6000
```

Таким образом, пользователи этого сегмента сети могут присоединяться к любым группам, кроме 238.0.0.0/8.

Кроме того, настроить список доступа к управлению пунктом назначения можно путем добавления списка профилей.

```
Switch (config)#profile-id 1 deny ip any 238.0.0.0 0.255.255.255
Switch (config)#access-list 6000 add profile-id 1
Switch (config)#multicast destination-control
Switch (config)#ip multicast destination-control 10.0.0.0/8 access-group 6000
```

34.2.3.3. Стратегия многоадресной рассылки

Сервер 210.1.1.1 передает важные многоадресные данные группе 239.1.2.3. Мы можем настроить подключаемый к нему коммутатор следующим образом:

```
Switch(config)#ip multicast policy 210.1.1.1/32 239.1.2.3/32 cos 4
```

Таким образом, когда многоадресный поток поступит через данный коммутатор на другие коммутаторы, значение его приоритета будет равно 4. Как правило, задается более высокий приоритет. Наивысший приоритет получают протокольные данные. Если установлен более высокий приоритет, а многоадресных данных слишком много, может произойти сбой протокола коммутации.

34.2.4. Устранение неисправностей DCSCM

Модуль DCSCM работает аналогично спискам ACL. Возникающие проблемы связаны, как правило, с неверными настройками. Внимательно прочтите изложенную выше информацию. Если определить причину проблемы не удается, отправьте свои настройки и ожидаемые результаты работы персоналу по послепродажному обслуживанию нашей компании.

34.3. Отслеживание IGMP-пакетов

34.3.1. Введение в отслеживание IGMP-пакетов

IGMP (протокол управления группами в сети Интернет) – это протокол, применяемый для многоадресной IP-маршрутизации. С помощью IGMP сетевое устройство (например, маршрутизатор), на котором включена функция многоадресной рассылки, выполняет запросы принадлежности узлов. Узлы, присоединяющиеся к многоадресной группе, используют данный протокол, чтобы сообщить маршрутизатору конкретный адрес, пакеты от которого следует принимать. Все эти операции выполняются с помощью обмена IGMP-сообщениями. Маршрутизатор будет использовать адрес групповой передачи (224.0.0.1) для рассылки всем узлам IGMP-запросов принадлежности. Если узел хочет присоединиться к многоадресной группе, он отправит IGMP-отчет о принадлежности на адрес этой группы.

Отслеживание IGMP-пакетов также известно как IGMP-прослушивание. Коммутатор предотвращает массовую рассылку многоадресного трафика посредством отслеживания IGMP-пакетов. В этом случае многоадресный трафик передается только в те порты, которые связаны с устройствами многоадресной рассылки. Коммутатор прослушивает IGMP-сообщения между многоадресным маршрутизатором и узлами и в зависимости от результатов прослушивания ведет таблицу переадресации многоадресной группы. После этого возможно принятие решения о переадресации многоадресных пакетов в соответствии с данной таблицей.

Коммутатор поддерживает отслеживание IGMP-пакетов и может отправить запрос, позволяющий пользователю применять этот коммутатор для многоадресной IP-рассылки.

34.3.2. Список задач по настройке отслеживания IGMP-пакетов

1. Включить отслеживание IGMP-пакетов.
2. Настроить отслеживание IGMP-пакетов.

1. Включить отслеживание IGMP-пакетов.

Команда	Описание
Режим общих настроек	
ip igmp snooping no ip igmp snooping	Включает отслеживание IGMP-пакетов. Команда, начинающаяся со слова «no», выключает отслеживание

2. Настроить отслеживание IGMP-пакетов.

Команда	Описан ие
Режим общих настроек	
ip igmp snooping vlan <vlan-id> no ip igmp snooping vlan <vlan-id>	Включает отслеживание IGMP-пакетов в указанной сети VLAN. Команда, начинающаяся со слова «no», выключает отслеживание
ip igmp snooping proxy no ip igmp snooping proxy	Включает прокси-функцию отслеживания IGMP-пакетов. Команда, начинающаяся со слова «no», отключает эту функцию
ip igmp snooping vlan < vlan-id > limit {group <g_limit> | source <s_limit>} no ip igmp snooping vlan < vlan-id > limit	Задает максимальное количество групп в сети VLAN и максимальное количество источников для каждой группы. Команда «no ip igmp snooping vlan <vlan-id> limit» отменяет настройки
ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit {group <1-65535>| source <1-65535>} strategy (replace | drop) no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit group source strategy	Задает количество групп, к которым можно присоединяться, и максимальное количество источников для всех групп, относящихся к порту отслеживания IGMP-пакетов. Определяет стратегию поведения при достижении верхнего предела: заменить старую группу или отбросить новую. Команда, начинающаяся со слова «no», означает отсутствие ограничений

Команда	Описан ие
ip igmp snooping vlan <vlan-id> l2-generalquerier no ip igmp snooping vlan <vlan-id> l2-generalquerier	Устанавливает генератор общих запросов уровня 2 для данной сети VLAN. Рекомендуется настраивать генератор общих запросов уровня 2 для сегмента сети. Команда «no ip igmp snooping vlan <vlan-id> l2-general-querier» отменяет настройки
ip igmp snooping vlan <vlan-id> l2-generalquerier-version <version>	Задает номер версии общего запроса от генератора запросов уровня 2
ip igmp snooping vlan <vlan-id> l2-generalquerier-source <source>	Задает адрес источника общего запроса от генератора запросов уровня 2
ip igmp snooping vlan <vlan-id> mrouter-port interface <interface –name> no ip igmp snooping vlan <vlan-id> mrouter-port interface <interface –name>	Задает статический порт многоадресного маршрутизатора в сети VLAN. Команда, начинающаяся со слова «no», отменяет настройки
ip igmp snooping vlan <vlan-id> mrouter-port learnpim no ip igmp snooping vlan <vlan-id> mrouter-port learnpim	Включает функцию, которая позволяет указанной сети VLAN получить информацию о порте многоадресного маршрутизатора (на основе PIM-пакетов). Команда, начинающаяся со слова «no», отключает эту функцию
ip igmp snooping vlan <vlan-id> mrpt <value> no ip igmp snooping vlan <vlan-id> mrpt	Задает время жизни порта многоадресного маршрутизатора. Команда «no ip igmp snooping vlan <vlan-id> mrpt» восстанавливает значение по умолчанию
ip igmp snooping vlan <vlan-id> query-interval <value> no ip igmp snooping vlan <vlan-id> query-interval	Задает интервал между запросами. Команда «no ip igmp snooping vlan <vlan-id> query-interval» восстанавливает значение по умолчанию
ip igmp snooping vlan <vlan-id> immediatelyleave no ip igmp snooping vlan <vlan-id> immediatelyleave	Включает функцию быстрого выхода IGMP для указанной сети VLAN. Команда «no ip igmp snooping vlan <vlan-id> immediate-leave» отключает эту функцию
ip igmp snooping vlan <vlan-id> query-mrsp <value> no ip igmp snooping vlan <vlan-id> query-mrsp	Устанавливает максимальный период между ответами на запрос. Команда «no ip igmp snooping vlan <vlan-id> query-mrsp» восстанавливает значение по умолчанию

Команда	Описан ие
ip igmp snooping vlan <vlan-id> query-robustness <value> no ip igmp snooping vlan <vlan-id> queryrobustness	Задает надежность запроса. Команда «no ip igmp snooping vlan <vlan-id> query-robustness» восстанавливает значение по умолчанию
ip igmp snooping vlan <vlan-id> suppressionquery-time <value> no ip igmp snooping vlan <vlan-id> suppressionquery-time	Задает время подавления запроса. Команда «no ip igmp snooping vlan <vlan-id> suppressionquery-time» восстанавливает значение по умолчанию
ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME> no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>	Устанавливает статическую группу на указанном порте VLAN. Команда, начинающаяся со слова «no», отменяет настройки
ip igmp snooping vlan <vlan-id> report sourceaddress <A.B.C.D> no ip igmp snooping vlan <vlan-id> report sourceaddress	Задает адрес источника, передаваемого IGMP-пакета. Команда, начинающаяся со слова «no», отменяет настройки
ip igmp snooping vlan <vlan-id> specific-querymrsp <value> no ip igmp snooping vlan <vlan-id> specific-querymrspt	Задает максимальное время ответа на запрос конкретной группы или источника. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию

34.3.3. Примеры отслеживания IGMP-пакетов

34.3.3.1. Сценарий 1: функция отслеживания IGMP-пакетов

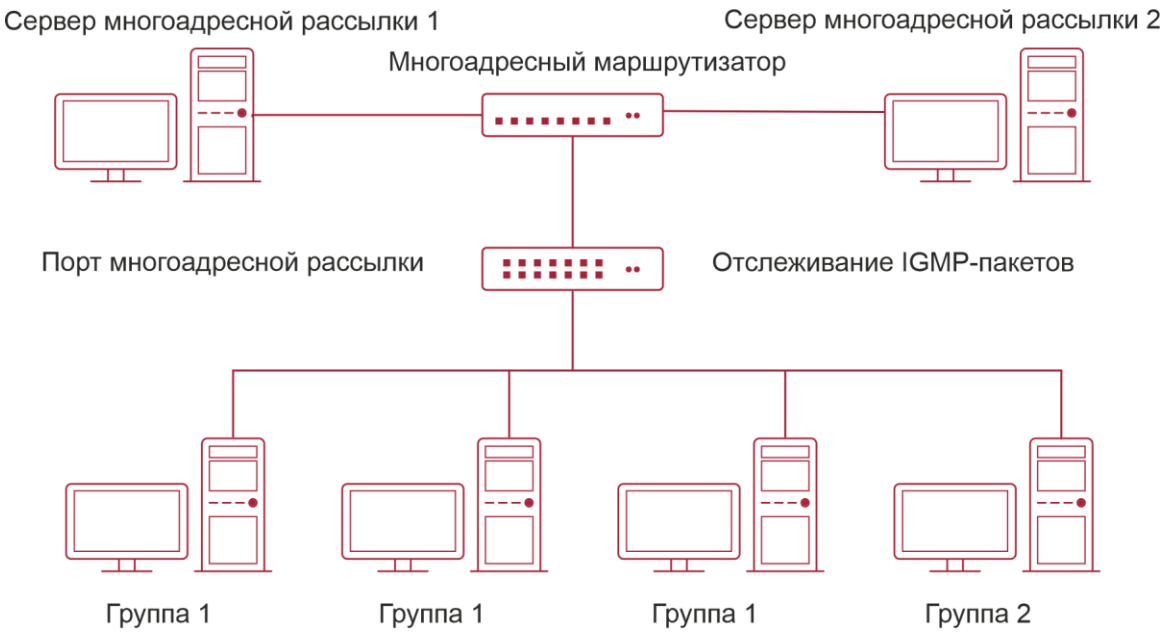


Рисунок 34-1. Включение функции отслеживания IGMP-пакетов

Пример. Как показано на рисунке выше, на коммутаторе настроена сеть VLAN 100, которой принадлежат порты 1, 2, 6, 10 и 12. Четыре узла подключены к портам 2, 6, 10 и 12 соответственно. Многоадресный маршрутизатор подключен к порту 1. По умолчанию отслеживание IGMP-пакетов отключено либо на коммутаторе, либо в сетях VLAN. Следовательно, если требуется включить данную функцию в сети VLAN 100, сначала необходимо включить ее в режиме общих настроек на коммутаторе и затем в сети VLAN 100. Кроме того, следует назначить порт 1 портом многоадресной рассылки.

Ниже приведены этапы настройки:

```
Switch(config)#ip igmp snooping
Switch(config)#ip igmp snooping vlan 100
Switch(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/0/1
```

Настройка многоадресной рассылки.

Предположим, что сервер многоадресной рассылки предлагает две программы, адреса которых Группа 1 и Группа 2. Три из четырех узлов, на которых запущены многоадресные приложения, подключены к портам 2, 6 и 10 и воспроизводят программу 1, а узел, подключенный к порту 12, воспроизводит программу 2.

Результат IGMP-прослушивания.

В таблице многоадресной маршрутизации, построенной в сети VLAN 100 функцией отслеживания IGMP-пакетов, порты 1, 2, 6 и 10 относятся к Группе 1, а порты 1 и 12 — к Группе 2.

Каждый из четырех узлов может принимать нужную ему программу: порты 2, 6 и 10 не будут получать трафик программы 2, а порт 12 — трафик программы 1.

34.3.3.2. Сценарий 2: генератор общих запросов L2

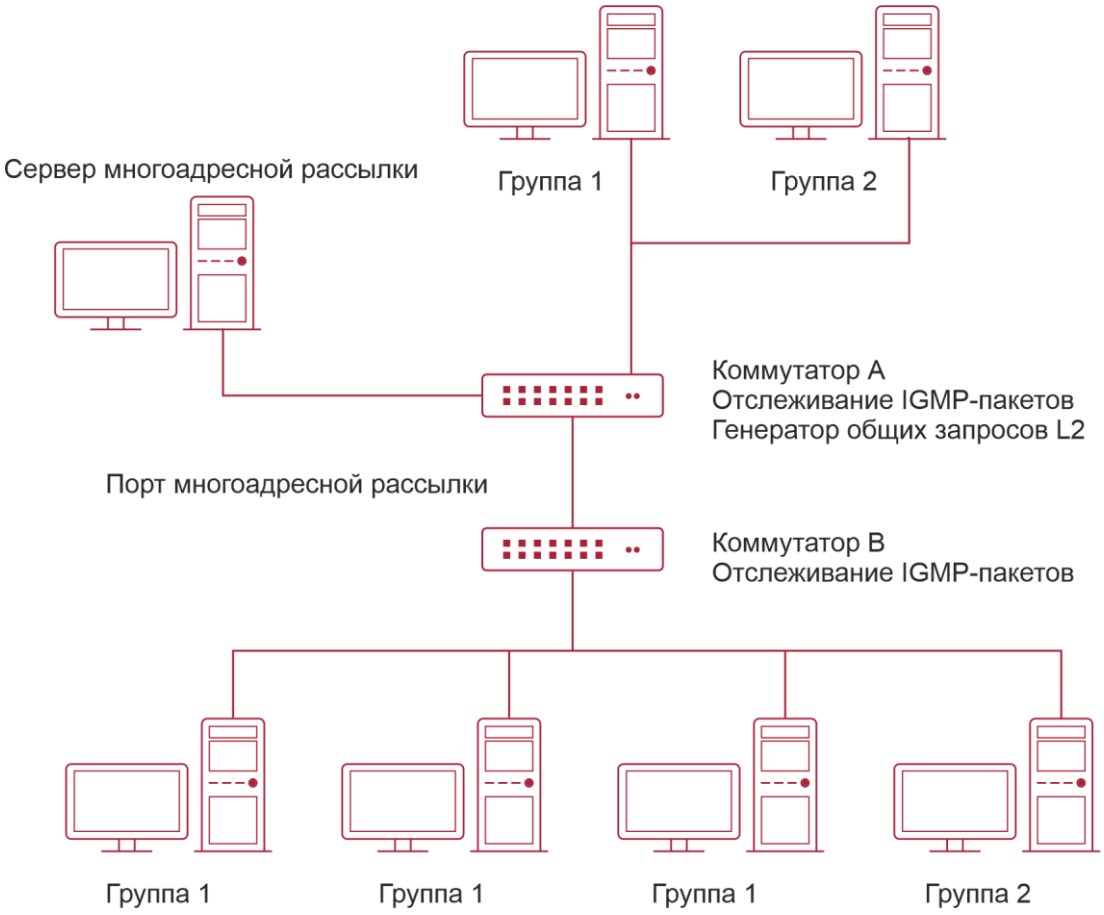


Рисунок 34-2. Коммутаторы как IGMP-запросы

Коммутатор B настроен так же, как коммутатор в сценарии 1. Коммутатор A заменяет многоадресный маршрутизатор в сценарии 1. Предположим, на коммутаторе A настроена сеть VLAN 60, которой принадлежат порты 1, 2, 10 и 12. Порт 1 подключен к серверу многоадресной рассылки, а порт 2 — к коммутатору 2. Для того чтобы отправлять запросы через определенные интервалы времени, необходимо включить функцию IGMP-запросов в режиме общих настроек и в сети VLAN 60.

Ниже приведены этапы настройки:

```
SwitchA#config
SwitchA(config)#ip igmp snooping
SwitchA(config)#ip igmp snooping vlan 60
SwitchA(config)#ip igmp snooping vlan 60 L2-general-querier
SwitchB#config
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 100
SwitchB(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/0/1
```

Настройка многоадресной рассылки. Такая же, как в сценарии 1.

Результат IGMP-прослушивания. Такой же, как и в сценарии 1.

34.3.4. Устранение неисправностей при отслеживании IGMP-пакетов

Неисправности при отслеживании IGMP-пакетов возникают в результате ошибок физического соединения или неправильной настройки. Пользователям следует выполнить следующие действия:

- Убедиться в правильности физического соединения.
- Активировать отслеживание IGMP-пакетов в режиме общих настроек (команда `ip igmp snooping`).
- Настроить отслеживание IGMP-пакетов в сети VLAN в режиме общих настроек (команда `ip igmp snooping vlan <vlan-id>`).
- Убедиться в том, что одна сеть VLAN настроена как стандартное устройство проверки L2 с той же маской или же настроен статический многоадресный маршрутизатор.
- Для проверки информации об отслеживании IGMP-пакетов использовать команду `show ip igmp snooping vlan <vid>`.

34.4. Аутентификация при отслеживании IGMP-пакетов

34.4.1. Введение в аутентификацию при отслеживании IGMP-пакетов

Аутентификация при отслеживании IGMP-пакетов представляет собой аутентификацию многоадресной группы, запрос на присоединение к которой отправляет клиент. Если многоадресная группа проходит аутентификацию, клиент успешно к ней присоединяется и может получать многоадресный трафик. В противном случае клиент получает отказ. В настоящее время аутентификация зависит только от группы. Аутентификация данных источника многоадресной рассылки в IGMPv3 не включена.

34.4.2. Список задач аутентификации при отслеживании IGMP-пакетов

1. Включить отслеживание IGMP-пакетов.
2. Включить аутентификацию при отслеживании IGMP-пакетов.
3. Настроить аутентификацию при отслеживании IGMP-пакетов.
4. Настроить Radius.

1. Включить отслеживание IGMP-пакетов.

Команда	Описание
Режим общих настроек	
ip igmp snooping no ip igmp snooping	Включает функцию отслеживания IGMP-пакетов. Команда, начинающаяся со слова «no», отключает эту функцию

2. Включить аутентификацию при отслеживании IGMP-пакетов.

Команда	Описание
Режим конфигурирования порта	
igmp snooping authentication enable no igmp snooping authentication enable	Включает на порте функцию аутентификации при отслеживании IGMP-пакетов. Команда, начинающаяся со слова «no», отключает эту функцию. После включения этой функции порт проведет аутентификацию многоадресной группы, запрос на присоединение к которой отправляет клиент. Если многоадресная группа проходит аутентификацию, то клиент успешно к ней присоединяется. В противном случае клиент получает отказ

3. Настроить аутентификацию при отслеживании IGMP-пакетов.

Команда	Описание
Режим конфигурирования порта	
igmp snooping authentication free-rule access-list <6000-7999> no igmp snooping authentication free-rule accesslist <6000-7999>	Настраивает список доступа многоадресной группы на основе правила, не требующего прохождения аутентификации. Команда, начинающаяся с «no», удаляет его
Режим общих настроек	
ip igmp snooping authentication radius none no ip igmp snooping authentication radius none	Позволяет коммутатору разрешить подключение к многоадресной группе, успешно прошедшей аутентификацию, в случае, если сервер Radius не отвечает. Команда, начинающаяся со слова «no», восстанавливает метод аутентификации по умолчанию. Коммутатор работает с невыполненной аутентификацией
ip igmp snooping authentication forwarding-first no ip igmp snooping authentication forwardingfirst	Настраивает процесс IGMP-аутентификации: делает в таблице многоадресной маршрутизации запись о многоадресной группе, запрос на присоединение к которой отправляет клиент, и потом выполняет аутентификацию. При успешной аутентификации ничего не происходит. Если аутентификация не удалась, запись удаляется из таблицы. Команда, начинающаяся со слова «no», восстанавливает метод аутентификации по умолчанию: сначала выполняется

Команда	Описание
	аутентификация, а запись в таблицу вносится после получения результата
ip igmp snooping authentication timeout <30-30000> no ip igmp snooping authentication timeout	Задает тайм-аут записи таблицы при IGMP-аутентификации. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию, равное 600 с

4. Настроить Radius.

Команда	Описание
Режим общих настроек	
aaa enable no aaa enable	Включает или отключает функцию AAA
radius-server key <word> no radius-server key	Задает или удаляет серверный ключ RADIUS
radius-server authentication host <A.B.C.D> no radius-server authentication host <A.B.C.D>	Задает или удаляет адрес сервера аутентификации RADIUS

34.4.3. Примеры аутентификации при отслеживании IGMP-пакетов

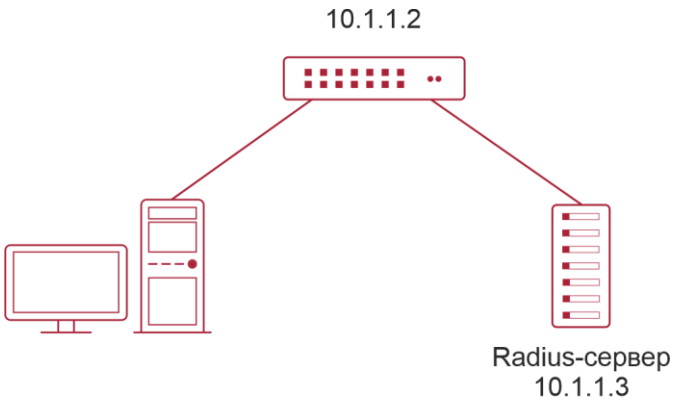


Рисунок 34-3. Аутентификация при отслеживании IGMP-пакетов

Как показано на рисунке выше, на коммутаторе настроены сети VLAN1, которой принадлежит порт 1, и VLAN10, которой принадлежит порт 2. Узел подключен к порту 1, сервер Radius — к порту 2. В сети VLAN1 включается отслеживание IGMP-пакетов, на

порте 1 — IGMP-аутентификация. Коммутатору назначен IP-адрес 10.1.1.2, а серверу Radius — 10.1.1.3.

Этапы настройки

```
Switch#config
Switch(config)#ip igmp snooping
Switch(config)#ip igmp snooping vlan 1
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#igmp snooping authentication enable
Switch(config-if-ethernet1/0/1)# exit
Switch(config)#ip igmp snooping authentication radius none
Switch(config)#interface vlan 10
Switch(config-if-vlan10)#ip address 10.1.1.2 255.255.255.0
Switch(config-if-vlan10)# exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
```

35. ПРОТОКОЛ МНОГОАДРЕСНОЙ МАРШРУТИЗАЦИИ (MULTICAST) IPV6

35.1. Отслеживание MLD-пакетов

35.1.1. Введение в отслеживание MLD-пакетов

С помощью MLD, многоадресного протокола обнаружения прослушивателей, реализуется многоадресная рассылка для IPv6. Обычно MLD используется сетевым оборудованием, например, маршрутизаторами, которые поддерживают многоадресную рассылку, для обнаружения прослушивателей. Кроме того, этот протокол применяют прослушиватели, ожидающие присоединения к конкретной многоадресной группе: маршрутизатору передается информация о том, что необходимо принимать пакеты данных от конкретного адреса групповой передачи. Все это осуществляется путем обмена MLD-сообщениями. Сначала маршрутизатор использует адрес групповой передачи, с которого можно рассылать сообщения всем прослушивателям (ff02::1), для отправки запроса прослушивателя многоадресной рассылки MLD. При наличии прослушивателя, желающего присоединиться к адресу групповой передачи, он посылает обратно по адресу групповой передачи отчет о прослушивании рассылки MLD.

Отслеживание MLD-пакетов представляет собой MLD-прослушивание. Коммутатор предотвращает массовую рассылку многоадресного трафика посредством отслеживания MLD-пакетов. В этом случае многоадресный трафик передается только в те порты, которые связаны с устройствами многоадресной рассылки. Коммутатор прослушивает MLD-сообщения между многоадресными маршрутизаторами и прослушивателями и на основе результатов прослушивания ведет список переадресации многоадресной группы. Коммутатор рассылает многоадресные пакеты в соответствии с этим списком.

На коммутаторе реализована функция отслеживания MLD-пакетов и одновременно поддерживается MLDv2. Таким образом, пользователь вместе с коммутатором получает многоадресную маршрутизацию IPv6.

35.1.2. Список задач по настройке отслеживания MLD-пакетов

1. Включить функцию отслеживания MLD-пакетов.
2. Настроить отслеживание MLD-пакетов.

1. Включить функцию отслеживания MLD-пакетов.

Команда	Описание
Режим общих настроек	
ipv6 mld snooping no ipv6 mld snooping	Включает глобальное отслеживание MLD-пакетов. Команда «no ipv6 mld snooping» отключает отслеживание

2. Настроить отслеживание MLD-пакетов.

Команда	Описание
Режим общих настроек	
ipv6 mld snooping vlan <vlan-id> no ipv6 mld snooping vlan <vlan-id>	Включает отслеживание MLD-пакетов в указанной сети VLAN. Команда, начинающаяся со слова «no», отключает отслеживание
ipv6 mld snooping vlan <vlan-id> limit {group <g_limit> | source <s_limit>} no ipv6 mld snooping vlan <vlan-id> limit	Задает количество групп, к которым может присоединиться отслеживание MLD-пакетов, и максимальное количество источников в каждой группе. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию
ipv6 mld snooping vlan <vlan-id> l2-generalquerier no ipv6 mld snooping vlan <vlan-id> l2-generalquerier	Устанавливает генератор общих запросов уровня 2 для сети VLAN (рекомендуется настраивать для всех сегментов). Команда, начинающаяся со слова «no», отменяет настройки генератора
ipv6 mld snooping vlan <vlan-id> mrouter-port interface <interface –name> no ipv6 mld snooping vlan <vlan-id> mrouter-port interface <interface –name>	Задает статический порт многоадресного маршрутизатора в указанной сети VLAN. Команда, начинающаяся со слова «no», отменяет настройки
ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6 no ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6	Включает функцию, которая позволяет указанной сети VLAN получить информацию о порте многоадресного маршрутизатора (на основе пакетов PIMv6). Команда, начинающаяся со слова «no», отключает эту функцию
ipv6 mld snooping vlan <vlan-id> mrpt <value> no ipv6 mld snooping vlan <vlan-id> mrpt	Задает время жизни порта многоадресного маршрутизатора. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию
ipv6 mld snooping vlan <vlan-id> query-interval <value> no ipv6 mld snooping vlan <vlan-id> query-interval	Задает интервал между запросами. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию

Команда	Описание
ipv6 mld snooping vlan <vlan-id> immediate-leave no ipv6 mld snooping vlan <vlan-id> immediateleave	Настраивает функцию быстрого выхода многоадресной группы при отслеживании MLD-пакетов в указанной сети VLAN. Команда, начинающаяся со слова «no», отменяет настройки
ipv6 mld snooping vlan <vlan-id> query-mrsp <value> no ipv6 mld snooping vlan <vlan-id> query-mrsp	Устанавливает максимальный период между ответами на запрос. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию
ipv6 mld snooping vlan <vlan-id> query-robustness <value> no ipv6 mld snooping vlan <vlan-id> queryrobustness	Задает надежность запроса. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию
ipv6 mld snooping vlan <vlan-id> suppressionquery-time <value> no ipv6 mld snooping vlan <vlan-id> suppressionquery-time	Задает время подавления запроса. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию
Ipv6 mld snooping vlan <vlan-id> static-group	Устанавливает статическую группу на указанном
<X:X::X:X> [source <X:X::X:X>] interface [ethernet | port-channel] <IFNAME> no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source <X:X::X:X>] interface [ethernet | port-channel] <IFNAME>	порте VLAN. Команда, начинающаяся со слова «no», отменяет настройки

35.1.3. Примеры отслеживания MLD-пакетов

35.1.3.1. Сценарий 1: функция отслеживания MLD-пакетов

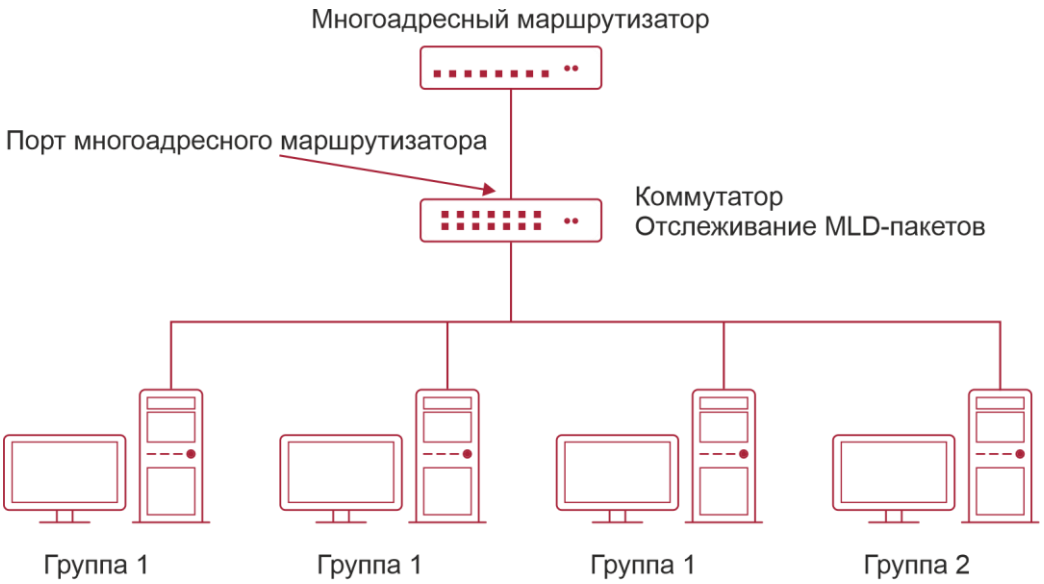


Рисунок 35-1. Функция отслеживания MLD-пакетов

Как показано на рисунке выше, на коммутаторе настроена сеть VLAN 100, которой принадлежат порты 1, 2, 6, 10 и 12. Четыре узла подключены к портам 2, 6, 10 и 12 соответственно. Многоадресный маршрутизатор подключен к порту 1. Предположим, требуется включить отслеживание MLD-пакетов в сети VLAN 100. Однако по умолчанию данная функция отключена как в режиме общих настроек, так и во всех сетях VLAN. Следовательно, сначала необходимо включить ее в режиме общих настроек на коммутаторе и затем в сети VLAN 100. Кроме того, следует назначить порт 1 портом многоадресной рассылки.

Ниже приводится процедура настройки.

```
Switch#config
Switch(config)#ipv6 mld snooping
Switch(config)#ipv6 mld snooping vlan 100
Switch(config)#ipv6 mld snooping vlan 100 mrouter-port interface ethernet 1/0/1
```

35.1.4. Настройка многоадресной рассылки

Предположим, что есть два сервера многоадресной рассылки: Сервер многоадресной рассылки 1 и Сервер многоадресной рассылки 2. Сервер 1 предлагает программы 1 и 2, а сервер 2 — программу 3. Программам назначены адреса групповой передачи Группа1, Группа 2 и Группа 3 соответственно. Многоадресное приложение работает одновременно на четырех узлах. Два узла, подключенные к портам 2 и 6, воспроизводят программу 1, узел, подключенный к порту 10 — программу 2, а узел, подключенный к порту 12 — программу 3.

35.1.5. Результат MLD-прослушивания

Из таблицы многоадресной маршрутизации сети VLAN 100 видно следующее: порты 1, 2, 6 относятся к (Сервер многоадресной рассылки 1, Группа 1), порты 1 и 10 относятся к (Сервер многоадресной рассылки 1, Группа 2), а порты 1, 121 и 12 относятся к (Сервер многоадресной рассылки 2, Группа 3).

Каждый из четырех узлов успешно принимает нужную ему программу: порты 2 и 6 не получают трафик программ 2 и 3, порт 10 — трафик программ 1 и 3, а порт 12 — трафик программ 1 и 2.

35.1.5.1. Сценарий 2: генератор общих запросов L2 MLD

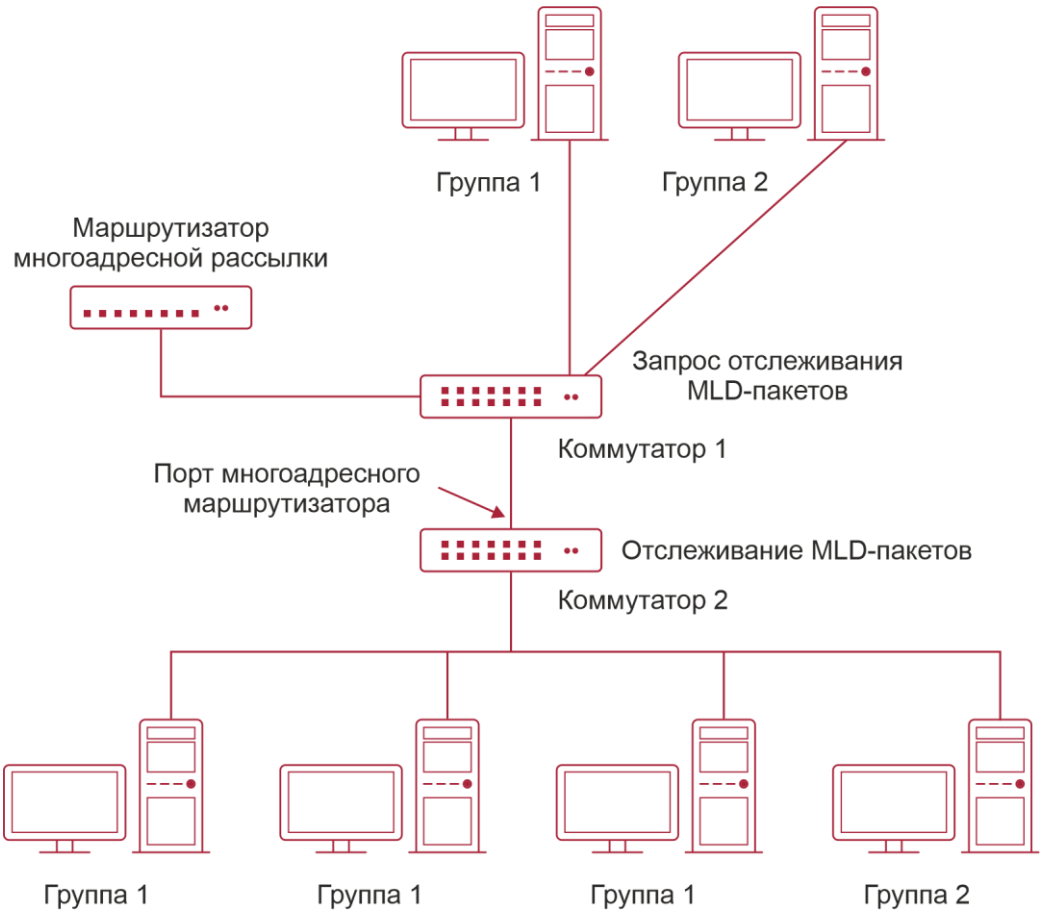


Рисунок 35-2. Коммутатор как генератор запросов при отслеживании MLD-пакетов

Коммутатор B настроен так же, как коммутатор в сценарии 1. Коммутатор A заменяет многоадресный маршрутизатор в сценарии 1. Предположим, что на нем настроена сеть VLAN 60, которой принадлежат порты 1, 2, 10 и 12. Порт 1 подключен к серверу многоадресной рассылки, а порт 2 — к коммутатору B. Для того чтобы отправлять запросы через определенный интервал времени, необходимо включить отслеживание MLD-пакетов в режиме общих настроек, а для сети VLAN 60 настроить генератор общих запросов уровня 2.

Ниже приводится процедура настройки.

```
SwitchA#config
```

```
SwitchA(config)#ipv6 mld snooping
SwitchA(config)#ipv6 mld snooping vlan 60
SwitchA(config)#ipv6 mld snooping vlan 60 l2-general-querier
SwitchB#config
SwitchB(config)#ipv6 mld snooping
SwitchB(config)#ipv6 mld snooping vlan 100
SwitchB(config)#ipv6 mld snooping vlan 100 mrouter interface ethernet 1/0/1
```

Настройка многоадресной рассылки. Такая же, как в сценарии 1.

Результат MLD-прослушивания. Такая же, как в сценарии 1.

35.1.6. Устранение неисправностей при отслеживании MLD-пакетов

Отказ сервера при настройке и использовании отслеживания MLD-пакетов может произойти в результате ошибок физического соединения, неправильной настройки и т. д. Пользователям следует выполнить следующие действия:

- Убедиться в правильности физического соединения.
- Убедиться, что отслеживание MLD-пакетов включено в режиме общих настроек (команда ipv6 mld snooping).
- Убедиться, что отслеживание MLD-пакетов в сети VLAN включено в режиме общих настроек (команда ipv6 mld snooping vlan <vlan-id>).
- Убедиться в том, что одна сеть VLAN настроена как генератор общих запросов L2 или же в сегменте сети настроен статический многоадресный маршрутизатор.
- Для проверки информации об отслеживании MLD-пакетов использовать команду.

36. СЕТЬ VLAN ДЛЯ МНОГОАДРЕСНОЙ РАССЫЛКИ (MULTICAST)

36.1. Введение в сеть VLAN для многоадресной рассылки

При текущем методе подачи многоадресных заявок происходит следующее: заявки пользователей находятся в разных сетях VLAN, и каждая VLAN копирует многоадресный трафик, что приводит к колоссальным тратам пропускной способности. При настройке сети VLAN для многоадресной рассылки в нее добавляется порт коммутатора, на котором включена функция отслеживания пакетов IGMP/MLD. Таким образом, пользователи, находящиеся в разных сетях VLAN, совместно используют одну сеть VLAN для многоадресной рассылки. Многоадресный трафик существует только в пределах VLAN для многоадресной рассылки, благодаря чему экономится пропускная способность. Поскольку VLAN для многоадресной рассылки работает отдельно от пользовательских VLAN, можно одновременно решать проблемы безопасности и пропускной способности. После настройки VLAN пользователи непрерывно получают многоадресный трафик.

36.2. Список задач по настройке сети VLAN для многоадресной рассылки

1. Включить функцию сети VLAN для многоадресной рассылки.
2. Настроить отслеживание IGMP-пакетов.
3. Настроить отслеживание MLD-пакетов.

1. Включить функцию сети VLAN для многоадресной рассылки.

Команда	Описание
Режим настройки сети VLAN	
multicast-vlan no multicast-vlan	Настраивает сеть VLAN и объявляет ее многоадресной. Команда «no multicast-vlan» отключает эту функцию
multicast-vlan association <vlan-list> no multicast-vlan association <vlan-list>	Устанавливает связь сети VLAN для многоадресной рассылки с несколькими сетями VLAN. Команда, начинающаяся со слова «no», удаляет сети VLAN, связанные с сетью VLAN для многоадресной рассылки
multicast-vlan association interface (ethernet | port-channel|) IFNAME no multicast-vlan association interface (ethernet | port-channel|) IFNAME	Устанавливает связь сети VLAN для многоадресной рассылки с конкретными портами. Таким образом, связанные порты смогут принимать многоадресный поток. Команда, начинающаяся со слова «no», отменяет эту связь

Команда	Описание
multicast-vlan mode {dynamic| compatible} no multicast-vlan mode {dynamic| compatible}	Настраивает два режима сети VLAN для многоадресной рассылки. Команда, начинающаяся со слова «no», отменяет настройки

2. Настроить отслеживание IGMP-пакетов.

Команда	Описание
ip igmp snooping vlan <vlan-id> no ip igmp snooping vlan <vlan-id>	Включает в сети VLAN для многоадресной рассылки функцию отслеживания IGMP-пакетов. Команда, начинающаяся со слова «no», отключает отслеживание
ip igmp snooping no ip igmp snooping	Включает функцию отслеживания IGMP-пакетов. Команда, начинающаяся со слова «no», отключает отслеживание

3. Настроить отслеживание MLD-пакетов.

Команда	Описание
Режим	
ipv6 mld snooping vlan <vlan-id> no ipv6 mld snooping vlan <vlan-id>	Включает в сети VLAN для многоадресной рассылки отслеживание MLD-пакетов. Команда, начинающаяся со слова «no», отключает отслеживание
ipv6 mld snooping no ipv6 mld snooping	Включает функцию отслеживания MLD-пакетов. Команда, начинающаяся со слова «no», отключает отслеживание

36.3. Примеры сети VLAN для многоадресной рассылки

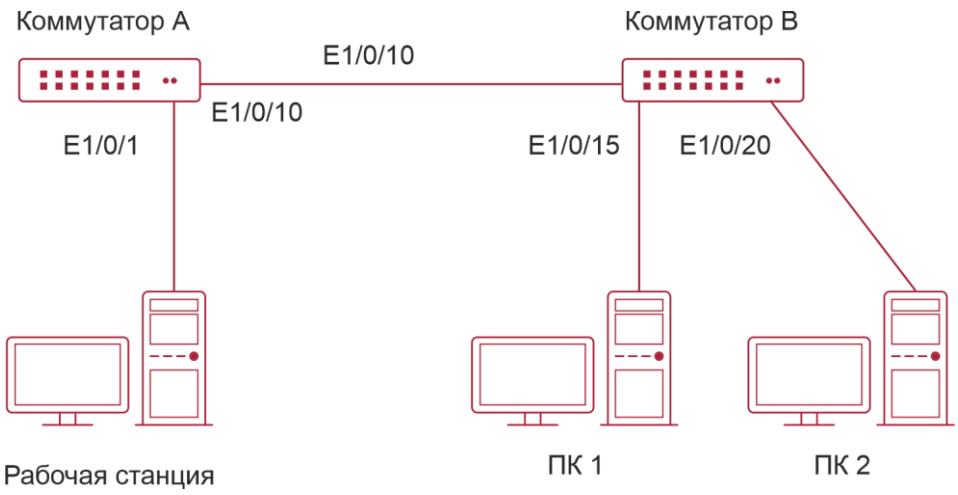


Рисунок 36-1. Функциональная конфигурация сети VLAN для многоадресной рассылки

Как показано на рисунке, сервер многоадресной рассылки подключен к коммутатору switchA уровня 3 через порт 1/0/1, который принадлежит сети коммутатора VLAN10. Коммутатор уровня 3 switchA подключен к коммутаторам уровня 2 через порт 1/0/10, настроенный в качестве магистрального порта. На коммутаторе switchB настроены сеть VLAN100, которой принадлежит порт 1/0/15, и сеть VLAN101, которой принадлежит порт 1/0/20. PC1 и PC2 подключены к портам 1/0/15 и 1/0/20 соответственно. Коммутатор switchB подключен к коммутатору switchA через порт 1/0/10, настроенный в качестве магистрального порта. VLAN 20 представляет собой сеть для многоадресной рассылки. Благодаря настройке VLAN для многоадресной рассылки PC1 и PC2 смогут получать от нее многоадресные данные.

Предполагается, что в приведенной ниже конфигурации коммутатору назначен IP-адрес, а все оборудование подключено правильно.

36.3.1. Процедура настройки

```
SwitchA#config
SwitchA(config)#vlan 10
SwitchA(config-vlan10)#switchport access ethernet 1/0/1
SwitchA(config-vlan10)exit
SwitchA(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip pim dense-mode
Switch(Config-if-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan20)#exit
SwitchA(config)#interface vlan 20
SwitchA(Config-if-Vlan20)#ip pim dense-mode
SwitchA(Config-if-Vlan20)#exit
```

```
SwitchA(config)#ip pim multicast
SwitchA(config)# interface ethernet1/0/10
SwitchA(Config-If-Ethernet1/0/10)switchport mode trunk
SwitchB#config
SwitchB(config)#vlan 100
SwitchB(config-vlan100)#Switchport access ethernet 1/0/15
SwitchB(config-vlan100)exit
SwitchB(config)#vlan 101
SwitchB(config-vlan101)#Switchport access ethernet 1/0/20
SwitchB(config-vlan101)exit
SwitchB(config)# interface ethernet 1/0/10
SwitchB(Config-If-Ethernet1/0/10)#switchport mode trunk
SwitchB(Config-If-Ethernet1/0/10)#exit
SwitchB(config)#vlan 20
SwitchB(config-vlan20)#multicast-vlan
SwitchB(config-vlan20)#multicast-vlan association 100,101
SwitchB(config-vlan20)#exit
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 20
```

Если сеть VLAN для многоадресной рассылки поддерживает многоадресную маршрутизацию IPv6, единственное различие с IPv4 заключается в отслеживании MLD-пакетов. В связи с этим пример не приводится.

37. НАСТРОЙКА АВТОМАТИЧЕСКИ ОПРЕДЕЛЯЕМЫХ СПИСКОВ ACL

37.1. Введение в автоматически определяемые списки ACL

ACL (списки контроля доступа) — это встроенный в коммутатор механизм фильтрации пакетов, который осуществляет контроль доступа в сеть и, таким образом, эффективно обеспечивает ее безопасность. На основе некоторых характерных для пакетов данных пользователь задает набор правил. Эти правила указывают, что именно следует сделать с пакетом, для которого найдено соответствие с этими данными: «разрешить» или «отклонить». Подобные правила можно применять на входящем направлении портов коммутатора. Таким образом, потоки данных, проходящие через конкретные порты, должны соответствовать назначенным правилам ACL.

Термин «автоматически определяемые списки ACL» означает, что при настройке ACL можно в качестве полей соответствия установить несколько автоматически определяемых окон. Автоматически определяемые окна указывают не конкретное поле, а смещение в пакете. Значение поля при этом игнорируется. Они сравнивают данные, находящиеся в положении смещения, и в соответствии с настройками значения и маски изменяют количество байт.

37.1.1. Шаблон стандартных автоматически определяемых списков ACL

Для стандартного автоматически определяемого списка ACL можно настроить 12 окон. Каждому окну задается начальное положение смещения: начало заголовка L3/начало заголовка L4. Кроме того, для всех окон можно установить смещение: значение находится в пределах от 0 до 178, а длина блока составляет 2 байта, т. е. 0 означает смещение в 0 байт, а 1 — смещение в 2 байта. Смещение зависит от начального положения смещения.

Прежде чем настраивать стандартный автоматически определяемый список ACL, необходимо создать шаблон стандартных автоматически определяемых списков ACL, чтобы установить смещение для каждого окна. Этот шаблон является общим и действует для всех стандартных автоматически определяемых списков ACL. Наибольшее число окон, для которых в таком шаблоне можно задать начальное положение и смещение, равно 12. Ненастроенное окно будет недоступным, т. е. если стандартный автоматически определяемый список ACL будет использовать это окно, оно не сможет успешно передать конфигурацию. Если вместе с окном задано правило стандартного автоматически определяемого списка ACL, то после завершения настройки окно изменить нельзя. В противном случае окно можно перенастроить, изменить или удалить. IPv6 поддерживает окна 1–6. Наибольшее смещение l3start включает заголовок L2, а наибольшее смещение l4start — заголовки L2 и L3.

37.1.2. Стандартные автоматически определяемые списки ACL

Стандартные автоматически определяемые списки ACL позволяют настраивать несколько списков ACL, каждый из которых позволяет задавать несколько правил. С помощью одного правила можно задать значение и маску не более чем 12 окнам. Длина окна составляет 2 байта. Диапазон имен стандартного автоматически определяемого списка ACL: <1200–1299>.

37.1.3. Передача конфигурации автоматически определяемых списков ACL

Как стандартные, так и расширенные автоматически определяемые списки ACL можно настроить для работы в направлении портов и сетей VLAN. Если для списка ACL существует правило, которое согласует VLAN ID, и этот список настроен для сети VLAN, то условие согласования для сообщения задается в настройках VLAN.

37.1.4. Дополнительное пояснение

Из-за ограничений микросхемы для стандартного автоматически определяемого списка ACL нельзя одновременно настроить метод доступа, предотвращение сканирования ARP или dot1x. Кроме того, для расширенного автоматически определяемого списка ACL нельзя одновременно настроить IPv6 ACL SAVI, IP/IPv4 DCSCM, перенаправление потока IPv6 или QoS (соответствует IPv6 ACL).

37.2. Настройка автоматически определяемых списков ACL

Список задач по настройке автоматически определяемых списков ACL:

1. Настроить шаблон определяемого пользователем списка ACL.
   1.1. Настроить шаблон стандартного определяемого пользователем списка ACL.
2. Настроить определяемый пользователем список ACL.
   2.1. Настроить стандартный определяемый пользователем список ACL.
3. Привязать определяемый пользователем список ACL к конкретному порту.
4. Привязать определяемый пользователем список ACL к конкретной сети VLAN.

1. Настроить шаблон определяемого пользователем списка ACL.
   1.1. Настроить шаблон стандартного определяемого пользователем списка ACL

Команда	Описание
Режим общих настроек	
userdefined-access-list standard offset [window1 {l3start | l4start} <offset>] [window2 { l3start | l4start } <offset>] [window3 { l3start | l4start } <offset>] [window4 { l3start | l4start } <offset>] [window5 { l3start | l4start } <offset>] [window6 { l3start | l4start } <offset>] [window7 { l3start | l4start } <offset>] [window8 { l3start | l4start } <offset>] [window9 { l3start | l4start } <offset>] [window10 { l3start | l4start } <offset>] [window11 { l3start | l4start } <offset>] [window12 { l3start | l4start } <offset>]	Создает шаблон стандартного автоматически определяемого списка ACL. Если шаблон существует, можно редактировать соответствующее окно

Команда	Описание
no userdefined-access-list standard offset [window1] [window2] [window3] [window4] [window5] [window6] [window7] [window8] [window9] [window10] [window11] [window12]	Команда, начинающаяся со слова «no», удаляет окно шаблона. Если окно не указано, шаблон будет удален

2. Настроить определяемый пользователем список ACL.

2.1. Настроить стандартный определяемый пользователем список ACL.

Команда	Описание
Режим общих настроек	
[no] vacl userdefined access-group <name> {in} vlan <vlanId> [traffic-statistic]	Применяет определяемый пользователем список доступа на одном направлении указанной сети VLAN. В зависимости от существующих вариантов принимает решение о том, следует ли добавлять в список ACL статистический счетчик. Команда, начинающаяся со слова «no», удаляет связанные с VLAN настройки

3. Привязать определяемый пользователем список ACL к конкретному порту.

Команда	Описание
Режим физического порта	
[no] userdefined access-group <name> {in} [traffic-statistic]	Применяет определяемый пользователем список доступа на одном направлении порта. В зависимости от существующих вариантов принимает решение о том, следует ли добавлять в список ACL статистический счетчик. Команда, начинающаяся со слова «no», удаляет связанные с портом настройки

4. Привязать определяемый пользователем список ACL к конкретной сети VLAN.

Команда	Описание
Режим общих настроек	
[no] vacl userdefined access-group <name> {in} vlan <vlanId> [traffic-statistic]	Применяет определяемый пользователем список доступа на одном направлении указанной сети VLAN. В зависимости от существующих вариантов принимает решение о том, следует ли добавлять в список ACL статистический счетчик. Команда, начинающаяся со слова «no», удаляет связанные с VLAN настройки

37.3. Пример автоматически определяемого списка ACL

Пользователь предъявляет к конфигурации следующие требования: порт 10 коммутатора подключен к сегменту 10.0.0.0/24, FTP не требуется.

37.3.1. Описание конфигурации

1. В соответствии с условиями создать шаблон автоматически определяемого списка ACL.
2. Создать соответствующий автоматически определяемый список ACL.
3. Привязать автоматически определяемый список ACL к порту.

Ниже приведены этапы настройки:

```
Switch(config)# userdefined-access-list standard offset window1 l3start 4 window2 l4start 1 window3 l3start 3
Switch(config)#userdefined-access-list standard 1300 deny window1 0006 00FF window2 0015 FFFF window3 0A000000 FFFFFF00
Switch(config)#firewall enable
Switch(config)#interface ethernet1/10
Switch(config-if-ethernet1/10)#userdefined access-group 1300 in
Switch(config-if-ethernet1/10)#exit
Switch(config)#exit
```

Результат настройки:

```
Switch#show access-lists
userdefined-access-list standard 1300(used 1 time(s)) 1 rule(s)
rule ID 1: window1 6 ff window2 15 ffff window3 a000000 ffffff00
Switch#show access-group interface ethernet 1/10
interface name:Ethernet1/10
Userdefined Ingress access-list used is 1300,trafficstatistics Disable.
```

38. НАСТРОЙКА ПРОТОКОЛА 802.1X

38.1. Введение в протокол 802.1x

Протокол 802.1x возник на основе протокола 802.11, который представляет собой протокол IEEE для коммуникации в беспроводных локальных сетях и разработан в качестве решения для аутентификации пользователей при входе в беспроводную сеть. Сеть LAN, определенная в протоколе IEEE 802 для коммуникации в локальных сетях, не поддерживает аутентификацию доступа. Это означает, что если у пользователей есть доступ к управляющему устройству LAN (например, к коммутатору), то им также доступны любые другие устройства и ресурсы в этой сети LAN. При таком устройстве LAN первым корпоративным сетям никакая опасность не угрожала.

Однако в связи с ростом популярности таких приложений, как мобильный офис и операции по обслуживанию, интернет-провайдерам следует управлять доступом пользователя и настраивать его. В частности, широкое распространение доступа к WLAN и LAN в телекоммуникационных сетях ведет к необходимости управлять портами, чтобы обеспечить контроль доступа на уровне пользователей. В результате, для того чтобы реализовать контроль доступа в сеть на уровне портов, комитетом по стандартам IEEE LAN/WAN был определен стандарт 802.1x. Этот стандарт получил широкое распространение в беспроводных сетях LAN и Ethernet.

Термин «контроль доступа в сеть на уровне портов» означает, что аутентификация и управление пользовательскими устройствами ведется на уровне портов устройств доступа к LAN. Ресурсы сети LAN становятся доступны только после того, как устройства пользователей, подключенные к портам, проходят аутентификацию. В противном случае ресурсы недоступны.

38.1.1. Структура системы аутентификации протокола 802.1x

Система, использующая протокол 802.1x, обладает типичной структурой клиент/сервер. Эта структура состоит из трех объектов (см. следующий рисунок): клиентская система, аутентификатор и сервер аутентификации.

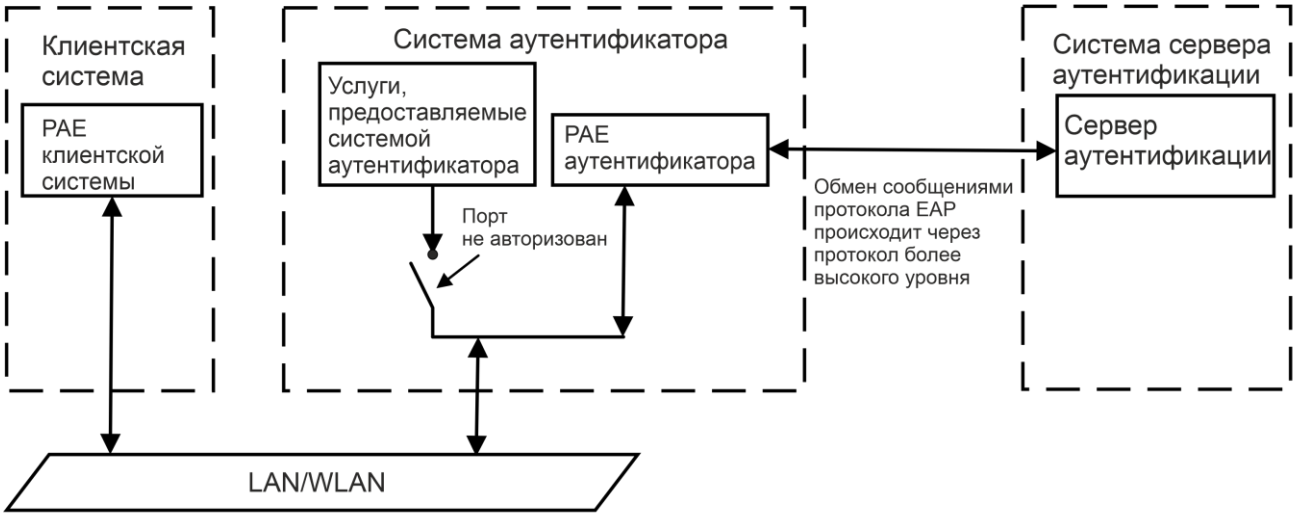


Рисунок 38-1. Структура системы аутентификации протокола 802.1x

- Клиентская система представляет собой объект на одном конце сегмента LAN. Она требует аутентификации от устройства контроля доступа на другом конце линии. Клиентская система — это, как правило, терминальное устройство пользователя. Аутентификация 802.1x начинается при запуске программного обеспечения клиентской системы. Клиентская система должна поддерживать EAPOL (расширяемый протокол аутентификации по сети LAN).
- Аутентификатор — это еще один объект на конце сегмента LAN, выполняющий аутентификацию подключенных клиентских систем. Аутентификатор, как правило, представляет собой сетевое устройство, которое поддерживает протокол 802.1x и предоставляет клиентским системам порты для доступа в сеть LAN. Эти порты могут быть либо физическими, либо логическими.
- Сервер аутентификации — это объект, который предоставляет аутентификаторам службу аутентификации. Сервер используется для аутентификации и авторизации пользователей, а также для учета и обычно представляет собой сервер RADIUS (служба удаленной аутентификации дозванивающихся пользователей). На нем можно хранить данные пользователей, включая имя пользователя, пароль и прочие параметры, такие как сеть VLAN и порты, к которым принадлежит пользователь.

Три вышеперечисленных объекта имеют дело со следующими ключевыми понятиями: PAE порта, управляемые порты и контроль направления.

38.1.1.1. PAE

PAE (объект доступа к порту) — это объект, с помощью которого реализуется работа алгоритмов и протоколов.

- PAE клиентской системы должен отправить ответ на запрос аутентификации от аутентификатора и предоставить ему информацию аутентификации пользователя. Кроме того, он может отправлять аутентификатору запросы аутентификации и автономные запросы.
- Через сервер аутентификации PAE-аутентификатора выполняет аутентификацию клиентских систем, которым требуется доступ к сети LAN, и после этого решает вопросы, связанные с результатом аутентификации управляемого порта (опознанный/неопознанный порт). Если порт опознан, пользователю разрешен доступ к сетевым ресурсам. Если порт не опознан, можно получать и отправлять только сообщения EAPOL, а доступ к сетевым ресурсам пользователю запрещен.

38.1.1.2. Управляемые/неуправляемые порты

Аутентификатор предоставляет клиентским системам порты для доступа в сеть LAN. Эти порты можно разделить на два логических типа: управляемые и неуправляемые.

- Неуправляемый порт всегда находится в состоянии двунаправленного соединения и используется главным образом для передачи кадров протокола EAPOL. Таким образом, клиентские системы всегда могут отправлять и получать сообщения аутентификации.
- Управляемый порт находится в состоянии соединения и аутентифицирован для передачи служебных сообщений. Если аутентификация не пройдена, принимать сообщения от клиентских систем запрещено.
- Управляемый и неуправляемый порты представляют собой две части одного порта. Это означает, что все кадры, попадающие на порт, видны на обоих портах.

38.1.1.3. Контроль направления

Пока управляемый порт не опознан, ему можно настроить как одно-, так и двунаправленное состояние соединения.

Если порт находится в состоянии двунаправленного соединения, запрещено как отправлять, так и получать любые кадры.

Если порт находится в состоянии однонаправленного соединения, получать кадры от клиентских систем запрещено, однако отправлять им кадры можно.

ПРИМЕЧАНИЕ: в настоящее время коммутаторы данного типа поддерживают только однонаправленное соединение.

38.1.2. Механизм работы протокола 802.1x

Для обмена информацией аутентификации между клиентской системой, аутентификатором и сервером аутентификации система аутентификации IEEE 802.1x использует EAP (расширяемый протокол аутентификации).

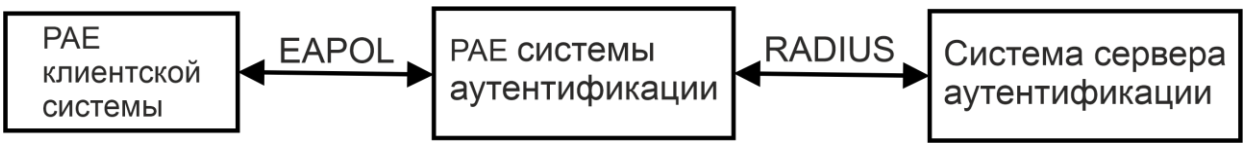


Рисунок 38-2. Механизм работы протокола 802.1x

- В сети LAN-сообщения EAP между PAE-клиентской системы и PAE-аутентификатора необходимо инкапсулировать в формат EAPOL.
- Существует два способа обмена данными между аутентификатором и сервером RADIUS. Первый способ заключается в инкапсуляции сообщений EAP в формат EAPOR (EAP over RADIUS) протокола RADIUS. При другом способе сообщения EAP оканчиваются PAE-аутентификатора, а для взаимодействия с сервером RADIUS при аутентификации используются сообщения, содержащие атрибуты PAP (протокол аутентификации по паролю) или CHAP (протокол аутентификации с предварительным согласованием вызова).
- Когда пользователь проходит аутентификацию, сервер аутентификации отправляет аутентификатору его данные. На основе результата аутентификации от сервера RADIUS PAE аутентификатора принимает решение о назначении порту состояния опознан/не опознан.

38.1.3. Инкапсуляция сообщений EAPOL

38.1.3.1. Формат пакетов данных EAPOL

EAPOL — это формат инкапсуляции сообщений, определенный в протоколе 802.1x. Он используется в основном для обмена сообщениями EAP между клиентской системой и аутентификатором, благодаря чему в сети LAN возможна передача этих сообщений. Формат пакета EAPOL в сетях IEEE 802/Ethernet LAN показан на рисунке ниже. В кадрах MAC-пакет EAPOL начинается с поля Тип/Размер.

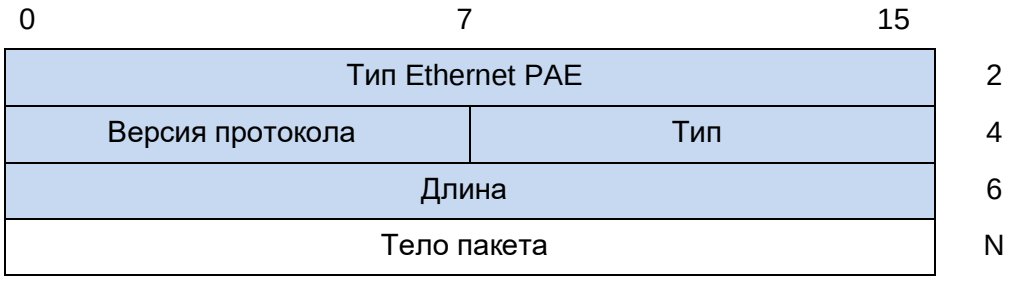


Рисунок 38-3. Формат пакета данных EAPOL

Тип PAE Ethernet: тип протокола, значение — 0x888E.

Версия протокола: версия протокола, поддерживаемая отправителем пакетов данных EAPOL.

Тип: тип пакетов данных EAPOL, включая:

- EAP-Packet (значение 0x00): кадр информации аутентификации, используется для переноса сообщений EAP. Кадр такого типа проходит через аутентификатор и выполняет обмен сообщениями EAP между клиентской системой и сервером аутентификации.
- EAPOL-Start (значение 0x01): кадр, который инициирует аутентификацию.
- EAPOL-Logoff (значение 0x02): кадр, который запрашивает отключение.
- EAPOL-Key (значение 0x03): кадр, содержащий ключевую информацию.
- EAPOL-Encapsulated-ASF-Alert (значение 0x04): используется для поддержки предупредительных сообщений ASF (Alert Standard Forum). Кадры такого типа используются для инкапсуляции данных сетевого управления, например, оповещений любых видов от конечных устройств.

Размер: размер данных, т. е. размер «тела пакета» в байтах. Если размер равен 0, следующие поля данных отсутствуют.

Тело пакета: содержание данных, форматы которых зависят от разных типов кадра.

38.1.3.2. Формат пакетов данных EAP

Если в поле «Тип» пакета EAPOL стоит EAP-Packet, тело пакета находится в формате EAP (см. рис. ниже).

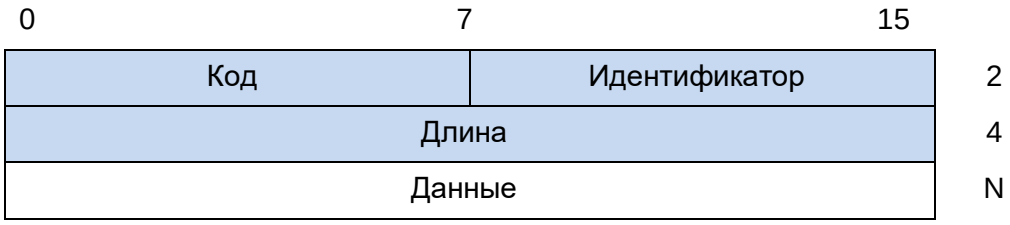


Рисунок 38-4. Формат пакетов данных EAP

Код: указывает тип пакета EAP. Всего существует четыре типа: запрос (1), отклик (2), успех (3), отказ (4).

- В пакетах типа «Успех» или «Отказ» отсутствует поле «Данные», а значение поля «Размер» равно 4.

- Формат поля «Данные» в пакетах типа «Запрос» и «Отклик» показан на следующем рисунке. Тип — тип аутентификации EAP. Содержание поля «Данные типа» зависит от типа. Например, если значение типа равно 1, это означает идентификатор, и выполняется запрос идентификатора другой стороны. Если тип равен 4, это означает MD5-Challenge, например, протокол PPP CHAP; содержит запросы.

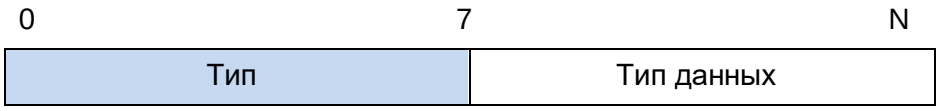


Рисунок 38-5. Формат поля «Данные» в пакетах типа

«Запрос» и «Отклик» Идентификатор: помогает сопоставлять запросы и отклики.

Размер: размер пакета EAP. Сюда входят поля «Код», «Идентификатор», «Размер» и «Данные» в байтах.

Данные: содержание пакета EAP, зависит от типа кода.

38.1.4. Инкапсуляция атрибутов EAP

Для поддержки аутентификации EAP сервер RADIUS добавляет два атрибута: EAP-сообщение и удостоверение сообщения. Посмотреть формат сообщений RADIUS можно во введении в работу протокола RADIUS в главе «Работа AAA-RADIUS-HWTACACS».

38.1.4.1. EAP-сообщение

Как показано на следующем рисунке, этот атрибут используется для инкапсуляции пакета EAP; код типа 79. Строка не должна быть длиннее 253 байт. Если размер данных в пакете EAP превышает 253 байта, этот пакет разделяется на фрагменты, которые затем в порядке следования инкапсулируются в несколько EAP-сообщений.

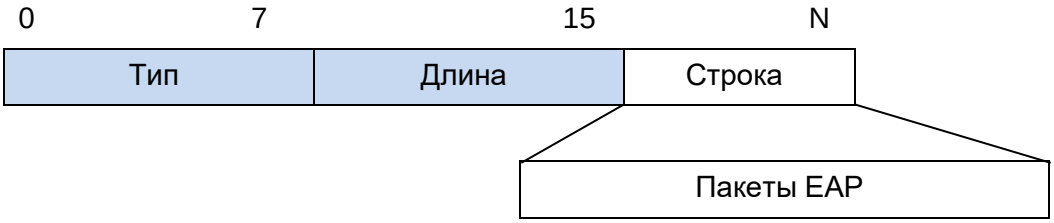


Рисунок 38-6. Инкапсуляция EAP-сообщения

38.1.4.2. Удостоверение сообщения

Как показано на следующем рисунке, этот атрибут применяется при использовании таких методов аутентификации, как EAP и CHAP, для предотвращения перехвата пакетов, запрашивающих доступ. Необходимо включать удостоверение сообщения в пакеты, содержащие EAP-сообщение. В противном случае пакеты будут сбрасываться как недействительные.

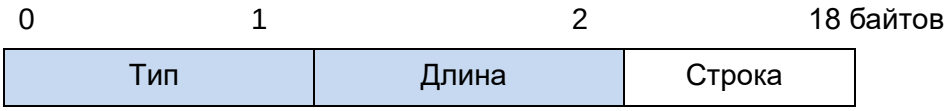


Рисунок 38-7. Удостоверение сообщения

38.1.5. Методы аутентификации 802.1x

Инициировать аутентификацию может как клиентская система, так и устройства. При обнаружении неопознанных пользователей, желающих получить доступ в сеть, устройство отправляет клиентской системе EAP-запрос/запрос идентификатора, после чего начинается аутентификация. С другой стороны, клиентская система может отправить устройству сообщение EAPOL-Start через клиентское программное обеспечение.

Для выполнения аутентификации через удаленный сервер RADIUS системы 802.1x поддерживают два метода: метод ретрансляции EAP и прерывающий метод EAP. Ниже описываются оба этих метода; процесс аутентификации инициирует клиентская система.

38.1.5.1. Режим ретрансляции EAP

В соответствии со стандартом IEEE 802.1x ретрансляция EAP предназначена для переноса EAP в таких протоколах верхнего уровня, как EAP через RADIUS. Таким образом, гарантируется прибытие сообщений расширяемого протокола аутентификации на сервер аутентификации через сложные сети. Как правило, для ретрансляции EAP требуется, чтобы сервер RADIUS поддерживал атрибуты EAP: EAP-сообщение и удостоверение сообщения.

EAP представляет собой скорее распространенный фреймворк аутентификации для передачи реального протокола, чем специальный механизм аутентификации. EAP предоставляет некоторые общие функции и позволяет использовать механизмы аутентификации, которые ожидаются при согласовании и носят название методов EAP. Преимущество EAP состоит в том, что механизм EAP является базовым и не требует настройки при появлении новых протоколов аутентификации. На следующем рисунке показан стек протокола метода аутентификации EAP.

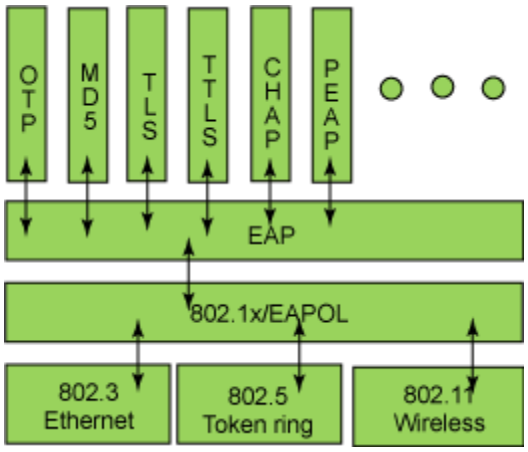


Рисунок 38-8. Стек протокола метода аутентификации EAP

В настоящее время разработано более 50 методов аутентификации EAP. Они отличаются механизмом аутентификации и управлением ключами. Ниже перечислены четыре самых популярных метода аутентификации EAP:

- EAP-MD5;

- EAP-TLS (безопасность транспортного уровня);
- EAP-TTLS (безопасность транспортного уровня через туннель);
- PEAP (защищенный расширяемый протокол аутентификации).

О них подробно рассказывается в следующей части руководства.

ПРИМЕЧАНИЕ:

Поскольку коммутатор представляет собой устройство контроля доступа к сквозной передаче данных и не проверяет содержание конкретного метода EAP, он поддерживает все вышеперечисленные методы EAP, а также любые методы аутентификации EAP, которые могут появиться в дальнейшем.

Какой бы метод ни применялся при ретрансляции EAP — EAP-MD5, EAP-TLS, EAPTTLS или PEAP, методы аутентификации клиентской системы и сервера RADIUS должны совпадать.

38.1.6. 1. Метод аутентификации EAP-MD5

EAP-MD5 — это открытый стандарт IETF, предоставляющий самый низкий уровень безопасности, так как хеш-функция MD5 подвержена словарным атакам.

На следующем рисунке показаны основные операции при работе метода аутентификации EAP-MD5.

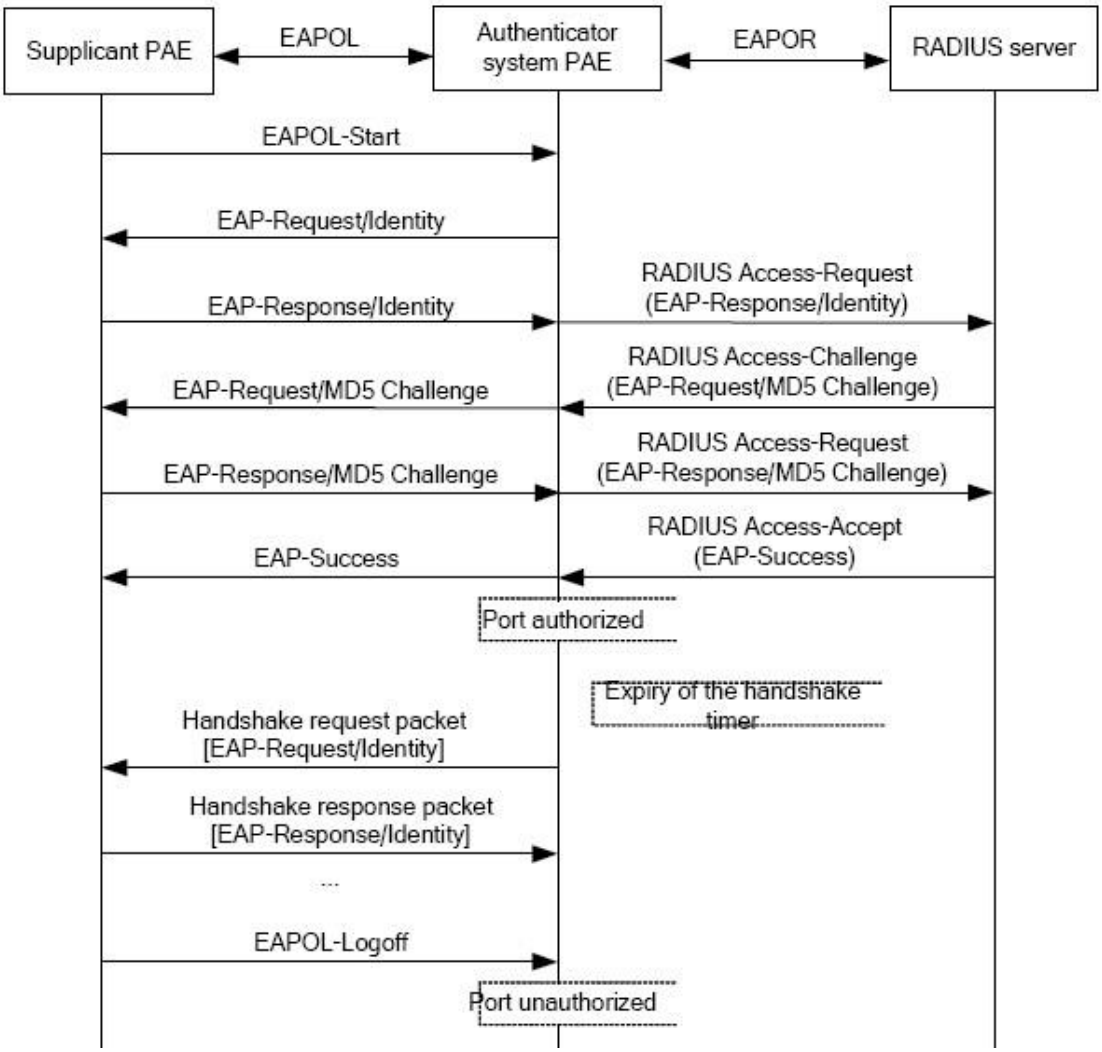


Рисунок 38-9. Поток аутентификации 802.1x EAP-MD5

38.1.7. Метод аутентификации EAP-TLS

EAP-TLS, предложенный компанией Microsoft, основан на протоколах EAP и TLS. Для того чтобы защитить аутентификацию идентификатора между клиентской системой и сервером RADIUS, он использует PKI и динамически формируемые сеансовые ключи. Как клиентская система, так и сервер RADIUS должны обладать цифровым сертификатом, чтобы можно было выполнить взаимную аутентификацию. Это самый ранний метод аутентификации EAP, используемый в беспроводных локальных сетях. Поскольку у всех пользователей должны быть цифровые сертификаты, а это создает сложности при обслуживании, метод редко используется на практике. Однако он по-прежнему является одним из наиболее безопасных стандартов EAP и поддерживается практически всеми поставщиками беспроводного оборудования и ПО.

На следующем рисунке показаны основные операции при работе метода аутентификации EAP-TLS.

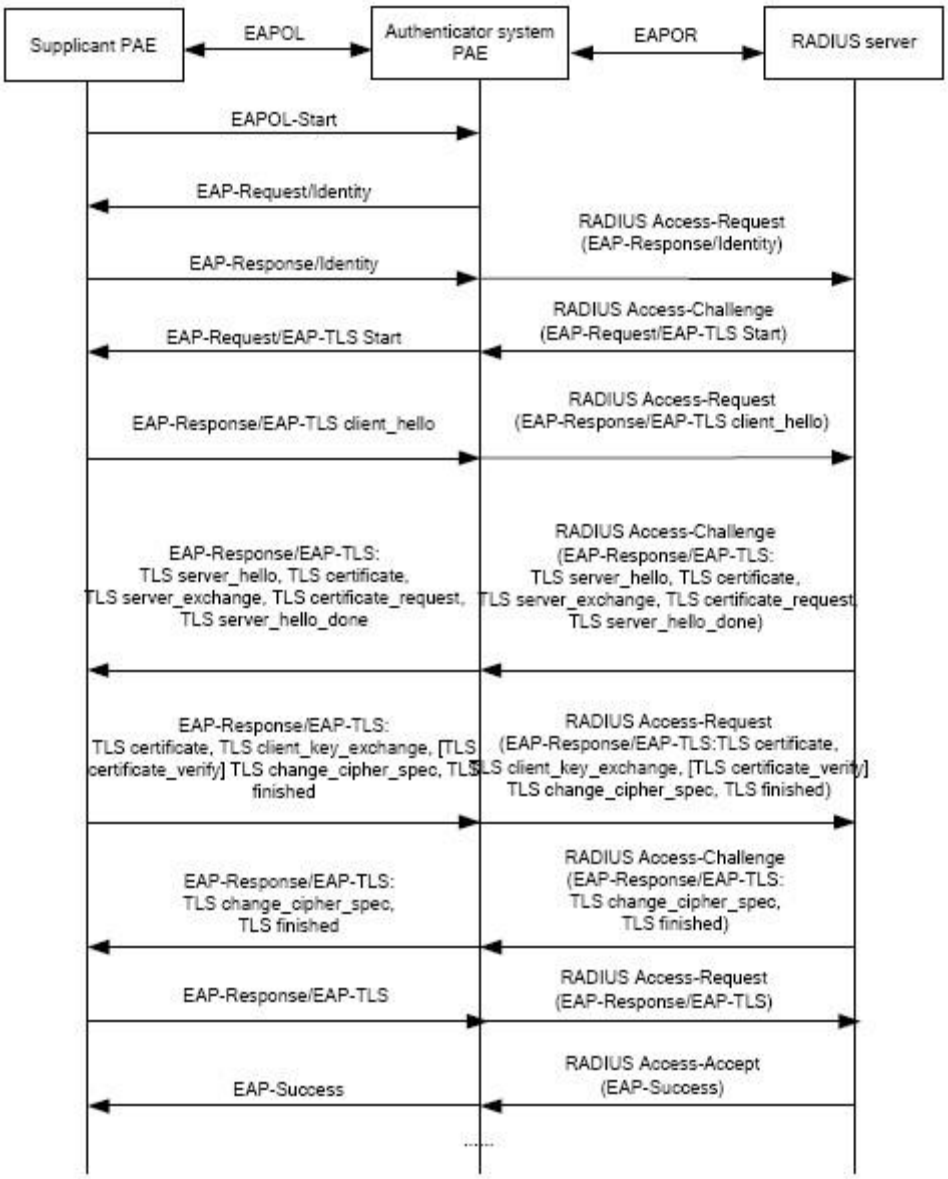


Рисунок 38-10. Поток аутентификации 802.1x EAP-TLS

38.1.8. Метод аутентификации EAP-TTLS

EAP-TTLS разработан совместно компаниями Funk Software и Certicom. Он предоставляет почти настолько же надежную аутентификацию, как и EAP-TLS, но при этом пользователям необязательно обладать собственным цифровым сертификатом. Единственное требование состоит в том, что у сервера RADIUS должен быть цифровой сертификат. Аутентификация пользователей реализуется посредством передачи паролей по защищенному туннелю, который устанавливается с помощью сертификата сервера аутентификации. Туннели TTLS позволяют передавать запросы аутентификации любых типов, включая EAP, PAP и MS-CHAPV2.

38.1.9. Метод аутентификации PEAP

EAP-PEAP разработан компаниями Cisco, Microsoft и RAS Security в качестве открытого стандарта, рекомендуемого к использованию. Он применяется давно и обеспечивает высокий уровень безопасности. Устройство протокола и схема защиты имеют много общего с методом EAP-TTLS: используется сертификат сервера PKI для установки защищенного туннеля TLS и, таким образом, обеспечивается безопасность при аутентификации пользователей.

На следующем рисунке показаны основные операции при работе метода аутентификации PEAP.

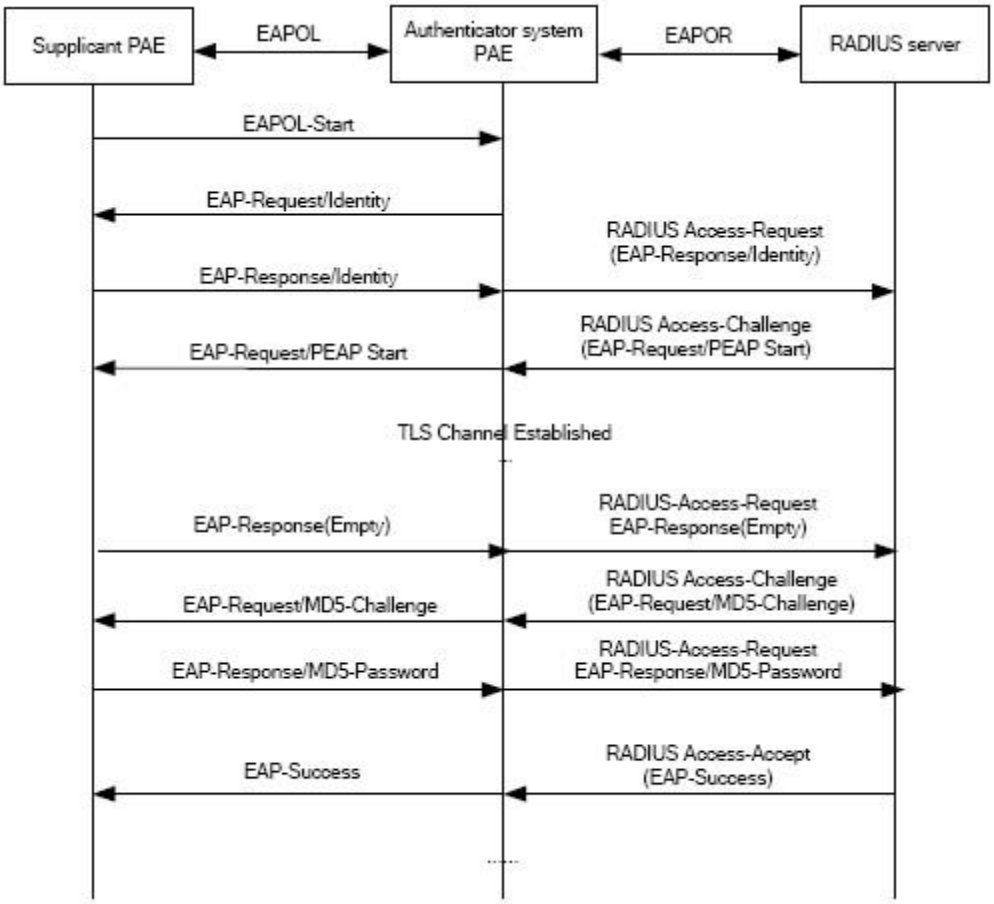


Рисунок 38-11. Поток аутентификации 802.1x PEAP

38.1.9.1. Прерывающий режим EAP

В данном режиме сообщения EAP прерываются на устройстве контроля доступа и преобразуются в сообщения RADIUS. Это позволяет реализовать аутентификацию, авторизацию и учет. На следующем рисунке показаны основные операции.

В прерывающем режиме EAP-устройство контроля доступа и сервер RADIUS могут использовать методы аутентификации PAP или CHAP. На следующем рисунке показаны основные операции при работе метода аутентификации CHAP.

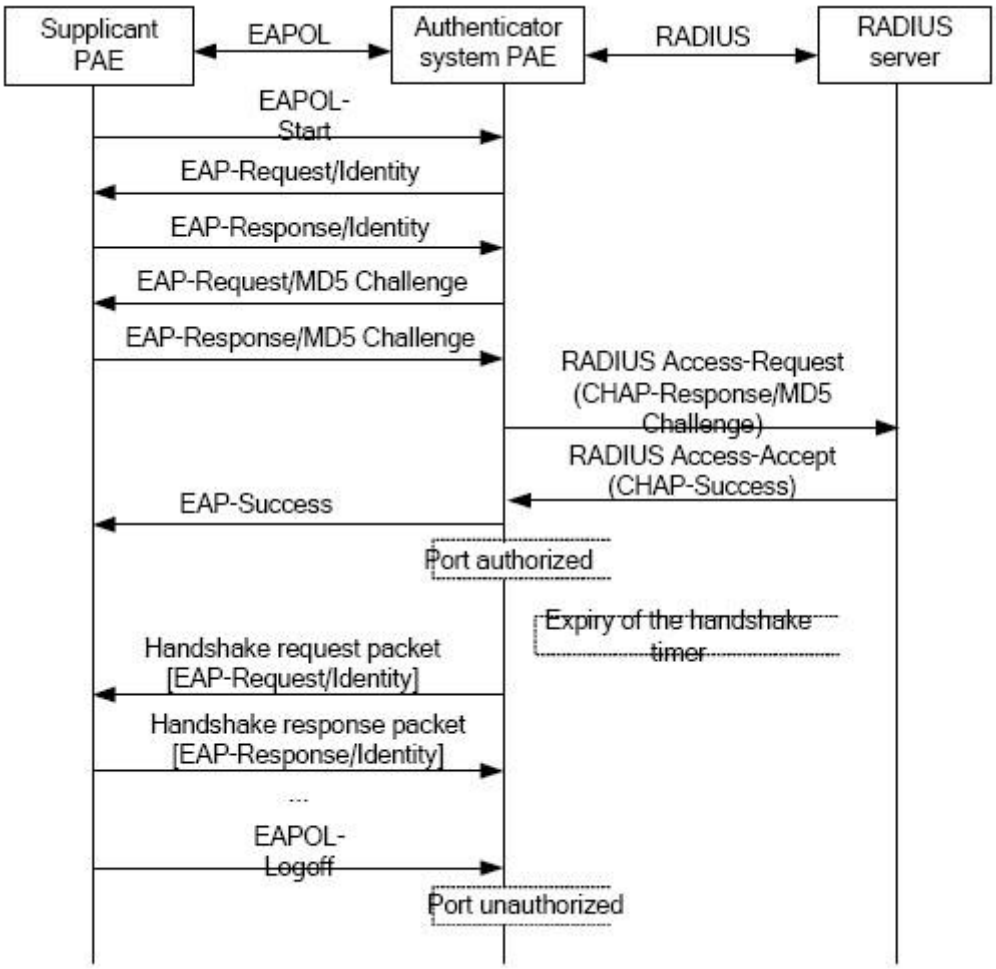


Рисунок 38-12. Поток аутентификации 802.1x прерывающего режима EAP

38.1.10. Расширение и оптимизация протокола 802.1x

Устройства не только поддерживают указанные протоколом методы аутентификации на уровне портов, но также расширяют и оптимизируют их при применении режима ретрансляции EAP и прерывающего режима EAP 802.1x.

- Поддержка некоторых приложений, в связи с которыми у одного физического порта может быть несколько пользователей.
- Существует три метода контроля доступа (аутентификации пользователей): на уровне портов, на уровне MAC-адресов и на уровне пользователей (IP-адрес + MAC-адрес + порт).

- При использовании метода на уровне портов все пользователи получают доступ к сетевым ресурсам сразу после того, как первый пользователь порта проходит аутентификацию. Аутентификация остальных пользователей не проводится.

Однако после выхода первого пользователя из сети остальные пользователи теряют доступ к ней.

- При использовании метода на уровне MAC-адресов все пользователи, запрашивающие доступ, должны пройти аутентификацию. Доступ к сети получают только те, аутентификация которых прошла успешно. Если один пользователь выходит из сети, на остальных это никак не влияет.
- При использовании метода на уровне пользователей (IP-адрес + MAC-адрес + порт) еще до аутентификации всем пользователям доступны ограниченные ресурсы. В данном методе существует два типа контроля: стандартный и расширенный. Стандартный контроль на уровне пользователей не ограничивает доступ к ресурсам. Это означает, что до выполнения аутентификации ограниченные ресурсы доступны всем пользователям порта. Расширенный контроль на уровне пользователей запрещает доступ к ограниченным ресурсам. Это означает, что до выполнения аутентификации ограниченные ресурсы доступны только некоторым пользователям порта. После выполнения аутентификации эти пользователи получают доступ ко всем ресурсам.

ПРИМЕЧАНИЕ: когда используются частные клиентские системы, рекомендуется применять расширенный контроль на уровне пользователей, поскольку это позволяет эффективно предотвращать ARP Cheat.

Максимальное число пользователей, прошедших аутентификацию, равно 4000. Однако предпочтительно, чтобы количество пользователей не превышало 2000.

38.1.11. Функции распределения сетей VLAN

38.1.11.1. Auto VLAN

Функция Auto VLAN позволяет серверу RADIUS на основе данных о пользователе и пользовательском устройстве доступа изменять сеть VLAN, к которой принадлежит порт доступа. Когда пользователь 802.1x проходит аутентификацию на сервере, сервер RADIUS отправляет устройству информацию авторизации. Если на сервере RADIUS включена функция назначения VLAN, то в сообщения «Доступ разрешен» необходимо включить следующие атрибуты:

- Tunnel-Type = VLAN (13);
- Tunnel-Medium-Type = 802 (6);
- Tunnel-Private-Group-ID = VLANID.

VLANID здесь означает VID сети VLAN; значение находится в диапазоне от 1 до 4094. Например, если Tunnel-Private-Group-ID = 30, то это сеть VLAN 30.

Когда коммутатор получает информацию о назначенной сети VLAN, текущий порт доступа покидает VLAN, заданную пользователем, и присоединяется к Auto VLAN.

Auto VLAN не изменяет конфигурацию порта и не влияет на нее. Однако, Auto VLAN обладает более высоким приоритетом, чем VLAN, заданная пользователем. Это означает, что после завершения аутентификации начинает действовать именно Auto VLAN, в то время как VLAN, заданная пользователем, не работает, пока пользователь не выйдет из сети.

ПРИМЕЧАНИЕ: в настоящее время Auto VLAN можно использовать только в режиме контроля доступа на уровне портов и только на портах с типом канала Access.

38.1.11.2. Guest VLAN

Функция Guest VLAN применяется для предоставления пользователям, не прошедшим аутентификацию, доступа к некоторым конкретным ресурсам.

До выполнения проверки подлинности 802.1x порт аутентификации пользователей принадлежит к сети VLAN по умолчанию (Guest VLAN) и обладает правом доступа к ресурсам этой VLAN без аутентификации. Однако ресурсы других сетей недоступны. После аутентификации порт покидает Guest VLAN, а пользователь получает доступ к ресурсам других сетей.

Находясь в сети Guest VLAN, пользователи могут работать с ПО клиентской системы 802.1x, а также обновлять это ПО или некоторые другие приложения, например, антивирусное ПО или исправления операционной системы. Если в течение определенного промежутка времени из-за отсутствия клиентов или слишком низкой версии клиентской системы никто не проходит аутентификацию, устройство доступа добавляет порт в сеть Guest VLAN.

При условии, что функция 802.1x включена, а сеть Guest VLAN правильно настроена, порт добавляется в Guest VLAN таким же образом, как в Auto VLAN, если ответ от клиента не получен, а количество отправленных устройством сообщений, инициирующих аутентификацию, превышает верхний предел (EAP-запрос/запрос идентификации).

- Сервер аутентификации назначает Auto VLAN, после чего порт покидает Guest VLAN и присоединяется к назначенной Auto VLAN. После выхода пользователя из сети порт снова назначается указанной Guest VLAN.
- Сервер аутентификации назначает Auto VLAN, после чего порт покидает Guest VLAN и присоединяется к указанной VLAN. После выхода пользователя из сети порт снова назначается указанной Guest VLAN.

38.2. Список задач по настройке 802.1x

1. Включить функцию IEEE 802.1x.
2. Получить доступ к настройкам параметров блока управления.
   2.1. Настроить на порте метод управления доступом: на уровне MAC-адресов или на уровне портов.
   2.2. Настроить расширенную функцию 802.1x.
3. Настроить параметры пользовательских устройств доступа (необязательно).

1. Включить функцию 802.1x.

Команда	Описание
Режим общих настроек	
dot1x enable no dot1x enable	Включает на коммутаторе и портах функцию 802.1x. Команда, начинающаяся со слова «no», отключает эту функцию
dot1x privateclient enable no dot1x privateclient enable	Включает функцию принудительного использования клиентским ПО формата сообщений аутентификации 802.1x. Команда, начинающаяся со слова «no», отключает эту функцию

Команда	Описание
dot1x user free-resource <prefix> <mask> no dot1x user free-resource	Задает ограниченные сетевые ресурсы, которые могут быть доступны пользователям dot1x до аутентификации. Команда, начинающаяся со слова «no», удаляет ресурсы
dot1x unicast enable no dot1x unicast enable	Включает на коммутаторе функцию одноадресной сквозной передачи данных 802.1x. Команда, начинающаяся со слова «no», отключает эту функцию

2. Настройка параметров блока управления.

2.1. Настройка метода доступа к порту.

Команда	Описание
Режим настроек порта	
dot1x port-method {macbased | portbased | userbased {standard | advanced}} no dot1x port-method	Задает на порте метод управления доступом. Команда, начинающаяся со слова «no», восстанавливает управление доступом на уровне MAC-адресов
dot1x max-user macbased <number> no dot1x max-user macbased	Задает максимальное количество пользователей, которым разрешен доступ к указанному порту. Команда, начинающаяся со слова «no», восстанавливает настройки по умолчанию (доступ разрешен одному пользователю)
dot1x max-user userbased <number> no dot1x max-user userbased	Задает указанному порту сеть Guest VLAN. Команда, начинающаяся со слова «no», удаляет заданную сеть
dot1x guest-vlan <vlanID> no dot1x guest-vlan	Включает на коммутаторе функцию одноадресной сквозной передачи данных 802.1x. Команда, начинающаяся со слова «no», отключает эту функцию
dot1x portbased mode single-mode no dot1x portbased mode single-mode	Устанавливает одномодовый режим на основе режима аутентификации на уровне портов. Команда, начинающаяся со слова «no», отключает эту функцию

2.2. Настроить расширенную функцию 802.1x.

Команда	Описание
Режим общих настроек	
dot1x macfilter enable no dot1x macfilter enable	Включает на коммутаторе функцию фильтрации адресов 802.1x. Команда, начинающаяся со слова «no», отключает эту функцию
dot1x macbased port-down-flush no dot1x macbased port-down-flush	Используется для удаления пользователя, прошедшего сертификацию на порте, когда, согласно MAC-адресу, сертификация dot1x не работает. Команда, начинающаяся со слова «no», не выполняет операцию
dot1x accept-mac <mac-address> [interface <interface-name>] no dot1x accept-mac <mac-address> [interface <interface-name>]	Добавляет запись в таблицу фильтрации адресов 802.1x. Команда, начинающаяся со слова «no», удаляет записи из таблицы
dot1x eapor enable no dot1x eapor enable	Включает на коммутаторе функцию аутентификации с помощью метода ретрансляции EAP. Команда, начинающаяся со слова «no», устанавливает локальную аутентификацию EAP

3. Настроить параметры клиента.

Команда	Описание
Режим общих настроек	
dot1x max-req <count> no dot1x max-req	Задает число запросов EAP/кадров MD5, посылаемых перед тем, как коммутатор повторно инициирует аутентификацию при неполучении ответа от клиента. Команда, начинающаяся со слова «no», восстанавливает настройки по умолчанию
dot1x re-authentication no dot1x re-authentication	Включает периодическую аутентификацию клиента. Команда, начинающаяся со слова «no», отключает эту функцию

Команда	Описание
dot1x timeout quiet-period <seconds> no dot1x timeout quiet-period	Задает время бездействия порта при сбое аутентификации. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию
dot1x timeout re-authperiod <seconds> no dot1x timeout re-authperiod	Задает интервал времени, по истечении которого выполняется повторная аутентификация клиента. Команда, начинающаяся со слова «no», восстанавливает настройки по умолчанию
dot1x timeout tx-period <seconds> no dot1x timeout tx-period	Задает интервал времени, по истечении которого клиент повторно отправляет запрос/кадр идентификатора EAP. Команда, начинающаяся со слова «no», восстанавливает настройки по умолчанию
dot1x re-authenticate [interface <interface-name>]	Включает на всех портах или на указанном порте повторную аутентификацию IEEE 802.1x (тайм-аут ожидания не требуется)

38.3. Примеры использования 802.1x

38.3.1. Примеры использования Guest VLAN

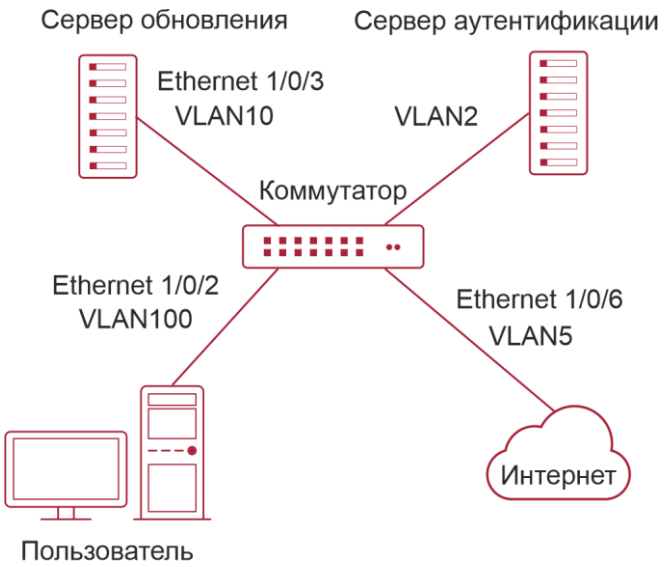


Рисунок 38-13. Топология сети Guest VLAN

ПРИМЕЧАНИЕ: на всех рисунках в данном разделе E2 означает Ethernet 1/0/2, E3 — Ethernet 1/0/3, а E6 — Ethernet 1/0/6.

Как показано на рисунке ниже, коммутатор получает доступ в сеть с помощью аутентификации 802.1x, используя в качестве сервера аутентификации сервер RADIUS. Ethernet1/0/2, порт, через который пользователь получает доступ к коммутатору, принадлежит сети VLAN100. Сервер аутентификации находится в сети VLAN2. Сервер обновления, находящийся в сети VLAN10, используется пользователями для загрузки и обновления ПО клиентской системы. Ethernet1/6 — порт, через который коммутатор получает доступ в сеть VLAN5.

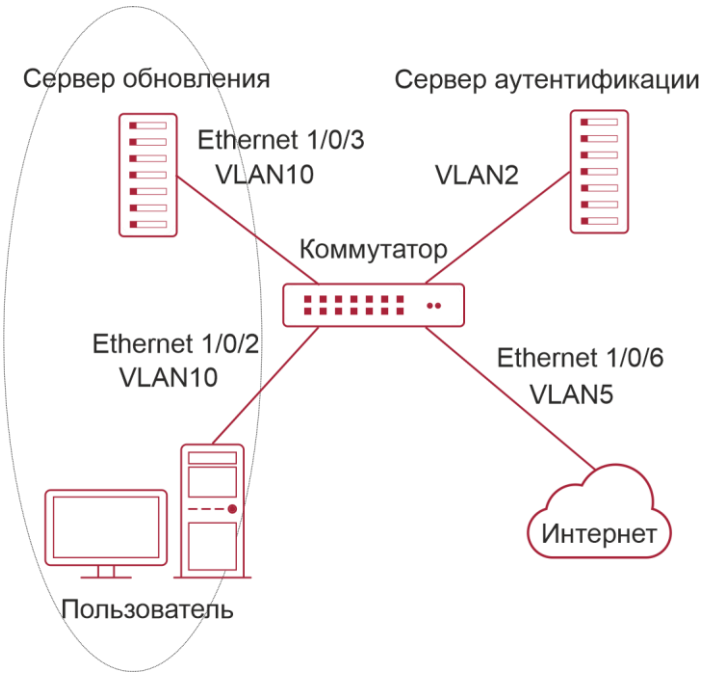


Рисунок 38-14. Пользователь присоединяется к сети Guest VLAN

Как показано на рисунке выше, на порте коммутатора Ethernet1/0/2 включена функция 802.1x, а сеть VLAN10 задана в качестве Guest VLAN-порта. Прежде чем пользователь проходит аутентификацию или в случае, если ему не удается ее пройти, порт Ethernet1/0/2 добавляется в сеть VLAN10, чтобы предоставить пользователю доступ к серверу обновления.

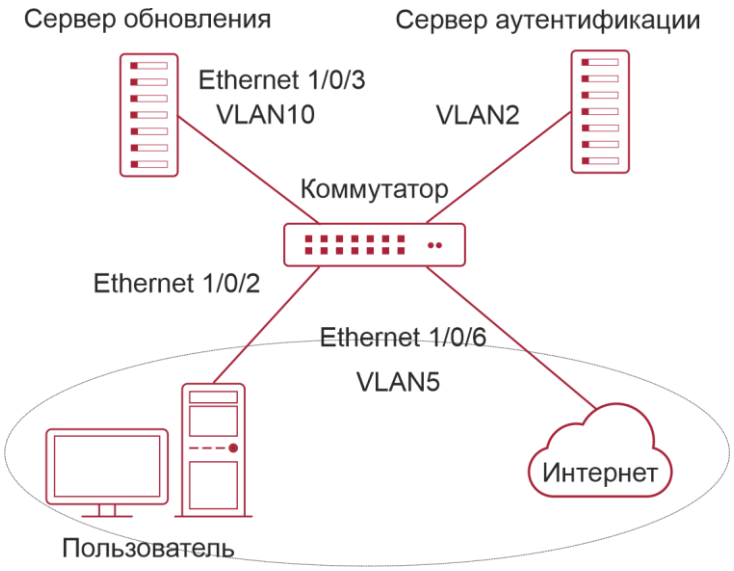


Рисунок 38-15. Пользователь в сети, VLAN отключена

Как показано на рисунке выше, когда пользователь после успешной аутентификации входит в сеть, сервер аутентификации назначает VLAN5. Таким образом, как пользователь, так и порт Ethernet1/0/6 оказываются в сети VLAN5, а пользователь получает доступ в Интернет.

Ниже приведены этапы настройки:

```
# Configure RADIUS server.
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable

# Create VLAN100.
Switch(config)#vlan 100

# Enable the global 802.1x function
Switch(config)#dot1x enable

# Enable the 802.1x function on port Ethernet1/0/2
Switch(config)#interface ethernet1/0/2
Switch(Config-If-Ethernet1/0/2)#dot1x enable

# Set the link type of the port as access mode.
```

```
Switch(Config-If-Ethernet1/0/2)#switch-port mode access

# Set the access control mode on the port as portbased.
Switch(Config-If-Ethernet1/0/2)#dot1x port-method portbased

# Set the port's Guest VLAN as 100.
Switch(Config-If-Ethernet1/0/2)#dot1x guest-vlan 100
Switch(Config-If-Ethernet1/0/2)#exit
```

Пользователи могут проверить конфигурацию сети Guest VLAN с помощью команд «show running-config» или «show interface ethernet1/0/2». Если в сети нет пользователей, отсутствуют пользователи, не прошедшие аутентификацию, или никому из пользователей не удается успешно выйти из сети, а количество сообщений, инициирующих аутентификацию (запрос EAP/запрос идентификации), превышает заданный верхний предел, пользователи могут проверить, работает ли настроенная на порте Guest VLAN, с помощью команды «show vlan id 100».

38.3.2. Пример использования IPv4 RADIUS

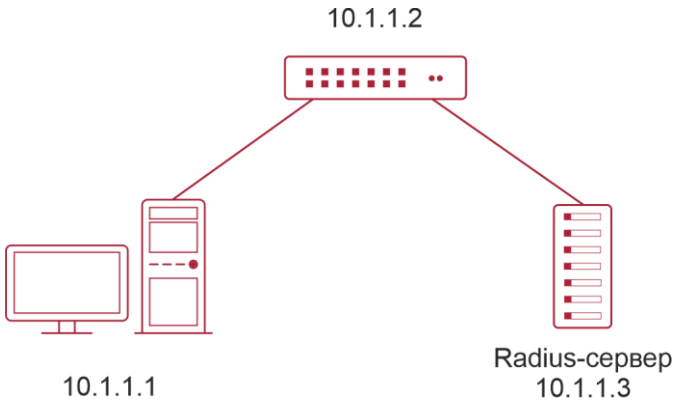


Рисунок 38-16. Пример топологии IEEE 802.1x

ПК подключен к порту 1/0/2 коммутатора. На порте 1/0/2 включена аутентификация IEEE 802.1x. По умолчанию выбран режим аутентификации на уровне MAC-адресов. IP-адрес коммутатора 10.1.1.2. Все порты, кроме 1/0/2, используются для связи с сервером аутентификации RADIUS, IP-адрес которого 10.1.1.3. Для аутентификации по умолчанию используется порт 1812, а для учета — 1813. Для выполнения аутентификации IEEE 802.1x на ПК установлено клиентское ПО. Ниже приведены этапы настройки:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
```

```
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/2
Switch(Config-Ethernet1/0/2)#dot1x enable
Switch(Config-Ethernet1/0/2)#exit
```

38.3.3. Пример использования IPv6 RADIUS

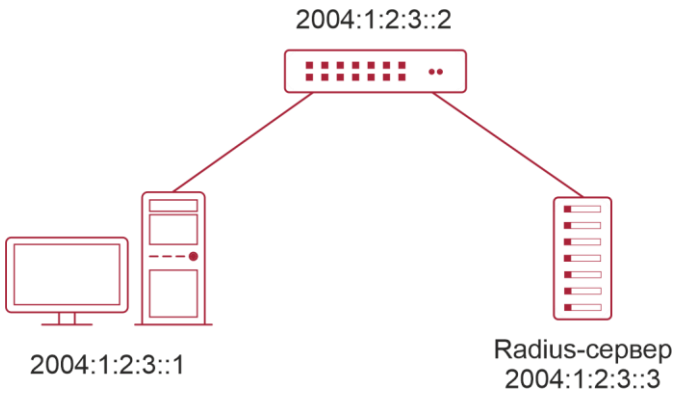


Рисунок 38-17. IPv6 Radius

Подключите компьютер к интерфейсу 1/0/2 коммутатора и на интерфейсе 1/2 включите IEEE 802.1x. Используйте аутентификацию на уровне MAC-адресов. Задайте коммутатору IP-адрес 2004:1:2:3::2 и подключите любой его интерфейс, кроме 1/0/2, к серверу аутентификации RADIUS. Задайте серверу RADIUS IP-адрес 2004:1:2:3::3. Для аутентификации и учета используйте порты по умолчанию 1812 и 1813 соответственно. Для выполнения аутентификации IEEE 802.1x установите на компьютер клиентское ПО.

Ниже приведены этапы настройки:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 2004:1:2:3::3
Switch(config)#radius-server accounting host 2004:1:2:3::3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#dot1x enable
Switch(Config-If-Ethernet1/0/2)#exit
```

38.4. Устранение неисправностей протокола 802.1x

Может возникнуть ситуация, при которой настройка 802.1x на портах выполнена и для аутентификации 802.1x задан режим auto (автоматически), но коммутатор не выполняет аутентификацию, после того как пользователь запускает клиентское ПО 802.1x. Ниже приведены возможные причины этого и предложены решения:

- Если на порте не удается включить 802.1x, следует убедиться, что отсутствует привязка к MAC-адресу и не используется агрегация портов. Для того чтобы включить аутентификацию 802.1x, необходимо отключить эти функции.
- Если коммутатор настроен правильно, но все равно не может выполнить аутентификацию, необходимо проверить соединение между коммутатором и сервером RADIUS, а также между коммутатором и клиентом 802.1x. Кроме того, следует проверить настройки порта и VLAN.
- Для поиска возможных причин используйте журнал регистрации событий сервера RADIUS. В этот журнал записываются не только безуспешные попытки входа в систему, но и их причины. Если из записей журнала следует, что пароль аутентификации неверен, необходимо изменить ключевой параметр сервера RADIUS. Если аутентификатора не существует, необходимо добавить его в сервер RADIUS. Если не существует пользователя с таким именем и паролем, необходимо проверить имя пользователя и пароль и ввести их еще раз.

39. НАСТРОЙКА ПРОТОКОЛА MRPP

39.1. Введение в протокол MRPP

MRPP (многоуровневый протокол защиты кольцевых сетей) — это протокол канального уровня, применяемый для защиты колец Ethernet. Он позволяет избегать широковещательных штормов, вызываемых петлями в кольце Ethernet, и восстанавливать соединение между узлами в кольцевой сети при разрыве связи в кольце Ethernet. MRPP представляет собой расширение протокола EAPS (протокол автоматического переключения на резерв канала Ethernet).

По функциональности MRPP похож на протокол STP. Ниже перечислены особенности MRPP:

1. MRPP используется в топологии Ethernet типа «кольцо».
2. Быстрая сходимость — меньше 1 с. В идеале может достигать 100 – 50 мс.

39.1.1. Концепция

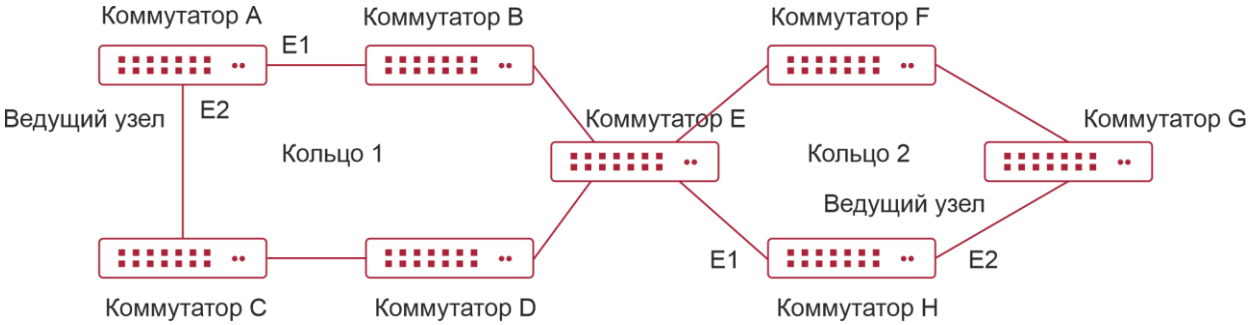


Рисунок 39-1. Схема протокола MRPP

39.1.1.1. Управляющая сеть VLAN

Управляющая сеть VLAN представляет собой виртуальную сеть, которая используется только для идентификации пакетов протокола MRPP, передаваемых по линии связи. Для того чтобы избежать путаницы, идентификаторы управляющей VLAN и других сетей VLAN должны различаться. Идентификаторы VLAN в разных MRPP-кольцах должны быть разными.

39.1.1.2. Кольцо Ethernet (MRPP-кольцо)

Топология Ethernet типа «кольцо».

У MRPP-колец существует два состояния:

Состояние работоспособности: отсутствуют разрывы физических линий связи в кольцевой сети.

Состояние разрыва: в кольцевой сети имеется разрыв одной или нескольких физических линий связи.

39.1.1.3. Узлы

Все коммутаторы носят те же названия, что и узлы Ethernet. Существует несколько типов узлов.

Первичный узел: имеется в каждом кольце; это основной узел, осуществляющий обнаружение и обеспечивающий безопасность.

Транспортный узел: в каждом кольце все узлы, кроме первичного, являются транспортными.

Роли узлов определяются пользовательскими настройками. Как показано на рис. 39-1, Коммутатор A — первичный узел Кольца 1. Коммутатор B, Коммутатор C; Коммутатор D и Коммутатор E — транспортные узлы Кольца 1.

39.1.1.4. Основной и дополнительный порты

Как у первичного, так и у транспортного узла есть два порта (основной и дополнительный), которые подключаются к Ethernet независимо друг от друга. Роли портов определяются пользовательскими настройками.

Основной и дополнительный порты первичного узла.

Основной порт первичного узла используется для отправки пакетов, содержащих запрос о работоспособности кольца (hello). Дополнительный порт используется для приема пакетов Hello, идущих от первичного узла. Если Ethernet находится в состоянии работоспособности, дополнительный порт первичного узла блокирует все пакеты, кроме MRPP-пакетов. Если Ethernet находится в состоянии разрыва, с дополнительного порта первичного узла снимается блокировка, и он перенаправляет пакеты данных. Основной и дополнительный порты транспортных узлов работают одинаково.

Роли портов определяются пользовательскими настройками. Из рис. 39-1 видно, что E1 — основной порт Коммутатора A, а E2 — дополнительный.

39.1.1.5. Таймер

При отправке и получении первичным узлом MRPP-пакета используются два таймера: Hello-таймер и Fail-таймер.

Hello-таймер задает период между отправкой основным портом первичного узла пакетов, содержащих запрос о работоспособности.

Fail-таймер задает дополнительное время, в течение которого дополнительный порт первичного узла получает пакеты, содержащие запрос о работоспособности. Значение Fail-таймера должно быть равно тройному значению Hello-таймера или превышать его.

39.1.2. Типы пакетов протокола MRPP

Тип пакета	Описание
Пакет Hello (пакет, содержащий запрос о работоспособности) Hello	Основной порт первичного узла вызывается для обнаружения кольца. Если дополнительный порт первичного узла получает пакет Hello в течение заданного дополнительного времени, кольцо находится в нормальном состоянии
LINK-DOWN (пакет события «Разрыв связи»)	При обнаружении на порте разрыва связи транспортный узел немедленно отправляет первичному узлу пакет LINK-DOWN и сообщает ему об отказе кольца

Тип пакета	Описание
Пакет LINK-DOWN-FLUSH_FDB	После обнаружения отказа кольца или получения пакета LINK-DOWN первичный узел снимает блокировку с дополнительного порта и использует два порта для отправки пакета, который сообщает транспортным узлам о необходимости обновления MAC-адресов
Пакет LINK-UP-FLUSH_FDB	После того как первичный узел обнаруживает, что отказавший участок кольца вернулся в рабочее состояние, и получает пакет от основного порта, он сообщает транспортным узлам о необходимости обновления MAC-адресов

39.1.3. Работа протокола MRPP

39.1.3.1. Сигнализация о разрыве связи

Когда транспортный узел обнаруживает, что порт MRPP-кольца, которому он принадлежит, не работает, то немедленно отправляет первичному узлу пакет LINKDOWN. Получив этот пакет, первичный узел немедленно снимает блокировку с дополнительного порта и отправляет всем транспортным узлам пакет LINK-DOWNFLUSH_FDB, который сообщает о необходимости обновить таблицу MAC-адресов.

39.1.3.2. Система опроса

Основной порт первичного узла рассылает соседям пакет Hello в соответствии с настройками Hello-таймера.

Если кольцо находится в рабочем состоянии, дополнительный порт первичного узла получает пакет Hello и остается заблокированным.

Если кольцо находится в состоянии разрыва, дополнительный порт первичного узла не принимает пакеты Hello в течение дополнительного времени. Первичный узел снимает блокировку с дополнительного порта и отправляет всем транспортным узлам пакет LINKDOWN-FLUSH_FDB, который сообщает о необходимости обновить таблицу MAC-адресов.

39.1.3.3. Восстановление кольца

Если после обнаружения первичным узлом отказа кольца дополнительный порт получает от него пакет Hello, значит, кольцо восстановлено. Одновременно первичный узел блокирует дополнительный порт и рассылает соседям пакет LINK-UP-FLUSH_FDB.

После того как порт MRPP-кольца сообщает транспортным узлам о смене состояния связи на UP, первичный узел спустя какое-то время обнаруживает, что кольцо восстановлено. В обычных сетях VLAN возможно формирование временной петли и появление широковещательного шторма. Чтобы избежать возникновения временной петли, транспортный узел обнаруживает ее и присоединяет к порту кольцевой сети для смены состояния связи на UP, после чего порт немедленно блокируется (пропускаются только пакеты управляющей сети VLAN). Блокировка снимается только после того, как от первичного узла приходит пакет LINK-UP-FLUSH_FDB.

39.2. Список задач по настройке MRPP

1. Глобально включить MRPP.
2. Настроить MRPP-кольцо.
3. Задать время запроса MRPP.
4. Настроить режим совместимости.
5. Вывести на экран и отладить данные MRPP.

1. Глобально включить MRPP.

Команда	Описание
Режим общих настроек	
mrpp enable no mrpp enable	Глобально включает и отключает MRPP

2. Настроить MRPP-кольцо.

Команда	Описание
Режим общих настроек	
mrpp ring <ring-id> no mrpp ring <ring-id>	Создает MRPP-кольцо. Команда, начинающаяся со слова «no», удаляет кольцо и его настройки
Режим MRPP-кольца	
control-vlan <vid> no control-vlan	Задает идентификатор управляющей сети VLAN. Команда, начинающаяся со слова «no», удаляет идентификатор
node-mode {master | transit}	Задает тип узла MRPP-кольца (первичный или транспортный)
hello-timer < timer> no hello-timer	Задает период между отправкой первичным узлом MRPP-кольца пакетов Hello. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию
fail-timer <timer> no fail-timer	Задает дополнительное время, в течение которого первичный узел MRPP-кольца отправляет пакеты Hello. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию

Команда	Описание
Режим конфигурирования порта	
mrpp ring <ring-id> primary-port {cos <cos>|} no mrpp ring <ring-id> primary-port	Указывает основной порт MRPP-кольца и значение COS в заголовках пакетов, отправляемых портом
mrpp ring <ring-id> secondary-port {cos <cos>|} no mrpp ring <ring-id> secondary-port	Указывает дополнительный порт MRPP-кольца и значение COS в заголовках пакетов, отправляемых портом

3. Задать время запроса MRPP.

Команда	Описание
Режим общих настроек	
mrpp poll-time <20-2000>	Задает интервал между запросами MRPP

4. Настроить режим совместимости.

Команда	Описание
Режим общих настроек	
mrpp errp compatible no mrpp errp compatible	Включает режим совместимости с протоколом ERRP. Команда, начинающаяся со слова «no», выключает режим совместимости
mrpp eaps compatible no mrpp eaps compatible	Включает режим совместимости с протоколом EAPS. Команда, начинающаяся со слова «no», выключает режим совместимости
errp domain <domain-id> no errp domain <domain-id>	Создает домен ERRP. Команда, начинающаяся со слова «no», удаляет домен

5. Вывести на экран и отладить данные MRPP.

Команда	Описание
Режим общих настроек	
debug mrpp no debug mrpp	Выводит на экран данные об отладке модуля MRPP. Команда, начинающаяся со слова «no», отключает вывод данных
show mrpp {<ring-id>}	Выводит на экран данные о настройках MRPP-кольца
show mrpp statistics {<ring-id>} clear mrpp statistics {<ring-id>}	Выводит на экран статистические данные о принятых MRPP-кольцом пакетах данных. Удаляет статистические данные о принятых MRPP-кольцом пакетах данных

39.3. Типичный сценарий применения протокола MRPP

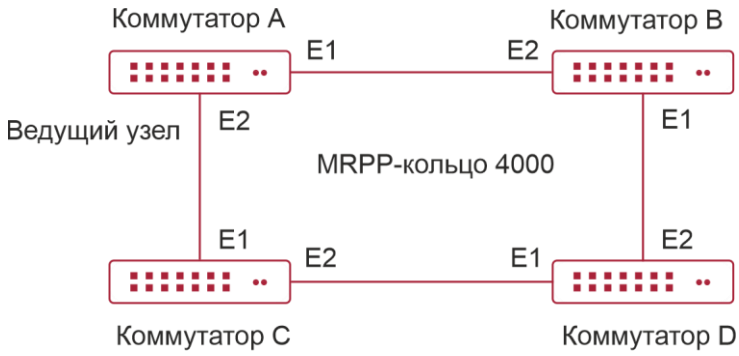


Рисунок 39-2. Типичный сценарий настройки протокола MRPP

Топология, показанная на рисунке выше, часто применяется при использовании протокола MRPP. Мультикоммутатор представляет собой одно MRPP-кольцо, все коммутаторы в котором настроены как MRPP-кольцо 4000.

В приведенной выше конфигурации первичным узлом MRPP-кольца 4000 является КОММУТАТОР A. E1/0/1 — основной порт этого коммутатора, E1/0/2 — дополнительный. Все остальные коммутаторы представляют собой транспортные узлы MRPP-кольца. Основной и дополнительный порты на них настраиваются отдельно.

Чтобы избежать возникновения временной петли, при активации нескольких MRPP-колец основного MRPP-кольца необходимо временно отключить один из портов первичного узла. Блокировка снимается после завершения настройки всех узлов.

При отключении MRPP-кольца следует убедиться в отсутствии в нем петель.

Последовательность задач по настройке КОММУТАТОРА A:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
```

```
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#fail-timer 18
Switch(mrpp-ring-4000)#hello-timer 5
Switch(mrpp-ring-4000)#node-mode master
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#exit Switch(Config)#
```

Последовательность задач по настройке КОММУТАТОРА B:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#exit Switch(Config)#
```

Последовательность задач по настройке КОММУТАТОРА C:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#
```

Последовательность задач по настройке КОММУТАТОРА D:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
```

```
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)# .
```

39.4. Устранение неисправностей при работе протокола MRPP

Работа протокола MRPP зависит от правильной настройки всех коммутаторов в MRPP-кольце. В противном случае возможно формирование петель и возникновение широковещательных штормов.

- При настройке MRPP-кольца рекомендуется отключить его. Активировать кольцо можно только после настройки всех коммутаторов.
- При блокировке в общем MRPP-кольце. MRPP-кольцо активированного коммутатора отключается.
- При возникновении в MRPP-кольце широковещательного шторма сначала отключается кольцо, а потом выполняется проверка настроек MRPP-колец на всех коммутаторах. Если настройки верны, выполняется восстановление кольца, после чего ведется наблюдение за его работой.
- Время сходимости кольцевой сети MRPP зависит от режима отклика UP/DOWN. В режиме опроса время сходимости простой кольцевой сети составляет несколько сотен миллисекунд. В режиме прерывания время сходимости находится в пределах 50 миллисекунд.
- Как правило, порт работает в режиме опроса. Режим прерывания используется только для повышения производительности. Безопасность режима опроса надежнее режима прерывания. Используйте команду «port-scan-mode {interrupt | poll}».
- Если в нормальном режиме работы все еще возникает широковещательный шторм или происходит блокировка кольца, откройте функцию отладки первичного узла MRPP и выполните команду «show MRPP statistics». Эта команда позволит просмотреть состояния первичного и транспортного узлов, а также их статистические данные. Отправьте полученные результаты в центр технической поддержки и обслуживания компании.

40. НАСТРОЙКА ПРОТОКОЛА ULPP

40.1. Введение в ULPP

У всех ULPP-групп есть два порта исходящей связи: ведущий и ведомый. В роли порта может выступать как физический порт, так и канал порта. У каждого порта ULPP-группы имеется три состояния: переадресация, ожидание, отказ. Как правило, в состоянии переадресации находится только один порт. Другой порт находится в состоянии ожидания. При возникновении проблемы связи ведущий порт переходит в состояние отказа, а ведомый — в состояние переадресации.

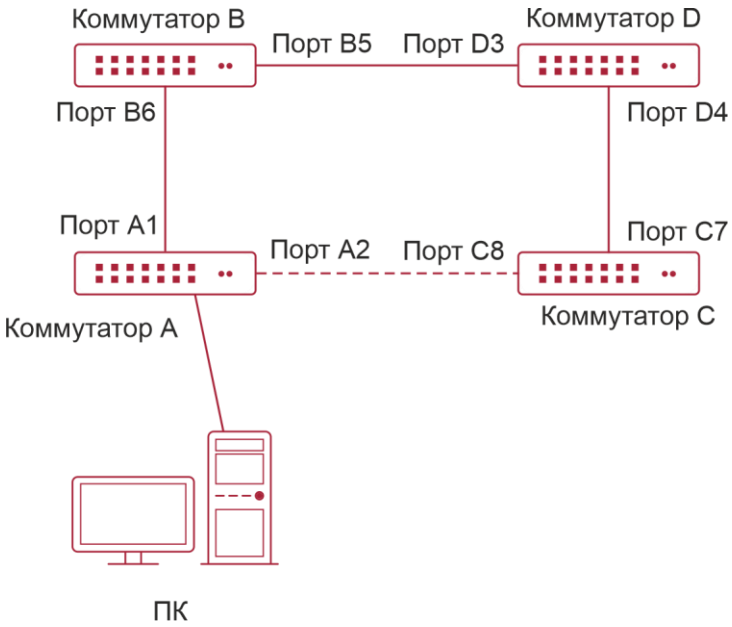


Рисунок 40-1. Схема применения протокола ULPP

На рисунке выше показан типичный сценарий применения протокола ULPP, при котором используется сеть с двумя портами исходящей связи. Коммутатор SwitchA соединяется с коммутатором SwitchD через коммутаторы SwitchB и SwitchC; A1 и A2 — порты исходящей связи. На коммутаторе SwitchA настроен протокол ULPP. Соответственно в качестве ведущего порта задается порт A1, а в качестве ведомого — A2. Когда на порте A1, находящемся в состоянии переадресации, возникает проблема, порты исходящей связи сразу же меняются местами, т. е. порт A2 переключается в состояние переадресации. Если режим приоритетного переключения не настроен, после восстановления ведущего порта A2 остается в состоянии переадресации, а A1 переключается в состояние ожидания.

После активации режима приоритетного переключения и устранения проблемы ведущий порт возвращается в состояние переадресации. Для того чтобы избежать частой смены портов исходящей связи, в коммутатор встроен механизм задержки приоритетного переключения: должно пройти некоторое время, прежде чем ведущий порт сможет перейти в состояние переадресации. Для того чтобы передача данных была непрерывной, по умолчанию на ведущем порте режим приоритетного переключения деактивирован. Вместо этого порт переходит в состояние ожидания.

При настройке протокола ULPP необходимо указать сеть VLAN, безопасность которой обеспечивается с помощью метода экземпляров MSTP этой ULPP-группой. ULPP не обеспечивает безопасность других сетей VLAN.

При переключении портов исходящей связи первичная переадресация устройства к новой сетевой топологии не применяется. На рисунке выше протокол ULPP настроен на коммутаторе SwitchA. Порт A1 назначен ведущим и находится в состоянии переадресации. Коммутатор SwitchD получает MAC-адрес ПК от порта D3. При возникновении на порте A1 проблемы переадресация трафика переключается на порт A2. Если коммутатор SwitchD отправил на ПК данные, их переадресация по-прежнему выполняется на порте D3, в результате они теряются. Следовательно, при переключении портов исходящей связи устройство, на котором настраивается протокол ULPP, должно отправить flush-пакеты через порт, находящийся в состоянии переадресации, а также обновить таблицы MAC-адресов и таблицы ARP других устройств в сети. Для обновления записей протокол ULPP соответственно использует flush-пакеты двух типов: обновленные пакеты MAC-адресов и удаленные пакеты ARP.

Для более эффективного использования пропускной способности протокол ULPP может выполнять балансировку нагрузки на сеть VLAN. Как показано на рисунке, на коммутаторе SwitchA настроены две ULPP-группы: порт A1 назначен ведущим, а порт A2 — ведомым в группе 1; порт A2 назначен ведущим, а порт A1 — ведомым в группе 2. Группы 1 и 2 обеспечивают безопасность сетей VLAN 1–100 и 101–200 соответственно. Как порт A1, так и порт A2 находятся в состоянии переадресации. Ведущий и ведомый порты взаимозаменяемы и перенаправляют пакеты разных диапазонов VLAN соответственно. При возникновении проблемы на порте A1 переадресация трафика VLAN 1–200 выполняется портом A2. После восстановления порта A1 порт A2 продолжает последовательно перенаправлять пакеты VLAN 101–200, однако переадресация данных VLAN 1–100 переключается на порт A1.

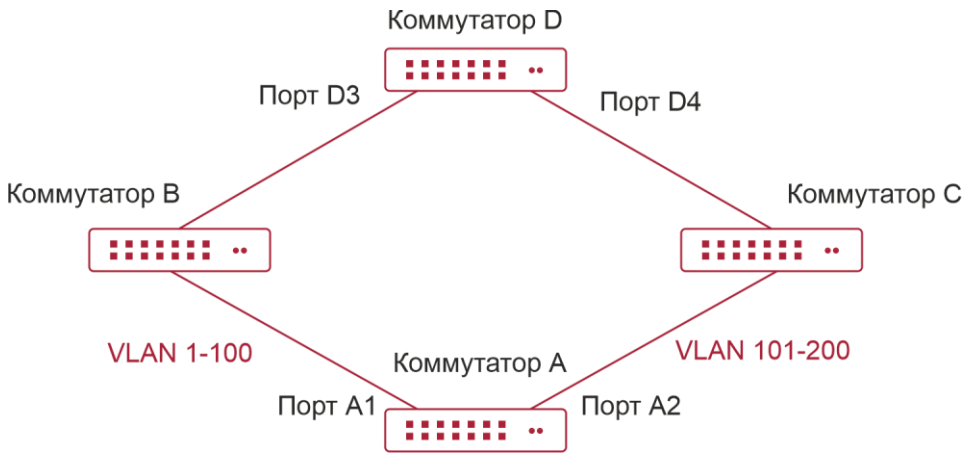


Рисунок 40-2. Балансировка нагрузки на сеть VLAN

40.2. Список задач по настройке протокола ULPP

1. Глобально создать ULPP-группу.
2. Настроить ULPP-группу.
3. Вывести на экран и отладить данные протокола ULPP.

1. Глобально создать ULPP-группу.

Команда	Описание
Режим общих настроек	
ulpp group <integer> no ulpp group <integer>	Создает и удаляет ULPP-группу

2. Настроить ULPP-группу.

Команда	Описание
Режим настройки ULPP-группы	
preemption mode no preemption mode	Задает режим приоритетного переключения ULPP-группы. Команда, начинающаяся со слова «no», удаляет этот режим
preemption delay <integer> no preemption delay	Задает задержку приоритетного переключения. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию 30 с
control vlan <integer> no control vlan	Задает идентификатор сети VLAN, управляющей передачей. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию 1
protect vlan-reference-instance <instance-list> no protect vlan-reference-instance <instance-	Задает сети VLAN, безопасность которых обеспечивается ULPP-группой. Команда, начинающаяся со слова «no», удаляет сети
flush enable mac flush disable mac	Включает или выключает отправку flushпакетов, обновляющих MAC-адреса
flush enable arp flush disable arp	Включает или выключает отправку flushпакетов, удаляющих ARP
flush enable mac-vlan flush disable mac-vlan	Включает или выключает отправку flushпакетов, удаляющих динамические MAC-адреса одноадресной рассылки в соответствии с VLAN
description <string> no description	Задает или удаляет описание ULPP-группы

Команда	Описание
Режим работы порта	
ulpp control vlan <vlan-list> no ulpp control vlan <vlan-list>	Задает идентификатор сети VLAN, управляющей приемом. Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию 1
ulpp flush enable mac ulpp flush disable mac	Включает или выключает прием flush-пакетов, обновляющих MAC-адреса
ulpp flush enable arp ulpp flush disable arp	Включает или выключает прием flush-пакетов, удаляющих ARP
ulpp flush enable mac-vlan ulpp flush disable mac-vlan	Включает или выключает прием flush-пакетов типа MAC-VLAN
ulpp group <integer> master no ulpp group <integer> master	Задает или удаляет ведущий порт ULPP-группы
ulpp group <integer> slave no ulpp group <integer> slave	Задает или удаляет ведомый порт ULPP-группы

3. Вывести на экран и отладить данные протокола ULPP.

Команда	Описание
Режим администратора	
show ulpp group [group-id]	Выводит на экран данные о настройках ULPP-группы
show ulpp flush counter interface {ethernet <IFNAME> | <IFNAME>}	Выводит на экран статистические данные о flush-пакетах
show ulpp flush-receive-port	Выводит на экран тип flush-пакета, полученного портом, и управляющую VLAN
clear ulpp flush counter interface <name>	Удаляет статистические данные о flush-пакетах

Команда	Описание
debug ulpp flush {send | receive} interface <name> no debug ulpp flush {send | receive} interface <name>	Выводит на экран данные о полученных и отправленных flush-пакетах. Команда, начинающаяся со слова «no», отключает вывод данных
debug ulpp flush content interface <name> no debug ulpp flush content interface <name>	Выводит на экран содержимое полученных flush-пакетов. Команда, начинающаяся со слова «no», отключает вывод данных
debug ulpp error no debug ulpp error	Выводит на экран данные об ошибках ULPP. Команда, начинающаяся со слова «no», отключает вывод данных
debug ulpp event no debug ulpp event	Выводит на экран данные о событиях ULPP. Команда, начинающаяся со слова «no», отключает вывод данных

40.3. Типичные примеры применения протокола ULPP

40.3.1. Применение протокола ULPP: типичный пример 1

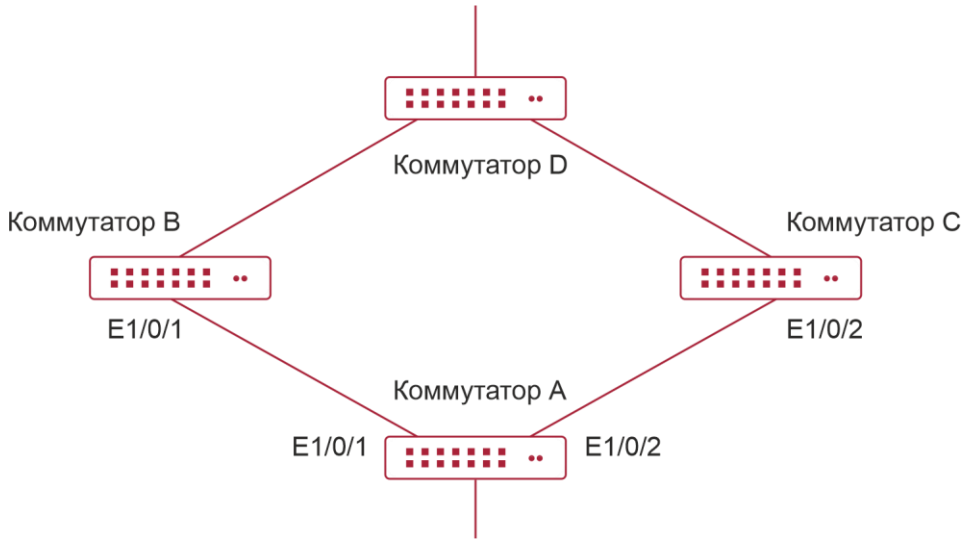


Рисунок 40-3. Применение протокола ULPP: типичный пример 1

Приведенная выше топология представляет собой типичный пример использования протокола ULPP.

У коммутатора A имеется два порта исходящей связи: коммутатор B и коммутатор C. Если протоколы не настроены, эта топология формирует кольцо. Чтобы избежать закольцовывания, на коммутаторе A настраивается протокол ULPP, а также ведущий и ведомый порты ULPP-группы. Если оба порта работают, ведомый порт переводится в

состояние ожидания и не перенаправляет flush-пакеты. При сбое ведущего порта ведомый порт переходит в состояние переадресации. На коммутаторах B и C можно выполнить команду, которая разрешает принимать flush-пакеты. Она применяется для связывания протокола ULPP, работающего на коммутаторе A, с целью немедленного переключения порта исходящей связи и уменьшения задержки переключения.

При настройке протокола ULPP на коммутаторе A необходимо прежде всего создать ULPP-группу и в качестве VLAN, безопасность которой обеспечивается этой группой, задать VLAN10. После этого следует настроить интерфейс Ethernet 1/0/1 в качестве ведущего порта, интерфейс Ethernet 1/0/2 — в качестве ведомого, а в качестве идентификатора управляющей сети VLAN —10. На коммутаторах B и C следует настроить flush-пакеты для получения ULPP. Список задач по настройке коммутатора A:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/1; 1/0/2
Switch(Config-vlan10)#exit
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 10
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#control vlan 10
Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)#exit
```

Список задач по настройке коммутатора B:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/1
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/1)# ulpp flush enable arp
Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10
```

Список задач по настройке коммутатора C:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/2
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/0/2
```

```
Switch(config-If-Ethernet1/0/2)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/2)# ulpp flush enable arp
Switch(config-If-Ethernet1/0/2)# ulpp control vlan 10
```

40.3.2. Применение протокола ULPP: типичный пример 2

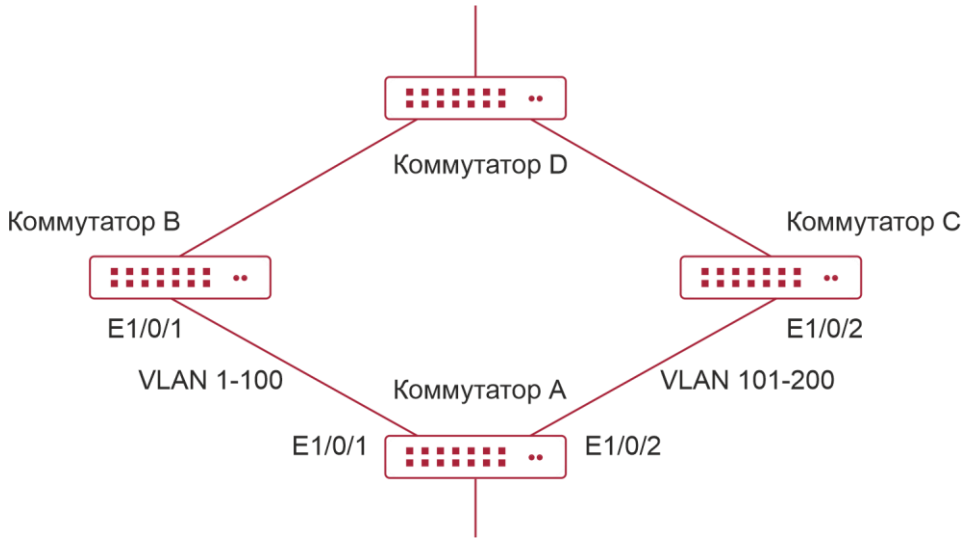


Рисунок 40-4. Применение протокола ULPP: типичный пример 2

Протокол ULPP может выполнять балансировку нагрузки на сеть VLAN. Как показано на рисунке, на коммутаторе A настроены две ULPP-группы: порт E1/0/1 назначен ведущим, а порт E1/0/2 — ведомым в группе 1; порт E1/0/2 назначен ведущим, а порт E1/0/1 — ведомым в группе 2. Группы 1 и 2 обеспечивают безопасность сетей VLAN 1–100 и 101–200 соответственно. Как порт E1/0/1, так и порт E1/0/2 находятся в состоянии переадресации. Ведущий и ведомый порты взаимозаменяемы и перенаправляют пакеты разных диапазонов VLAN соответственно. При возникновении проблемы на порте E1/0/1 переадресация трафика VLAN 1–200 выполняется портом E1/0/2. После восстановления порта E1/0/1 порт E1/0/2 продолжает перенаправлять пакеты VLAN 101–200, однако переадресация данных VLAN 1–100 переключается на порт E1/0/1.

Список задач по настройке коммутатора A:

```
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1-100
Switch(Config-Mstp-Region)#instance 2 vlan 101-200
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#preemption mode
Switch(ulpp-group-1)#exit
Switch(Config)#ulpp group 2
Switch(ulpp-group-2)#protect vlan-reference-instance 2
Switch(ulpp-group-1)#preemption mode
```

```
Switch(ulpp-group-2)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#switchport mode trunk
Switch(config-If-Ethernet1/0/1)#ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#ulpp group 2 slave
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#switchport mode trunk
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)# ulpp group 2 master
Switch(config-If-Ethernet1/0/2)#exit
```

Список задач по настройке коммутатора B:

```
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#switchport mode trunk
Switch(config-If-Ethernet1/0/1)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/1)# ulpp flush enable arp
```

Список задач по настройке коммутатора C:

```
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# switchport mode trunk
Switch(config-If-Ethernet1/0/2)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/2)# ulpp flush enable arp
```

40.4. Устранение неисправностей при работе протокола ULPP

- В настоящее время разрешена настройка более чем двух мультипортов исходящей связи. Однако в связи с риском закольцовывания использовать такую конфигурацию не рекомендуется.
- Если в нормальном режиме работы возникает широковещательный шторм или происходит разрыв связи в кольце, включите отладку ULPP, скопируйте данные за последние 3 минуты и информацию о настройках и отправьте все это в центр технической поддержки и обслуживания компании.

41. НАСТРОЙКА ПРОТОКОЛА ULSM

41.1. Введение в протокол ULSM

Протокол ULSM (наблюдение за состоянием портов исходящей связи) применяется для синхронизации состояний портов. Все ULSM-группы состоят из портов исходящей и нисходящей связи. И тех и других портов может быть несколько. В роли порта может выступать как физический порт, так и канал порта. Однако порт канала порта использоваться не может. Любой порт принадлежит только одной ULSM-группе.

За портом исходящей связи ULSM-группы ведется наблюдение. Если все порты исходящей связи находятся в состоянии отказа или в ULSM-группе нет таких портов, то группа также находится в состоянии отказа. ULSM-группа находится в рабочем состоянии, если хотя бы один порт исходящей связи работает.

Порт нисходящей связи является управляемым. Его состояние изменяется при смене состояния ULSM-группы и всегда совпадает с ним.

ULSM, как правило, работает вместе с протоколом ULPP, что позволяет устройству нисходящего уровня определить проблему связи на устройстве восходящего уровня и должным образом ее решить. Как показано на рисунке, на коммутаторе SwitchA настроен протокол ULPP. Переадресация трафика выполняется на порте A1. Если между коммутаторами SwitchB и SwitchD возникает проблема связи, коммутатор SwitchA не в состоянии определить проблему на устройстве восходящего уровня и выполнить последовательную переадресацию трафика с порта A1. В результате происходит потеря трафика.

Описанные выше проблемы можно решить с помощью настройки ULSM на коммутаторе SwitchB. Для этого необходимо настроить порт B5 в качестве порта исходящей связи ULSM-группы, а порт B6 — в качестве порта нисходящей связи. При возникновении между коммутаторами SwitchB и SwitchD проблемы связи порт нисходящей связи B6 и ULSM-группа переходят в состояние отказа. В результате коммутатор SwitchA, на котором настроен протокол ULPP, выполняет переключение портов исходящей связи, что предотвращает потерю данных.

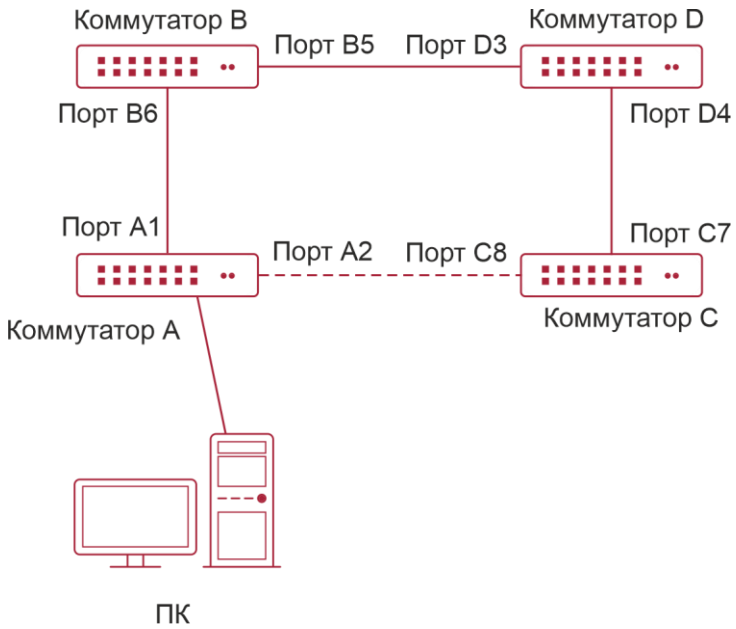


Рисунок 41-1. Схема применения протокола ULSM

41.2. Список задач по настройке протокола ULSM

1. Глобально создать ULSM-группу.
2. Настроить ULSM-группу.
3. Вывести на экран и отладить данные протокола ULSM.

1. Глобально создать ULSM-группу.

Команда	Описание
Режим общих настроек	
ulsm group <group-id> no ulsm group <group-id>	Создает и удаляет ULSM -группу

2. Настроить ULSM-группу.

Команда	Описание
Режим конфигурирования порта	
ulsm group <group-id> {uplink | downlink} no ulsm group <group-id> {uplink | downlink}	Задает порт исходящей/нисходящей связи ULSM-группы. Команда, начинающаяся со слова «no», удаляет порт

3. Вывести на экран и отладить данные протокола ULSM.

Команда	Описание
Режим администратора	
show ulsm group [group-id]	Выводит на экран информацию о настройках ULSM-группы
debug ulsm event no debug ulsm event	Выводит на экран информацию о событиях ULSM. Команда, начинающаяся со слова «no», отключает вывод данных

41.3. Типичный пример применения протокола ULSM

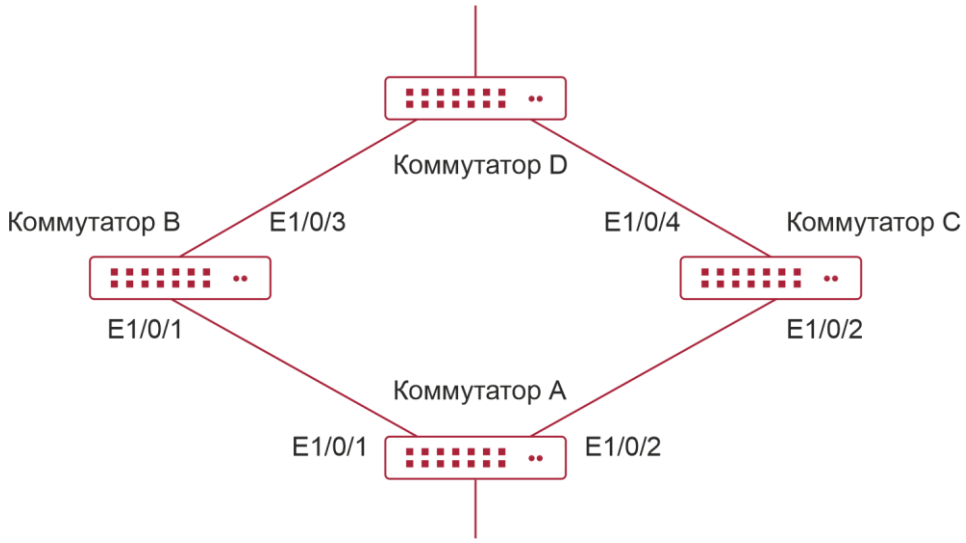


Рисунок 41-2. Типичный пример применения протокола ULSM

Приведенная выше топология представляет собой типичный пример использования протоколов ULSM и ULPP.

Протокол ULSM применяется для синхронизации состояний портов. Запускать его отдельно не имеет смысла, поэтому он, как правило, используется вместе с протоколом ULPP. В данной топологии на коммутаторе A для переключения портов исходящей связи настроен протокол ULPP. На коммутаторах B и C настроен протокол ULSM, позволяющий определить, находится ли порт исходящей связи в состоянии отказа. Если порт исходящей связи находится в состоянии отказа, ULSM закрывает порт нисходящей связи, а протокол ULPP на коммутаторе A выполняет соответствующую операцию переключения порта исходящей связи.

Список задач по настройке коммутатора A:

```
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)#exit
```

Список задач по настройке коммутатора B:

```
Switch(Config)#ulsm group 1
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#ulsm group 1 downlink
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)#ulsm group 1 uplink
Switch(config-If-Ethernet1/0/3)#exit
```

Список задач по настройке коммутатора C:

```
Switch(Config)#ulsm group 1
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#ulsm group 1 downlink
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#interface ethernet 1/0/4
Switch(config-If-Ethernet1/0/4)#ulsm group 1 uplink
Switch(config-If-Ethernet1/0/4)#exit
```

41.4. Устранение неисправностей при работе протокола ULSM

Если в нормальном режиме работы порт нисходящей связи не отвечает на событие разрыва связи на порте исходящей связи, включите отладку ULSM, скопируйте данные за последние 3 минуты и данные о настройках и отправьте все это в центр технической поддержки и обслуживания компании.

42. НАСТРОЙКА ПРОТОКОЛА SNTP

42.1. Введение в протокол SNTP

Протокол сетевого времени (NTP) широко применяется для синхронизации времени на компьютерах, подключенных к Интернету. NTP оценивает задержку передачи/приема пакетов в сети и независимо рассчитывает отклонение времени на компьютере, благодаря чему достигается высокая точность часов компьютера. В большинстве случаев протокол NTP достигает точности от 1 до 50 мс в зависимости от характеристик источника синхронизации и сетевого маршрута.

Простой протокол сетевого времени (SNTP) представляет собой упрощенную версию NTP и использует более простую реализацию алгоритма NTP. SNTP используется узлами, которым не требуются все функции NTP. Этот протокол является частным случаем протокола NTP. Общепринятой практикой является синхронизация времени на нескольких узлах в локальной сети с другими NTP-узлами в сети Интернет, а также использование этих узлов для предоставления услуг по синхронизации времени другим клиентам LAN. На рисунке ниже изображена топология сети при применении NTP/SNTP. SNTP работает в основном между серверами второго уровня и различными терминалами, поскольку в подобных сценариях, как правило, не требуется высокой точности времени, для этих служб точности SNTP (1 – 50 мс) достаточно.

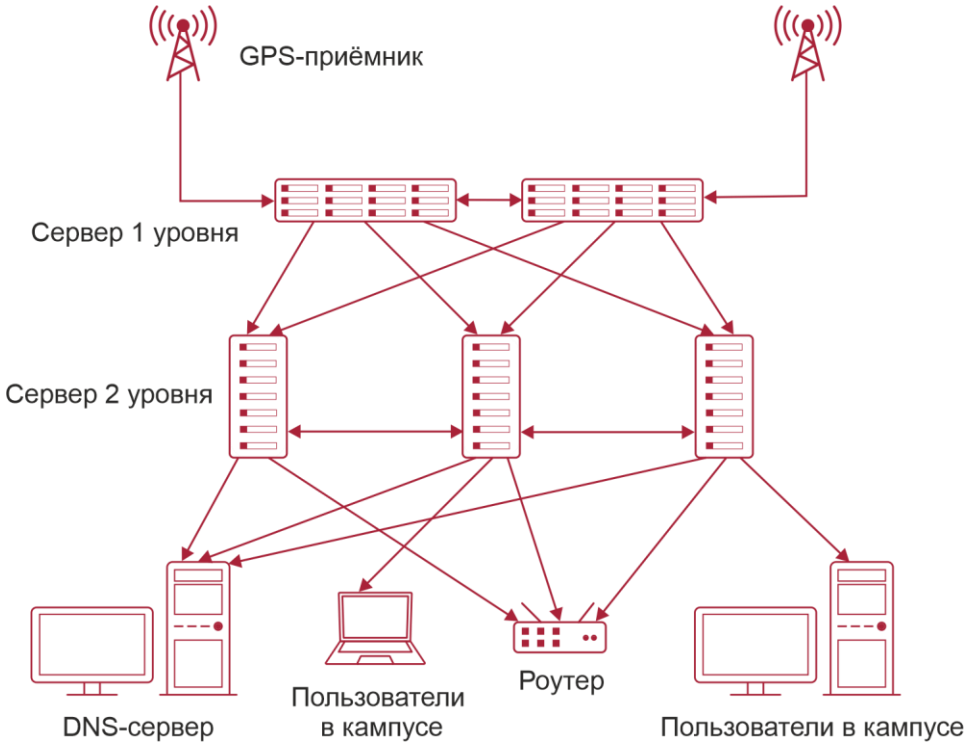


Рисунок 42-1. Сценарий работы

На коммутаторе реализован протокол SNTPv4 и поддерживается одноадресный режим работы SNTP-клиента, как описано в стандарте RFC2030. Многоадресный и одноадресный режимы работы SNTP-клиента, а также функции SNTP-сервера не поддерживаются.

42.2. Типичные примеры настройки протокола SNTP

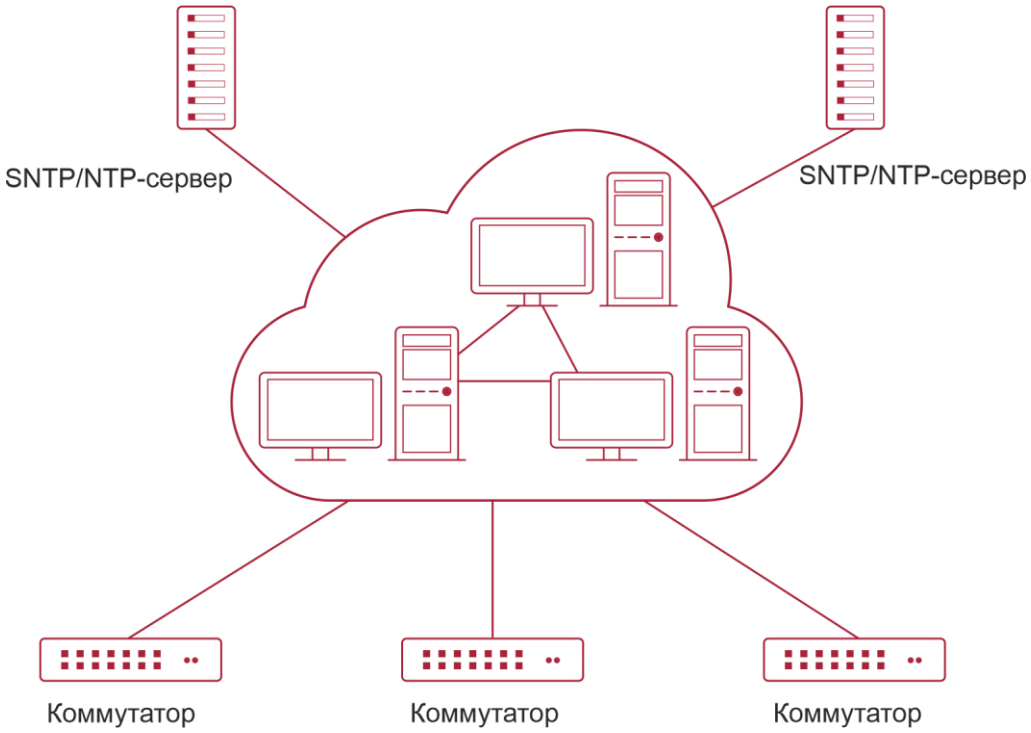


Рисунок 42-2. Типичная конфигурация протокола SNTP

Необходимо, чтобы на всех коммутаторах в автономной зоне была выполнена синхронизация времени. Это осуществляется с помощью двух резервных SNTP/NTP-серверов. Для синхронизации времени следует выполнить правильную настройку сети. Между каждым коммутатором и двумя SNTP/NTP-серверами должны быть досягаемые маршруты.

Пример. Пусть SNTP/NTP-серверам назначены IP-адреса 10.1.1.1 и 20.1.1.1 соответственно, и включена функция SNTP/NTP-сервера (например, главный NTP-сервер). Тогда настройки всех коммутаторов будут выглядеть следующим образом:

```
Switch#config
Switch(config)#sntp server 10.1.1.1
```

43. НАСТРОЙКА ФУНКЦИЙ ПРОТОКОЛА NTP

43.1. Введение в протокол NTP

NTP (протокол сетевого времени) применяется для синхронизации серверов точного времени и клиентов в сетях WAN и LAN. Он может достигать точности в несколько миллисекунд. События, состояния, функции передачи и действия определяются стандартом RFC-1305.

NTP используется для синхронизации часов всех устройств в сети, что дает возможность разворачивать на них различные приложения на основе единого времени.

Время локальной системы, в которой запущен протокол NTP, можно синхронизировать с помощью других источников опорного сигнала. Эта система в свою очередь может служить источником опорного сигнала для синхронизации других часов. Кроме того, синхронизация устройств может выполняться путем передачи друг другу NTP-пакетов.

43.2. Список задач по настройке функции NTP

1. Включить функцию NTP.
2. Настроить функцию NTP-сервера.
3. Задать максимальное количество серверов широковещательной или многоадресной рассылки, которые могут поддерживаться NTP-клиентом.
4. Задать часовой пояс.
5. Настроить список контроля доступа NTP.
6. Настроить аутентификацию NTP.
7. Задать какой-либо интерфейс в качестве широковещательного/многоадресного интерфейса NTP-клиента.
8. Задать интерфейс, который не принимает NTP-пакеты.
9. Задать период отправки NTP-клиентом пакетов запроса.
10. Вывести данные на экран.
11. Выполнить отладку.

1. Включить функцию NTP.

Команда	Описание
Режим общих настроек	
ntp enable ntp disable	Включает или отключает функцию NTP

2. Настроить функцию NTP-сервера.

Команда	Описание
Режим общих настроек	
ntp server {<ip-address> | <ipv6-address>} [version <version_no>] [key <key-id>] no ntp server {<ip-address> | <ipv6-address>}	Включает указанный сервер точного времени для источника синхросигналов

3. Задать максимальное количество серверов широковещательной или многоадресной рассылки, которые могут поддерживаться NTP-клиентом.

Команда	Описание
Режим общих настроек	
ntp broadcast server count <number> no ntp broadcast server count	Задает максимальное количество серверов широковещательной или многоадресной рассылки, поддерживаемых NTP-клиентом. Команда, начинающаяся со слова «no», отменяет настройки и восстанавливает значение по умолчанию

4. Задать часовой пояс.

Команда	Описание
Режим общих настроек	
clock timezone WORD {add | subtract} <0-23> [<0-59>] no clock timezone WORD	Эта команда задает часовой пояс в режиме общих настроек. Команда, начинающаяся со слова «no», удаляет заданный часовой пояс

5. Настроить список контроля доступа NTP.

Команда	Описание
Режим общих настроек	
ntp access-group server <acl> no ntp access-group server < acl>	Настраивает список контроля доступа NTP

6. Настроить аутентификацию NTP.

Команда	Описание
Режим общих настроек	
ntp authenticate no ntp authenticate	Включает функцию аутентификации NTP
ntp authentication-key <key-id> md5 <value> no ntp authentication-key <key-id>	Задает ключ аутентификации для аутентификации NTP
ntp trusted-key <key-id> no ntp trusted-key <key-id>	Задает доверяемый ключ

7. Задать какой-либо интерфейс в качестве многоадресного интерфейса NTP-клиента.

Команда	Описание
Режим настройки VLAN	
ntp multicast client no ntp multicast client	Задает интерфейс для приема многоадресных NTP-пакетов
ntp ipv6 multicast client no ntp ipv6 multicast client	Задает интерфейс для приема многоадресных NTP-пакетов IPv6

8. Задать интерфейс, который не принимает NTP-пакеты.

Команда	Описание
Режим настройки VLAN	
ntp disable no ntp disable	Отключает функцию NTP

9. Задать период отправки NTP-клиентом пакетов запроса.

Команда	Описание
Режим общих настроек	
ntp syn-interval <1-3600> no ntp syn-interval	Задает период отправки NTP-клиентом пакетов запроса (1 – 3600 с). Команда, начинающаяся со слова «no», восстанавливает значение по умолчанию, равное 64 с

10. Вывести данные на экран.

Команда	Описание
Режим администратора	
show ntp status	Выводит на экран состояние синхронизации времени
show ntp session [<ip-address> | <ipv6-address>]	Выводит на экран данные NTP-сеанса

11. Выполнить отладку.

Команда	Описание
Режим администратора	
debug ntp authentication no debug ntp authentication	Включает режим отладки аутентификации NTP
debug ntp packets [send | receive] no debug ntp packets [send | receive]	Включает режим отладки данных NTP-пакетов
debug ntp adjust no debug ntp adjust	Включает режим отладки данных об обновлении времени
debug ntp sync no debug ntp sync	Включает режим отладки данных о синхронизации времени
debug ntp events no debug ntp events	Включает режим отладки данных NTP-событий

43.3. Типичные примеры применения функции NTP

Часы коммутатора клиента необходимо синхронизировать с сервером точного времени. В сети находятся два сервера точного времени: один используется в качестве узла, другой выступает в качестве резервного. Соединение и конфигурация представлены на рисунке ниже (Switch A и Switch B — коммутаторы или маршрутизаторы, поддерживающие NTP-сервер):

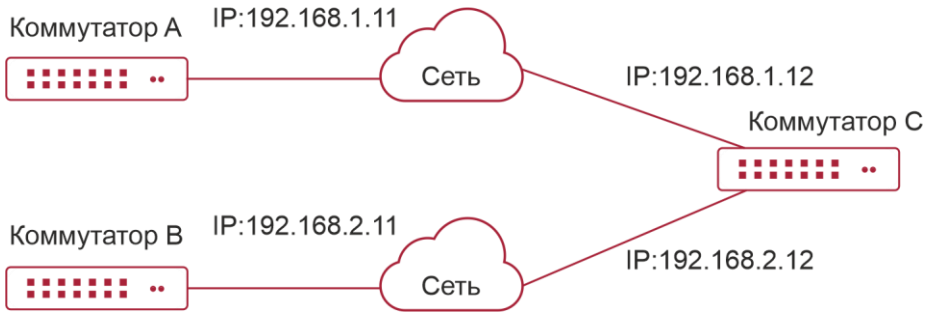


Рисунок 43-1.

Ниже приводится настройка коммутатора Switch C (коммутаторы Switch A и Switch B могут настраиваться иначе в зависимости от компании-производителя; пояснения не приводятся, поскольку в настоящее время наши коммутаторы не поддерживают NTP-сервер).

Коммутатор Switch C:

```
Switch(config)#ntp enable
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 192.168.1.12 255.255.255.0
Switch(config)#interface vlan 2
Switch(Config-if-Vlan1)#ip address 192.168.2.12 255.255.255.0
Switch(config)#ntp server 192.168.1.11
Switch(config)#ntp server 192.168.2.11
```

43.4. Устранение неполадок при работе функции NTP

Система может предоставить отладочную информацию об ошибке, возникшей в процессе настройки.

По умолчанию функция NTP отключена. Для просмотра текущих настроек следует выполнить команду «show». Для отображения данных конкретной процедуры и проверки настроек функции используйте команды отладки. Для просмотра рабочих данных NTP следует выполнить команду «show». Если у вас есть вопросы, отправьте записанное сообщение в центр технической поддержки и обслуживания компании.

44. НАСТРОЙКА ЛЕТНЕГО ВРЕМЕНИ

44.1. Введение в летнее время

Летнее время — это система времени, которая применяется для экономии электроэнергии. Весной время переводится на 1 час вперед для более рационального использования светлого времени суток и экономии электроэнергии на освещение. Перевод часов на летнее время в разных странах осуществляется по-разному. На сегодняшний день на летнее время переходит почти 110 стран.

Летнее время обычно переводят на 1 ч позже относительно стандартного времени. Например, при переходе на летнее время 10:00 по стандартному времени — это 11:00 по-летнему.

44.2. Последовательность задач по настройке летнего времени

44.2.1. Задать абсолютный или повторяющийся диапазон летнего времени

Команда	Описание
Режим общих настроек	
clock summer-time <word> absolute <HH:MM> <YYYY.MM.DD> <HH:MM> <YYYY.MM.DD> [<offset>] no clock summer-time	Задает абсолютный диапазон летнего времени. Время начала и время завершения задаются вместе с конкретным годом
clock summer-time <word> recurring <HH:MM> <MM.DD> <HH:MM> <MM.DD> [<offset>] no clock summer-time	Задает повторяющийся диапазон летнего времени. Каждый год переход на летнее время и обратно происходит в одно и то же время
clock summer-time <word> recurring <HH:MM> <week> <day> <month> <HH:MM> <week> <day> <month> [<offset>] no clock summer-time	Задает повторяющийся диапазон летнего времени. Каждый год переход на летнее время и обратно происходит в одно и то же время

44.3. Примеры перехода на летнее время

Пример 1.

Требования к настройкам выглядят следующим образом. Переход на летнее время происходит в 23:00 1 апреля 2012 г.; возвращение к стандартному времени выполняется в 0:00 1 октября 2012 г. Сдвиг времени составляет 1 час, название летнего времени — 2012.

Ниже приводится процедура настройки:

```
Switch(config)# clock summer-time 2012 absolute 23:00 2012.4.1 00:00 2012.10.1
```

Пример 2.

Требования к настройкам выглядят следующим образом. Переход на летнее время каждый год происходит в 23:00 первой субботы апреля; возвращение к стандартному времени выполняется в 0:00 последнего воскресенья октября. Сдвиг времени составляет 2 часа, название летнего времени — time_travel.

Ниже приводится процедура настройки:

```
Switch(config)#clock summer-time time_travel recurring 23:00 first sat apr 00:00
last sun oct 120
```

44.4. Устранение неполадок при настройке летнего времени

Если при настройке летнего времени возникает какая-либо проблема, проверьте, не вызвана ли она одной из следующих причин:

- Проверьте, выполняются ли команды в режиме общих настроек.
- Проверьте, правильно ли работает тактовый генератор системы.

45. ОБЩАЯ ИНФОРМАЦИЯ

45.1. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» –> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» –> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

45.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 269-08-81

Центральный офис +7 (495) 477-81-18

45.3. Электронная версия документа

Дата публикации 13.08.2024

https://files.qtech.ru/upload/switchers/QSW-3420_3750_3750r_4610_user_manual.pdf