Руководство пользователя по использованию сервисных IP-маршрутизаторов

Серия QSR

Оглавление

1. УПРАВЛЕНИЕ МАРШРУТИЗАТОРОМ

1.1. Варианты Управления

Для управления необходимо настроить маршрутизатор. Маршрутизатор 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 маршрутизатора, либо, когда внутриполосное управление недоступно. Например, пользователь может через консольный порт присвоить маршрутизатору IP-адрес для доступа по протоколам Telnet, SSH.

Процедура управления маршрутизатором через консольный интерфейс описана ниже:

Шаг 1: подключить персональный компьютер к консольному (серийному) порту маршрутизатора.

Рисунок 1. Подключение ПК к консольному порту маршрутизатора

Как показано выше, серийный порт (RS-232) подключен к маршрутизатору 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 маршрутизатора.
Маршрутизатор	Требуется работающий Console порт.

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, COM1. Затем в поле «Speed» необходимо задать скорость передачи данных (baudrate) – 115200 бит/с.

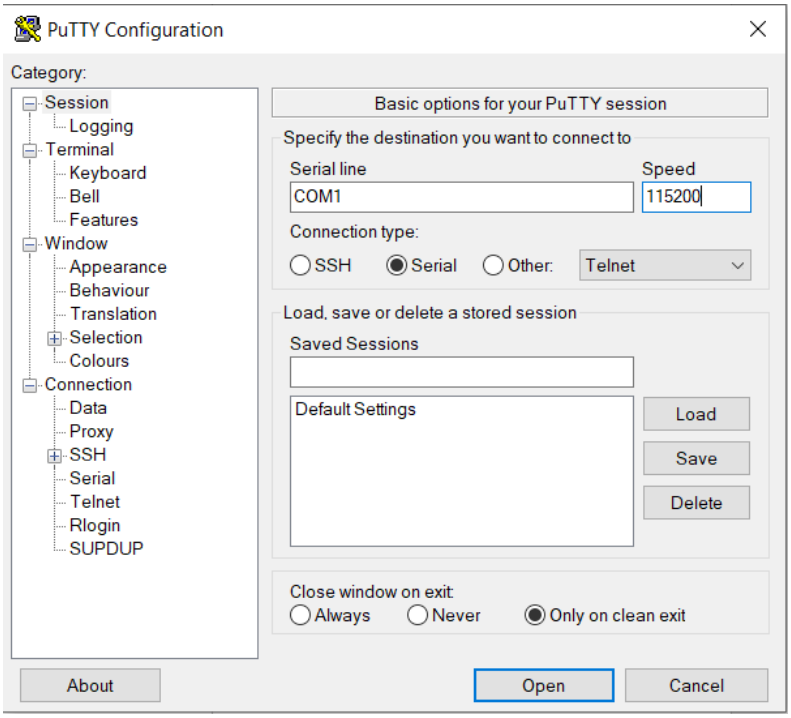


Рисунок 2. Основныве настройки PuTTY.

2. Для облегченного повторного подключения с использованием PuTTY, следует сохранить настройки сессии. Для этого необходиомо в поле «Saved Session» ввести название сессии (например, Router1) и нажать кнопку «Save»

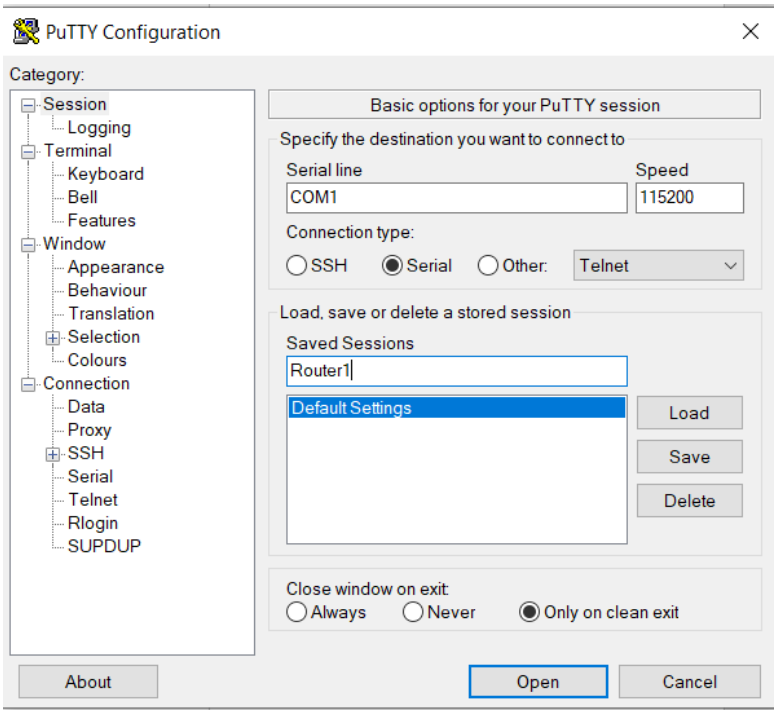


Рисунок 3.Сохранение сессии в PuTTY.

3. Выбирете сохраненную сессию и нажмите копку «Open»

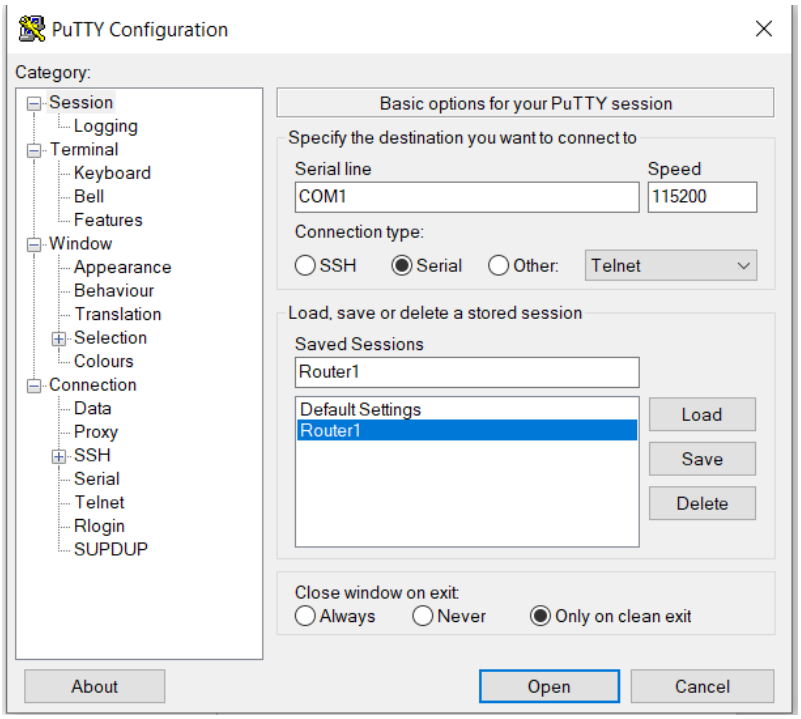


Рисунок 4. Запуск сохраненной сессии.

Шаг 3: Вызов командного интерфейса (CLI) маршрутизатора.

Включите маршрутизатор и дождитесь полной загрузки. После чего в окне PuTTY появятся следующие сообщения – это пользовательский режим маршрутизатора.

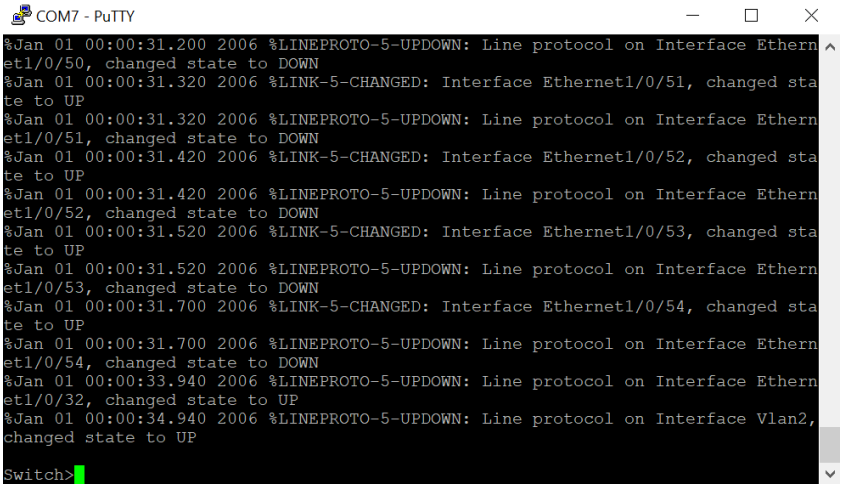


Рисунок 5. Маршрутизатор загрузился.

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

1.1.2. In-band управление.

In-band управление относится к удалённому управлению посредством доступа к маршрутизатору с использованием таких протоколов как Telnet, SSH, а также SNMP. В тех случаях, когда In-band управление из-за изменений, сделанных в конфигурации маршрутизатора, работает со сбоями или стало недоступным, для управления и конфигурирования маршрутизатора необходимо использовать Out-band управление (Console).

1.1.2.1. Управление по Telnet

Чтобы управлять маршрутизатором по Telnet, должны выполняться следующие условия:

1. Маршрутизатор должен иметь сконфигурированный IPv4/IPv6-адрес.
2. IP-адрес хоста (Telnet-клиент) и VLAN-интерфейс маршрутизатора, 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 маршрутизатора с других устройств, таких как маршрутизатор.

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

Рисунок 5. Управление маршрутизатором по Telnet

Шаг 1: Настройка IP-адресов для маршрутизатора и запуск функции Telnet Server на маршрутизаторе.

- Первым делом идет настройка IP-адреса хоста. Он должен быть в том же сегменте сети, что и IP-адрес VLAN1-интерфейса маршрутизатора. Предположим, что IP-адрес интерфейса VLAN1 маршрутизатора 192.168.0.1/24. Тогда IP-адрес хоста может быть 192.168.0.2/24. Подключаем маршрутизатор к хосту сетевым кабелем (патч-корд RJ-45 – RJ-45). С помощью утилиты ping, введя команду «ping 192.168.0.2», можно проверить связность маршрутизатора с хостом.
- Команды настройки IP-адреса для интерфейса VLAN1 указаны ниже. Перед началом In-band управления, IP-адрес маршрутизатора должен быть настроен посредством Out-band-управления (через порт Console маршрутизатора). Команды конфигурирования следующие (далее считается, что все приглашения режима конфигурирования маршрутизатора начинаются со слова «Router», если отдельно не указано иного). После того, как маршрутизатор полностья загрузился, он начинает поиск DHCP сервера с целью получения IP-адреса для интерфейса VLAN 1. Не найдя DHCP сервер, маршрутизатор присваивает интерфейсу VLAN 1 по умолчанию IP-адрес: 192.168.0.1 255.255.255.0. Если интерфейсу VLAN 1 IP-адрес не был присвоен, можно его ввести вручную, введя команды:

```
Router>enable
Router#config
Router(config)#interface vlan 1
Router(Config-if-Vlan1)#ip address 192.168.0.1 255.255.255.0
```

По умолчанию функция Telnet сервера на маршрутизаторе включена. Если по каким-либо причинам функция Telnet сервера отключена, то для активации функции Telnet сервера пользователь должен включить её в режиме глобального конфигурирования, как показано ниже:

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

Шаг 2: Запуск программы Telnet Client.

Необходимо запустить Telnet-клиент в программе «Выполнить» Windows. Открыть окно ввода программы «Выполнить» можно комдбинацией клавиш Win+R. Также можно воспользоваться программой PuTTY, где следует указать IP-адрес маршрутизатора.

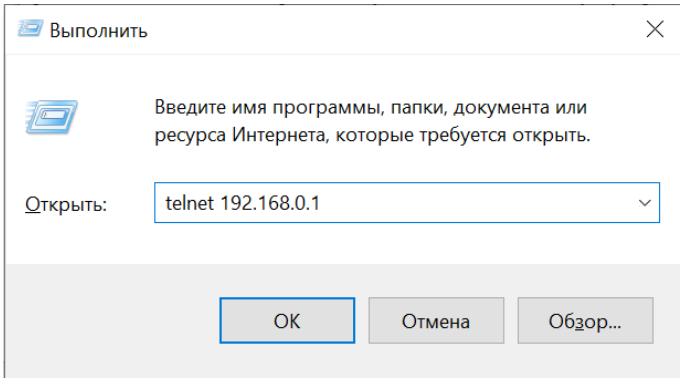


Рисунок 6. Запуск программы Telnet-клиент в Windows

Шаг 3: получить доступ к маршрутизатору.

Для того что бы получить доступ к конфигурации по протоколу 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 маршрутизатора, имя пользователя (username) и пароль (password) для авторизованных пользователей должны быть настроены следующей командой: «**username <username> privilege <privilege> [password (0|7) <password>]**». По умолчанию логин (login) – admin, пароль (password) – admin.

Для локальной аутентификации можно использовать следующую команду:

```
Router(config)#authentication line vty login local
```

Для доступа в привелигерованный режим необходимо, что бы был задан уровень привилегий 15.

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

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

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

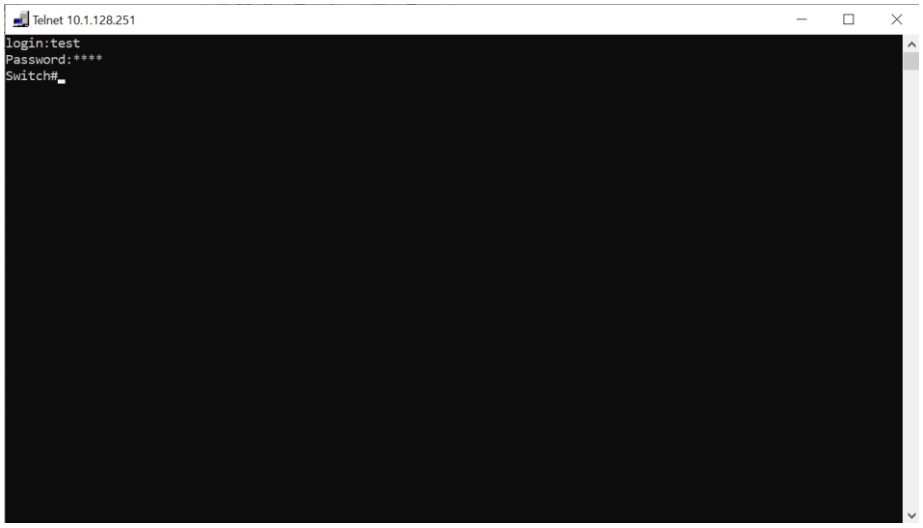


Рисунок 7. Подключение, используя протокол Telnet

1.2. CLI-интерфейс

Маршрутизатор обеспечивает три интерфейса управления для пользователя: CLI-интерфейс (Command Line Interface), сетевое управление программным обеспечением SNMP. Мы познакомим вас с CLI, а также с конфигурациями в деталях. SNMP будет рассматриваться в главе «Настройка SNMP». CLI-интерфейс знаком большинству пользователей. Как упомянуто выше, при управлении по независимым каналам связи и Telnet-управление маршрутизатором 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 маршрутизатора. Каждая категория представляет свой, отличный от всех, режим конфигурации.

Возможности Shell для маршрутизаторов описаны ниже:

- режим настройки;
- настройка синтаксиса;
- поддержка сочетания клавиш;
- справка;
- проверка ввода;
- поддержка язык нечеткой логики (Fuzzy math).

1.2.1. Режим настройки

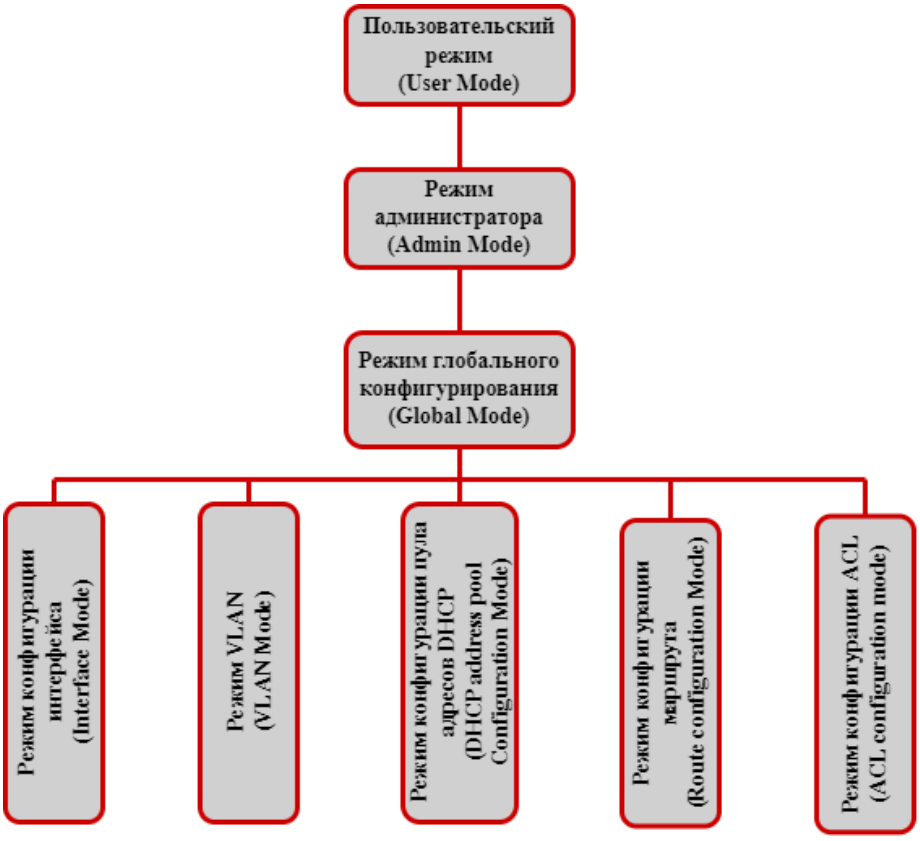


Рисунок 8. Режимы настройки Shell

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 «Router>», 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 маршрутизатора.

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 маршрутизатора будет выглядеть как «Router#». Маршрутизатор также поддерживает комбинацию клавиш «Ctrl + Z», что позволяет простым способом выйти в режим администратора из любого режима конфигурации (за исключением пользовательского).

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

для предотвращения неавторизованного доступа и злонамеренного изменения конфигурации маршрутизатора.

1.2.1.3. Режим глобального конфигурирования.

Наберите команду «Router#config» в режиме администратора для того, чтобы войти в режим глобального конфигурирования. Используйте команду выхода в соответствии с другими режимами конфигурации, такими, как режим конфигурации 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.

1.2.1.3.1. Режим конфигурирования интерфейса

Использование команды интерфейса в режиме глобального конфигурирования позволяет входить в режим конфигурирования указанного интерфейса. Маршрутизатор 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 <1-4094> в режиме глобального конфигурирования (для входа в настройки интерфейса необходимо наличие созданного vlan <vlan-id>).	Настройка IP-адресов маршрутизатора и т.д.	Используйте команду exit для возвращения в режим глобального конфигурирования.
Ethernet-порт	Наберите команду interface ethernet <interface name> в режиме глобального конфигурирования.	Режим конфигурирования порта	Используйте команду exit для возвращения в режим глобального конфигурирования.

1.2.1.3.2. Режим VLAN

Использование команды vlan <vlan-id> в режиме глобального конфигурирования помогает создать и 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.

1.2.1.3.3. Режим DHCP Address Pool

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

1.2.1.3.4. ACL-режим

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

1.2.2. Настройка синтаксиса

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

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

Расшифровка: cmdtxt жирным шрифтом указывает на ключевое слово команды;

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

Вот примеры некоторых актуальных команд конфигурации:

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

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

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

snmp-server community ro public

snmp-server community rw private

1.2.3. Сочетания клавиш

Маршрутизатор 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.

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

1.2.4. Справка

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

Доступ к справке	Использование и функции
Help	Вывод краткого описания справочной системы интерпретатора команд
«?»	Для получения описания всех доступных команд в данном режиме
«?»	Введите "?" после команды. Если позиция должна быть с параметром, описание этого параметра типа, масштаба и т.д., будут отображены, если

Доступ к справке	Использование и функции
	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.
«?»	Если после ввода команды или части команды ввести «?», то маршрутизатор выдаст варианты продолжения команды с кратким описанием. Пример: Router#show mac-? mac-address Mac address information mac-address-table Mac address table commands mac-authentication-bypass information Show MAC authentication bypass feature mac-notification transmit MAC address information notification message mac-vlan Mac vlan

1.2.5. Проверка ввода

1.2.5.1. Отображаемая информация: успешное выполнение (successfull)

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

1.2.5.2. Отображаемая информация: ошибочный ввод (error)

Отображаемое основных сообщений ошибок	Пояснение
Unrecognized command	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.
% Incomplete command	Команда введена не полностью
% Invalid input detected at '^' marker.	Команда не существует или не применима в данном режиме

Отображаемое основных сообщений ошибок	Пояснение
% Unrecognized command	Команда не распознана
Invalid command or parameter	Команда существует (признается), но задан неправильный параметр.
This command is not existing in current mode	Команда существует (признается), но не может быть использована в данном режиме.
Please configure precursor command "*»at first!	Команда существует (признается), но отсутствует условие команды.
syntax error: missing "" before the end of command line!	Ошибка синтаксиса: кавычки не могут использоваться в паре.

1.2.6. Поддержка языка нечеткой логики (Fuzzy math)

Shell на маршрутизаторе 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 МАРШРУТИЗАТОРА

2.1. Основные настройки

Основные настройки маршрутизатора 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 маршрутизаторе, отображения информации о версии системы маршрутизатора 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.

Команда	Пояснение
Режим администратора	
config	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.
Расширенный пользовательский режим/Режим администратора	
end	Выход из текущего режима и возвращение в режим администратора, только когда пользователь находится не в пользовательском/администраторском режимах.
Режим администратора	
clock set <HH:MM:SS> [YYYY.MM.DD]	Установка даты и времени.
show version	Отображение версии маршрутизатора.
set default	Возвращает заводские настройки.
write	Сохраняет текущую конфигурацию на Flash-память.
reload	Перезагрузка маршрутизатора.

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. Маршрутизатор может быть, как Telnet-сервером, так и Telnet-клиентом.

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

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

2.2.1.2. Команды конфигурирования Telnet

1. Настройка Telnet-сервера.
2. Использование Telnet для удаленного доступа к маршрутизатору.

1. Настройка Telnet-сервера.

Команда	Описание
Режим глобального конфигурирования	
telnet-server enable no telnet-server enable	Активирует функцию Telnet-сервера на маршрутизаторе, 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 line {console | vty | web} login {local | radius | tacacs} no authentication line {console | vty | web} login	Настройка режима аутентификации для подключения по протоколу Telnet, консольного подключения и с помощью протокола HTTP. Команда «no» удаляет команду
authentication enable {console | vty| web} no authentication enable	Настройка включения списков методов аутентификации. Команда «no» отменяет применение методов аутентификации
authorization line {console | vty | web} exec {local | radius | tacacs} no authorization line {console | web | web} exec	Настройка режима авторизации. Команда «no» отменяет режим авторизации.

Команда	Описание
accounting line {console | vty} command <1- 15> {start-stop | stop-only | none} tacacs no accounting line {console | vty} command <1-15>	Настройка списка методов учета. Команда «no» удаляет списки метода учета.
Режим администратора	

2. Использование Telnet для удаленного доступа к маршрутизатору.

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

2.2.2. SSH

2.2.2.1. Введение в SSH

SSH (англ. *Secure SHell* – «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 маршрутизатору, соответствующему требованиям SSH2.0, необходимо SSH2.0 клиентское программное обеспечение, такое, как SSH Secure Client и Putty. Пользователи могут запускать вышеперечисленное программное обеспечение для управления маршрутизатором удаленно. Маршрутизатор 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 маршрутизаторе; команда «no» отменяет предыдущую команду.
Username <username> [privilege <privilege>] [password [0 | 7] <password>]	Настраивает имя пользователя и пароль для доступа к маршрутизатору через SSH-клиент.

Команда	Описание
no username <username>	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 числа повторных попыток SSH-аутентификации; Команда «no» восстанавливает значения по умолчанию.

2.2.2.2.1. Пример настройки SSH-сервера

Пример 1:

Задачи:

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

```
Router(config)#ssh-server enable
Router(config)#interface vlan 1
Router(Config-if-Vlan1)#ip address 100.100.100.200 255.255.255.0
Router(Config-if-Vlan1)#exit
Router(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 маршрутизатора, за исключением распределения IPv6-адреса для локального хоста.

2.3. Настройка IP-адресов маршрутизатора

Все Ethernet-порты маршрутизатора 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 маршрутизатора. Все сети VLAN, связанные с интерфейсом, и их конфигурация могут быть настроены в подрежиме конфигурирования VLAN. Маршрутизатор предоставляет три метода конфигурации IP-адреса:

- Ручная
- DHCP

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

В BOOTP/DHCP-режиме, маршрутизатор работает как BOOTP/DHCP-клиент, отправляет широковещательные пакеты BOOTP-запроса на BOOTP/DHCP-сервера и BOOTP/DHCP-сервер назначает адрес отправителю запроса, кроме того, маршрутизатор 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. 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. DHCP конфигурация.

Команда	Описание
VLAN-режим	
ip dhcp-client enable no ip dhcp-client enable	Включение маршрутизатора 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. Маршрутизатор поддерживает функции агента.

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

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

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

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

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

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

2.4.2. Введение в MIB

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

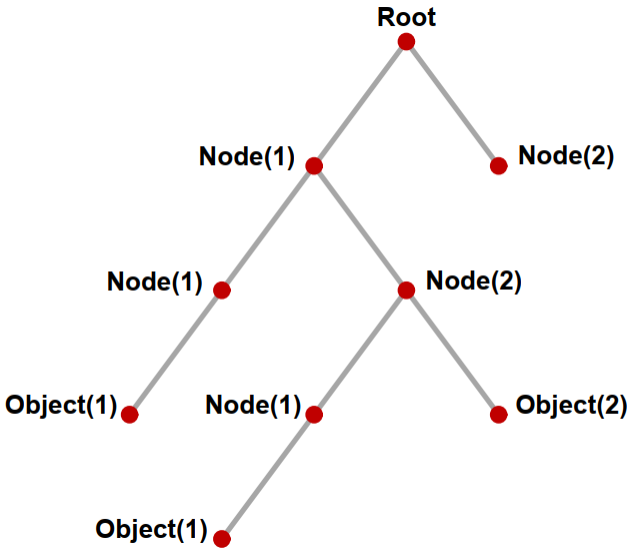


Рисунок 9. Пример дерева ASN.1

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.

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

2.4.2.1. Введение в RMON

RMON (англ. Remote Network MONitoring) — дистанционный мониторинг сети) 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 маршрутизаторами. RMON обеспечивает высокоэффективный метод контроля действий внутри подсети.

MIB RMON состоит из 10 групп. Маршрутизатор 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).

2.4.3. Настройка SNMP

2.4.3.1. 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.

1. Включение и отключение функции SNMP-агента.

Команда	**Описание**
Режим глобального конфигурирования	
snmp-server enable no snmp-server enable	Включение функции SNMP-агента на маршрутизаторе. 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 маршрутизатора. Команда «no» удаляет эту строку.

3. Настройка безопасного 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 маршрутизатору. 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 маршрутизаторе. 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 маршрутизаторе. 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 маршрутизаторе. Эта команда используется для SNMP v3.

8. Настройка TRAP.

Команда	Описание
Режим глобального конфигурирования	
snmp-server enable traps no snmp-server enable traps	Включить отправку Trap-сообщений. Эта команда используется для SNMP v1/0/v2/v3.
snmp-server host {<host- ipv4-address> | <host-ipv6-address>} {v1 {0|7} <community string> | v2c {0|7} <community string> | v3 {noauthnopriv | authnopriv | authpriv} <user-string> no snmp-server host {<host-ipv4-address> | <host-ipv6-address>} {v1 {0|7} <community string> | v2c {0|7} <community string> | v3 {noauthnopriv | authnopriv | authpriv} <user-string> }	Установка IPv4/IPv6-адреса хоста, который используется для получения информации SNMP Trap. Для SNMP v1/0/v2, эта команда также настраивает строку сообщества для Trap; для SNMP v3, эта команда также настраивает имя пользователя и уровень безопасности Trap. Команда "no" отменяет этот IPv4- или IPv6-адрес.
snmp-server trap-source {<ipv4-address> | <ipv6-address>} no snmp-server trap-source {<ipv4-address> | <ipv6-address>}	Установка IPv4- или IPv6-адреса источника, который используется для отправки Trap-пакетов, команда «no» удаляет конфигурацию.

2.4.4. Типичные примеры настройки SNMP

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

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

Конфигурация маршрутизатора, записана ниже:

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

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

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

Конфигурация маршрутизатора, изложена ниже:

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

Сценарий 3: NMS использует SNMP v3, чтобы получить информацию от маршрутизатора.

Конфигурация маршрутизатора, изложена ниже:

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

Сценарий 4: NMS хочет получить v3Trap-сообщение, отправленное маршрутизатором. Конфигурация маршрутизатора, изложена ниже:

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

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

Конфигурация маршрутизатора, изложена ниже:

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

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

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

Конфигурация маршрутизатора, изложена ниже:

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

2.4.5. 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

маршрутизатором и хостом может быть проверена путем pinga (используйте команду"ping").

- Убедиться, что включена функция SNMP-агента. (Использовать команду "snmp-server ").
- Убедиться, что безопасность IP для NMS (использовать команду "snmp-server securityip") и строка сообщества (использовать команду "snmp-server community") правильно настроены. Если что-то из этого не настроено, SNMP не сможет общаться с NMS должным образом.
- Если необходима Trap-функция, не забудьте включить Trap (использовать команду "snmp-server enable traps"). И не забудьте правильно настроить IP-адрес хоста и строку сообщества для Trap (использовать команду "snmp-server host"), чтобы обеспечить отправку Trap-сообщений на указанный хост.
- Если необходима RMON-функция, она должна быть включена (использовать команду "rmon enable").
- Используйте команду "show snmp», чтобы проверить отправленные и полученные сообщения SNMP; Используйте команду "show snmp status", чтобы проверить информацию о конфигурации SNMP; Используйте команду "debug snmp packet", чтобы включить функции отладки и проверки SNMP.
- Если пользователь по-прежнему не может решить проблемы с SNMP, обращайтесь в технический центр.

2.5. Модернизация маршрутизатора

Маршрутизатор предоставляет способ обновления программного обеспечения: TFTP/FTP-обновление под Shell.

2.5.1. Системные файлы маршрутизатора

Системные файлы включают в себя файл образа системы (image). Обновление системных файлов маршрутизатора подразумевает собой перезапись старых файлов новыми.

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

Маршрутизатор предоставляет пользователю два режима обновления:

TFTP- и FTP-обновление в режиме Shell.

2.5.2. Обновление FTP/TFTP

2.5.2.1. 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 маршрутизаторами. Оба они передают файлы в клиент-серверной модели. Разница между ними описана ниже.

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

запрос на передачу от FTP-клиента на порт 21 сервера для установления управляющего соединения и согласования передачи данных через управляющее соединение.

Существует два типа таких соединений: активные и пассивные соединения.

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

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

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

Маршрутизатор может работать как FTP/TFTP-клиент или сервер. Когда маршрутизатор 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 маршрутизаторы) без ущерба для его нормальной работы. И также может быть получен список файлов с сервера в режиме FTP-клиента. Конечно, маршрутизатор может также загрузить текущие конфигурационные файлы и системные файлы на удаленный FTP/TFTP-сервер (это могут быть как хосты, так и другие маршрутизаторы). Когда маршрутизатор 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: сокращённо от EPROM, СПЗУ. EPROM заменяет FLASH-память в маршрутизаторе.

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

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

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

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

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

Маршрутизатор 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 маршрутизатора. Файл начальной конфигурации хранится в энергонезависимой памяти. Если устройство не поддерживает CF, файл конфигурации

хранится только во FLASH. Если устройство поддерживает CF, файл конфигурации хранится во FLASH-памяти или CF. Если устройство поддерживает мультиконфигурационный файл, они должны иметь расширение. cfg, имя по-умолчанию startup.cfg. Если устройство не поддерживает мультиконфигурационный файл, имя файла начальной конфигурации должно быть startup-config.

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

Factory configuration file: файл конфигурации, поставляемый с маршрутизатором, 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 маршрутизатор.

2.5.2.2. Настройка FTP/TFTP

Конфигурации маршрутизатора 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 ftp://user:password@ip|host-name/remote-filename <destination filename> [ascii | binary] copy tftp://ip|host-name/remote-filename <destination filename> [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.

2.5.2.3. Примеры настройки FTP/TFTP

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

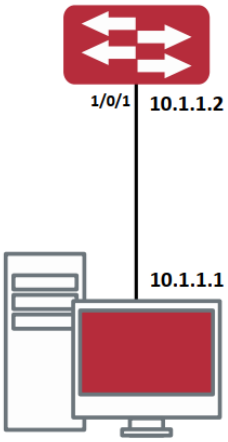


Рисунок 10. Загрузка nos.img файла FTP/TFTP-клиентом

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

2.5.2.3.1. Настройка FTP клиента.

Настройка компьютера:

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

Далее описана процедура настройки маршрутизатора:

```
Router(config)#interface vlan 1
Router(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Router(Config-if-Vlan1)#exit
Router(config)#exit
Router#copy ftp://PC:superuser@10.1.1.1/0/12_30_nos.img nos.img
```

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

2.5.2.4. Установка приоритетов загрузки IMG-файлов

После копирование IMG-file на flash память маршрутизатора, необходимо выставить приоритет загрузки (какой IMG-file будет загружаться в роли основного ПО, а какой будет в роли резервного).

Команда	Пояснение
Режим администратора	

Команда	Пояснение
boot img <Img file name> primary	Выставление парметров загрузки IMG-файла в качестве основного ПО, которое будет загружаться в первую очередь.
boot img <Img file name> backup	Выставление параметров загрузки IMG-файла, который будет выступать в роли резервного ПО и загружаться если загрузка основного ПО не удалась.
show boot-files	Просмотр загрузочных IMG-файлов (загружен в настоящий момент, будет згружен в роли основного после перезагрузки, выставлен в роли резевного), а также файлы конфигурации.

2.5.2.5. Устранение неисправностей FTP/TFTP

2.5.2.5.1. 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.
```

Если маршрутизатор 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 маршрутизатор может быть поврежден и его запуск будет невозможен. Если обновление через FTP не удается, попробуйте еще раз или используйте режим BootROM для обновления.

2.5.2.5.2. Поиск неисправностей TFTP

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

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

```
Begin to send file, please wait...
#####################################
File transfer 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...
Get Img file size success, Img file size is:14759737(bytes)
************************
#############################################################
File transfer complete.
Recv total 14759737 bytes
Begin to write local file, please wait...
Write ok.
close tftp client.
```

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

2.5.3. Использование флеш-накопителя USB для обновления устройства

Маршрутизатор оснащен USB портом. Для обновления ПО на маршрутизаторе, а также загрузки-выгрузки файлов конфигурации, можно использовать внешний флеш-накопитель USB.

2.5.3.1. Подготовка флеш-накопителя USB к обновлению.

На флеш-накопителе USB должны быть записаны файлы прошивки IMG-file или другие файлы для транспортиоровки на flash память маршрутизатора. Также необходимо свободное место на фйлеш-накопителе USB для выгрузки файлов из flash памяти маршрутизатора. Флеш-накопитель должен быть установлен в USB-разъем.

Установите флеш-накопитель USB в USB-разъем. Система автоматически выполнит поиск USB. После того, как флеш-накопитель USB установлен, модуль драйвера автоматически инициализирует драйвер USB. Позже система может прочитать или записать этот флеш-накопитель USB.

Если система обнаружит USB-накопитель и успешно загрузит драйвер, будет отображена следующая информация:

```
Router#fill_dyn_drive:dcnDrv=usb0: pFile=usb0:, transFileName=/media/sda1
```

fill_dyn_drive:dcnDrv=usb0: pFile=usb0:, transFileName=/media/sda1

%Jan 01 18:01:26.460 2006 %USB_DISK_FOUND: USB Disk <Mass Storage> has been inserted to USB port 0!

%Jan 01 18:01:26.460 2006 %USB_DISK_PARTITION_MOUNT: Mount usb0:(type:FAT),size:29862.0MB

2.5.3.2. Команды для работы с флеш-накопителем USB

1.Команды просмотра и перехода по разделам

Команда	Пояснение
Режим администратора	
show usb	Команда для отображения информации о USB флеш-накопителе с идентификатором 0.
dir usb0:/	Просмотр содержимого USB флеш-накопителя
cd usb0:/	Войти в корневой раздел флеш-накопителя USB.
dir	Просмотр содержимого USB флеш-накопителя, находясь в пазделе USB
cd usb0:/<folder name>	Переход в папку, расположенную на флеш-накопителе USB
cd	Просмотр текующего местонахождения
cd flash:/	Возвращение в корневой раздел flash памяти маршрутизатора

2. Команды транспортировки файлов с использованием флеш-накопителя

Команда	Пояснение
Режим администратора	
copy usb0:/nos.img flash:/nos.img	Копирование ПО (IMG-файла) с USB флеш-накопителя на flash память маршрутизатора
copy vsf_startup.cfg usb0:/vsf_startup.cfg	Копирование файла конфигурации из flash памяти маршрутизатора на USB флеш-накопитель (находиться необходимо в корневом разделе flash памяти маршрутизатора) Таким же образом можно скопировать любой файл.

Команда	Пояснение
copy flash:/vsf_startup.cfg usb0:/vsf_startup.cfg	Копирование файла конфигурации из flash памяти маршрутизатора на USB флеш-накопитель (из любого раздела). Таким же образом можно скопировать любой файл.
delete usb0:/<file name>	Удаление файла с флеш-накопителя USB
cd flash:/	Возвращение в корневой раздел flash памяти маршрутизатора

После копирования IMG-файлов в flash память маршрутизатора необходимо выставить параметры загрузки файлов (см. п.2.5.3.4).

3. КОНФИГУРИРОВАНИЕ ПОРТОВ

3.1. Введение

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

3.2. Список команд для конфигурирования портов

1. Вход в режим конфигурации Ethernet-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 маршрутизаторе.
   - 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-name>	Вход в режим конфигурации Ethernet-порта.

2. Конфигурация параметров сетевого порта.

Команда	Описание
Режим конфигурации порта	
media-type { dac-100cm | dac-300cm | dac-500cm | dac-50cm | fiber-100m | fiber-10g | fiber-1g }	Установка режима SFP+ портов.
shutdown no shutdown	Включение/выключение указанного порта.
description <string> no description	Назначение или отмена имени порта.
speed-duplex {auto [10 [100 [1000]] | force10-half | force10-full | force100- half | force100-full | force100-fx [module-type {auto-detected | no-phy- integrated | phy-integrated}] | {{force1g-half | force1g-full} [nonegotiate [master | slave]]}| force10g-full} no speed-duplex	Установка скорости и дуплекса на порту для 100/1000 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.
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

Команда	Описание
	NO данной команды отключает функцию контроля широковещательных штормов.
Switchport flood-control {bcast|mcast|ucast}	Конфигурирование маршрутизатора не передавать широковещательные, многопользовательские и персональные
no Switchport flood-control {bcast|mcast|ucast}	Пакеты в указанный порт, команда «no» отключает данную функцию.
rate-violation {all <200-2000000> | broadcast <200-2000000> | control {block | shutdown} | multicast <200-2000000> | unicast <200-2000000> } <200-2000000> no rate-violation	Устанавливает максимальную скорость приема пакетов на порту. Если скорость принятия пакетов превышает разрешенную, команда выключает этот порт и конфигурирует время восстановления порта (по умолчанию 300с). Команда «no» отключает установку.
Режим глобального конфигурирования	
port-rate-statistics interval <5-600>	Конфигурация интервала сбора статистики по скорости.

3. Виртуальный тест кабеля.

Команда	Описание
Режим администратора	
virtual-cable-test interface ethernet <IFNAME>	Виртуальный тест кабеля на порте.

3.3. Примеры конфигурации порта

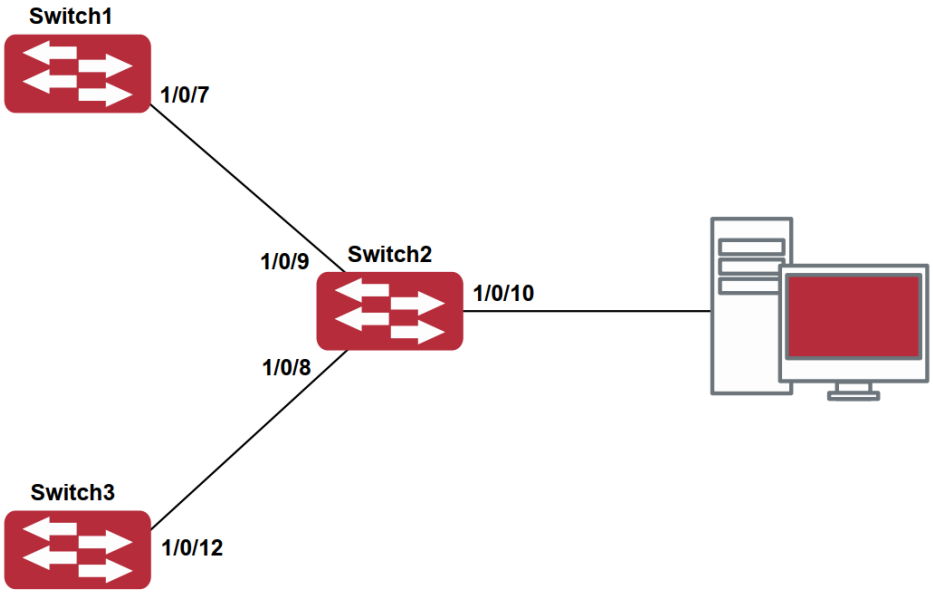


Рисунок 11. Пример конфигурации порта

VLAN не сконфигурированы на маршрутизаторе. По умолчанию используется VLAN1.

Маршрутизатор	Порт	Свойства
Router1	1/0/7	Лимит входящей полосы: 50 Mb
Router2	1/0/8	Зеркалированный порт источника
	1/0/9	100 Mbps full, зеркалированный порт источника
	1/0/10	1000 Mbps full, зеркалированный порт назначения
Router3	1/0/12	100 Mbps full

Конфигурация приведена ниже:

```
Router1:
Router1(config)#interface ethernet 1/0/7
Router1(Config-If-Ethernet1/0/7)#bandwidth control 50000 receive

Router2:
Router2(config)#interface ethernet 1/0/9
Router2(Config-If-Ethernet1/0/9)#speed-duplex force100-full
Router2(Config-If-Ethernet1/0/9)#exit
Router2(config)#interface ethernet 1/0/10
```

```
Router2(Config-If-Ethernet1/0/10)#speed-duplex force1g-full
Router2(Config-If-Ethernet1/0/10)#exit
Router2(config)#monitor session 1 source interface ethernet1/0/8;1/0/9
Router2(config)#monitor session 1 destination interface ethernet 1/0/10

Router3:
Router3(config)#interface ethernet 1/0/12
Router3(Config-If-Ethernet1/0/12)#speed-duplex force100-full
Router3(Config-If-Ethernet1/0/12)#exit
```

3.4. Устранение неисправностей на порту

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

- Два соединенных оптических интерфейса не поднимаются если один интерфейс настроен на автоопределение, а на втором жестко установлены скорость и дуплекс. Это определяется стандартом IEEE 802.3.
- Не рекомендуется следующая конфигурация: включение контроля трафика и одновременно установление лимита для многопользовательских пакетов на том же порту; установка одновременно контроля за широковещательными, многопользовательскими и персональными пакетами с неизвестным назначением и ограничения полосы на порту. Если такие комбинации установлены, пропускная способность порта может оказаться меньше ожидаемой.

4. КОНФИГУРАЦИЯ ФУНКЦИИ РАСПОЗНАВАНИЯ ПЕТЛИ НА ПОРТУ

4.1. Введение в функцию распознавания петли

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

Когда пакет с MAC-адресом источника, уже изученным маршрутизатором, 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.

4.2. 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 interval time range <5-300>s} {no loopback interval time range <1-30>s} 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 ID> no loopback-detection specified-vlan <vlan ID>	Включение и выключение функции распознавания петли

3. Вывод отладочной информации по распознаванию петли.

Команда	Описание
Режим администратора	
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

4. Конфигурирование режима восстановления при распознавании петли.

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

4.3. Примеры функции распознавания петли на порту

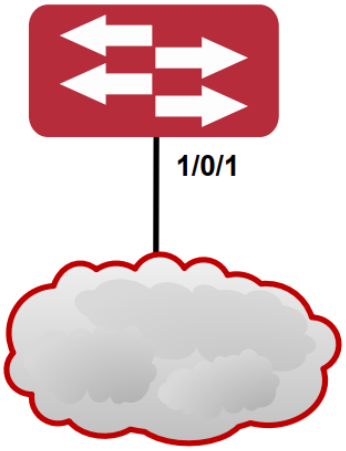


Рисунок 12. Типичный пример подключения

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

Последовательность конфигурации маршрутизатора:

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

4.4. Решение проблем с функцией распознавания петли на порту

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

5. НАСТРОЙКА ФУНКЦИИ LLDP

5.1. 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 устройствам, таким, как маршрутизаторы, маршрутизаторы и точки доступа уведомлять о своем существовании другие узлы сети и сохранять информацию обо всех соседних устройствах. Как следствие, 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 маршрутизаторы с какими соединены и т. п. Она так же может показывать маршруты между клиентами, маршрутизаторами, 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.

5.2. Список команд для конфигурирования LLDP

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

1. Включение LLDP на устройстве.

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

2. Включение функции LLDP на порту.

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

3. Конфигурация статуса LLDP на порту.

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

4. Конфигурация интервала обновления сообщений LLDP.

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

5. Отображение отладочной информации по функции LLDP.

Команда	Описание
Режим администратора	
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.

5.3. Типовой пример функции LLDP

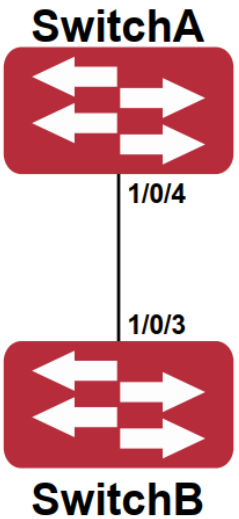


Рисунок 13. Типовой пример конфигурации функции LLDP

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

Маршрутизатор A. Последовательность команд конфигурации:

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

Маршрутизатор B. Последовательность команд конфигурации:

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

5.4. 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.

6. КОНФИГУРИРОВАНИЕ MTU

6.1. 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 маршрутизатором.

6.2. Конфигурирование MTU

1. Включение функции MTU

Команда	**Описание**
Режим глобального конфигурирования	
mtu [MTU size in bytes < 1500-9828 >] no mtu enable	Включает функцию приема/посылки JUMBO-фреймов. Команда «no» выключает функцию приема/посылки JUMBO-фреймов.

7. НАСТРОЙКА DDM

7.1. Введение

7.1.1. Краткое введение в DDM

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

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

Применение DDM показано далее:

1. Прогноз продолжительности жизни модуля.

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

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

1.2. Высокая RX-мощность приведёт 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 маршрутизатора.

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.

7.1.2. Функции DDM

Описание DDM показано в следующем примере:

1. Просмотр информации мониторинга на приемопередатчике.

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

2. Определение значения порога пользователем.

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

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

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

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

3. Контроль трансивера.

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

7.2. 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 режим глобального конфигурирования	
Show transceiver [interface ethernet < IFNAME >] [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 глобального конфигурирования	
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 состоние неисправности. После отключения функции на порте, информация о неисправности будет стерта.

7.3. Примеры применения DDM

Пример 1:

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

- 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:

  Router #show transceiver

Interface	Temp (°C)	Voltage (V)	Bias (mA)	RX Power (dBM)	TX Power (dBM)
1/0/21	28	3,28	23,34	−3,75	−0,79
1/0/23	46	3,28	26,00	−2,10	−2,21

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

  Router #show transceiver interface ethernet 1/0/21-22; 23

Interface	Temp (°C)	Voltage (V)	Bias (mA)	RX Power (dBM)	TX Power (dBM)
1/0/21	28	3,28	23,34	−3,75	−0,79
1/0/22	N/A	N/A	N/A	N/A	N/A
1/0/23	46	3,28	26,00	−2,10	−2,21

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

Router#show transceiver interface ethernet 1/0/21-22;24 detail

Ethernet 1/0/21 transceiver detail information:

Base information:

SFP found in this port, manufactured by company, on Sep 29 2010.

Type is 1000BASE-SX, Link length is 550 m for 50um Multi-Mode Fiber.

Link length is 270 m for 62.5um Multi-Mode Fiber.

Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.

Brief alarm information:

RX loss of signal

Voltage high

RX power low

Detail diagnostic and threshold information:

Diagnostic Threshold

	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn
Temperature (°C)	33,00	70,00	0,00	70,00	0,00
Voltage (V)	7,31 (A+)	5,00	0,00	5,00	0,00
Bias current (mA)	6,11 (W+)	10,30	0,00	5,00	0,00
RX Power (dBM)	−30,54 (A−)	9,00	−25,00	9,00	−25,00
TX Power (dBM)	−6,01	9,00	−25,00	9,00	−25,00

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

Ethernet 1/0/24 transceiver detail information:

Base information:

SFP found in this port, manufactured by company, on Sep 29 2010.

Type is 1000BASE-SX, Link length is 550 m for 50um Multi-Mode Fiber.

Link length is 270 m for 62.5um Multi-Mode Fiber.

Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.

Brief alarm information: N/A

Detail diagnostic and threshold information: N/A

Пример 2:

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

Шаг 1: Просмотр подробной информации о DDM.

Router#show transceiver interface ethernet 1/0/21 detail

Ethernet 1/0/21 transceiver detail information:

Base information:

……

Brief alarm information:

RX loss of signal

Voltage high

RX power low

Detail diagnostic and threshold information:

Diagnostic Threshold

	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn
Temperature (°C)	33,00	70,00	0,00	70,00	0,00
Voltage (V)	7,31 (A+)	5,00	0,00	5,00	0,00
Bias current (mA)	6,11 (W+)	10,30	0,00	5,00	0,00
RX Power (dBM)	−30,54 (A−)	9,00	−25,00	9,00	−25,00
TX Power (dBM)	−13,00	19,00	−25,00	9,00	−25,00

Шаг 2: Настройка порогового значения TX-power на оптическом интерфейсе, нижнее значение порогового оповещения – 12, нижнее значение пороговой сигнализации – 10,00.

Router#config

Router(config)#interface ethernet 1/0/21

Router(config-if-ethernet1/0/21)#transceiver threshold tx-power low- warning -12

Router(config-if-ethernet1/0/21)#transceiver threshold tx-power low- alarm -10.00

Шаг 3: Просмотр подробной информации о DDM на оптическом модуле. Сигнализация использует пороговое значение, настраиваемое пользователем, пороговое значение, настроенное производителем обозначено скобками. Сигнализация с ‘A−’ как −13,01 меньше, чем −12,00.

Router#show transceiver interface ethernet 1/0/21 detail

Ethernet 1/0/21 transceiver detail information:

Base information:

……

Brief alarm information:

RX loss of signal

Voltage high

RX power low

TX power low

Detail diagnostic and threshold information:

	Diagnostic		**Threshold**		
	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn
Temperature (°C)	33,00	70,00	0,00	70,00	0,00
Voltage (V)	7,31 (A+)	5,00	0,00	5,00	0,00
Bias current (mA)	6,11 (W+)	10,30	0,00	5,00	0,00
RX Power (dBM)	−30,54 (A−)	9,00	−25,00	9,00	−25,00
TX Power (BM)	−13,01(A−)	9,00	−12,00 (−25,00)	9,00	−10,00 (−25,00)

Пример 3:

В порт Ethernet 1/0/21 включен оптический модуль с DDM. Включение мониторинга трансивера на порте, после просмотра мониторинга на оптическом модуле.

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

Router(config)#show transceiver threshold-violation interface ethernet 1/0/21-22

Ethernet 1/0/21 transceiver threshold-violation information:

Transceiver monitor is disabled. Monitor interval is set to 30 minutes.

The last threshold-violation doesn't exist.

Ethernet 1/0/22 transceiver threshold-violation information:

Transceiver monitor is disabled. Monitor interval is set to 30 minutes.

The last threshold-violation doesn't exist.

Шаг 2: Включение мониторинга трансивера на Ethernet 21.

Router(config)#interface ethernet 1/0/21

Router(config-if-ethernet1/0/21)#transceiver-monitoring enable

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

```
Router(config-if-ethernet1/0/21)#quit
Router(config)#show transceiver threshold-violation interface ethernet 1/0/21-22
Ethernet 1/0/21 transceiver threshold-violation information:
Transceiver monitor is enabled. Monitor interval is set to 30 minutes.
The current time is Jan 02 12:30:50 2011.
The last threshold-violation time is Jan 02 11:00:50 2011.
Brief alarm information:
RX loss of signal
RX power low
Detail diagnostic and threshold information:
```

	Diagnostic		**Threshold**		
	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn
Temperature (°C)	33,00	70,00	0,00	70,00	0,00
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 (−34,00)	9,00	−25,00
TX Power (dBM)	−1,01	9,00	−12,05	9,00	−10,00

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

7.3.1. 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 будет показана.
- Убедитесь, что конфигурация SNMP работает, иначе оповещение о событии не сможет оповестить систему сетевого управления.
- Не все маршрутизаторы поддерживают SFP с DDM или XFP с DDM, убедитесь в использовании маршрутизатора с поддержкой соответствующей функции.

- Использование команд show transceiver или show transceiver detail может занять много времени, так как маршрутизатор 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.

8. LLDP-MED

8.1. 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 связью 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.

8.2. Конфигурация LLDP-MED

1. Базовая конфигурация

Команда	Описание
Режим конфигурирования порта	
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.
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.

8.3. Пример настройки LLDP-MED

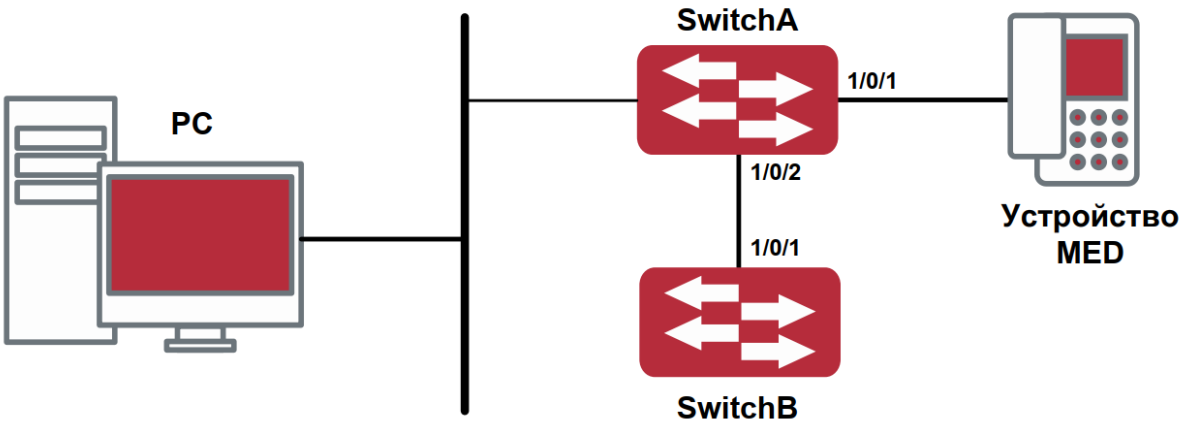


Рисунок 14. Топология базовой конфигурации LLDP-MED

1. Настройка Router A

RouterA(config)#interface ethernet1/0/1

RouterA (Config-If-Ethernet1/0/1)# lldp enable

RouterA (Config-If-Ethernet1/0/1)# lldp mode both（this configuration can be omitted, the default mode is RxTx）

RouterA (Config-If-Ethernet1/0/1)# lldp transmit med tlv capability

RouterA (Config-If-Ethernet1/0/1)# lldp transmit med tlv network policy

RouterA (Config-If-Ethernet1/0/1)# lldp transmit med tlv inventory

RouterB (Config-If-Ethernet1/0/1)# network policy voice tag tagged vid 10 cos 5 dscp 15

RouterA (Config-If-Ethernet1/0/1)# exit

RouterA (config)#interface ethernet1/0/2

RouterA (Config-If-Ethernet1/0/2)# lldp enable

RouterA (Config-If-Ethernet1/0/2)# lldp mode both

2. Настройка Router B

RouterB (config)#interface ethernet1/0/1

RouterB(Config-If-Ethernet1/0/1)# lldp enable

RouterB (Config-If-Ethernet1/0/1)# lldp mode both

RouterB (Config-If-Ethernet1/0/1)# lldp transmit med tlv capability

RouterB (Config-If-Ethernet1/0/1)# lldp transmit med tlv network policy

RouterB (Config-If-Ethernet1/0/1)# lldp transmit med tlv inventory

RouterB (Config-If-Ethernet1/0/1)# network policy voice tag tagged vid cos 4

3. Verify the configuration

Просмотр глобального статуса и статуса интерфейса на RouterA

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

SysCapSupported :4
SysCapEnabled :4

LLDP MED Information :
MED Codes:
(CAP)Capabilities, (NP) Network Policy
(LI) Location Identification, (PSE)Power Source Entity
(PD) Power Device, (IN) Inventory
MED Capabilities:CAP,NP,PD,IN
MED Device Type: Endpoint Class III
Media Policy Type :Voice
Media Policy :Tagged
Media Policy Vlan id :10
Media Policy Priority :3
Media Policy Dscp :5 Power Type : PD
Power Source :Primary power source
Power Priority :low
Power Value :15.4 (Watts) Hardware Revision:
Firmware Revision:4.0.1
Software Revision:6.2.30.0
Serial Number:
Manufacturer Name:****
Model Name:Unknown
Assert ID:Unknown
IEEE 802.3 Information :

auto-negotiation support: Supported

auto-negotiation support: Not Enabled

PMD auto-negotiation advertised capability: 1

operational MAU type: 1

RouterA# show lldp neighbors interface ethernet 1/0/2

Port name : interface ethernet 1/0/2

Port Remote Counter : 1

Neighbor Index: 1

Port name : Ethernet1/0/2

Port Remote Counter : 1

TimeMark :20

ChassisIdSubtype :4

ChassisId :00-03-0f-00-00-02

PortIdSubtype :Local

PortId 1

PortDesc :Ethernet1/0/1

SysName :****

SysDesc :*****

SysCapSupported :4

SysCapEnabled :4

Пояснение:

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

8.4. Устранение неисправностей LLDP-MED

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

- Убедитесь, что LLDP включен глобально.
- Только устройство сетевого соединения получает LLDP-пакеты с LLDP-MED TLV от ближайшего устройства MED, он так же посылает LLDP-MED TLV. Если на устройстве сетевого соединения настроена команда для отправки LLDP-MED TLV, пакеты без LLDP-MED TLV посылаются на порт, что означает, что никакой информации порт не получает и на порте отключена функция посылки информации LLDP-MED TLV.

- Если соседние устройства посылают информацию LLDP-MED устройству сетевого соединения, но она не является информацией LLDP-MED, проверяемая командой show lldp neighbors, что означает, что отправляемая информация LLDP-MED к соседним устройствам является ошибочной.

9. НАСТРОЙКА ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ VLAN

9.1. Конфигурирование VLAN

9.1.1. 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 маршрутизаторе 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.

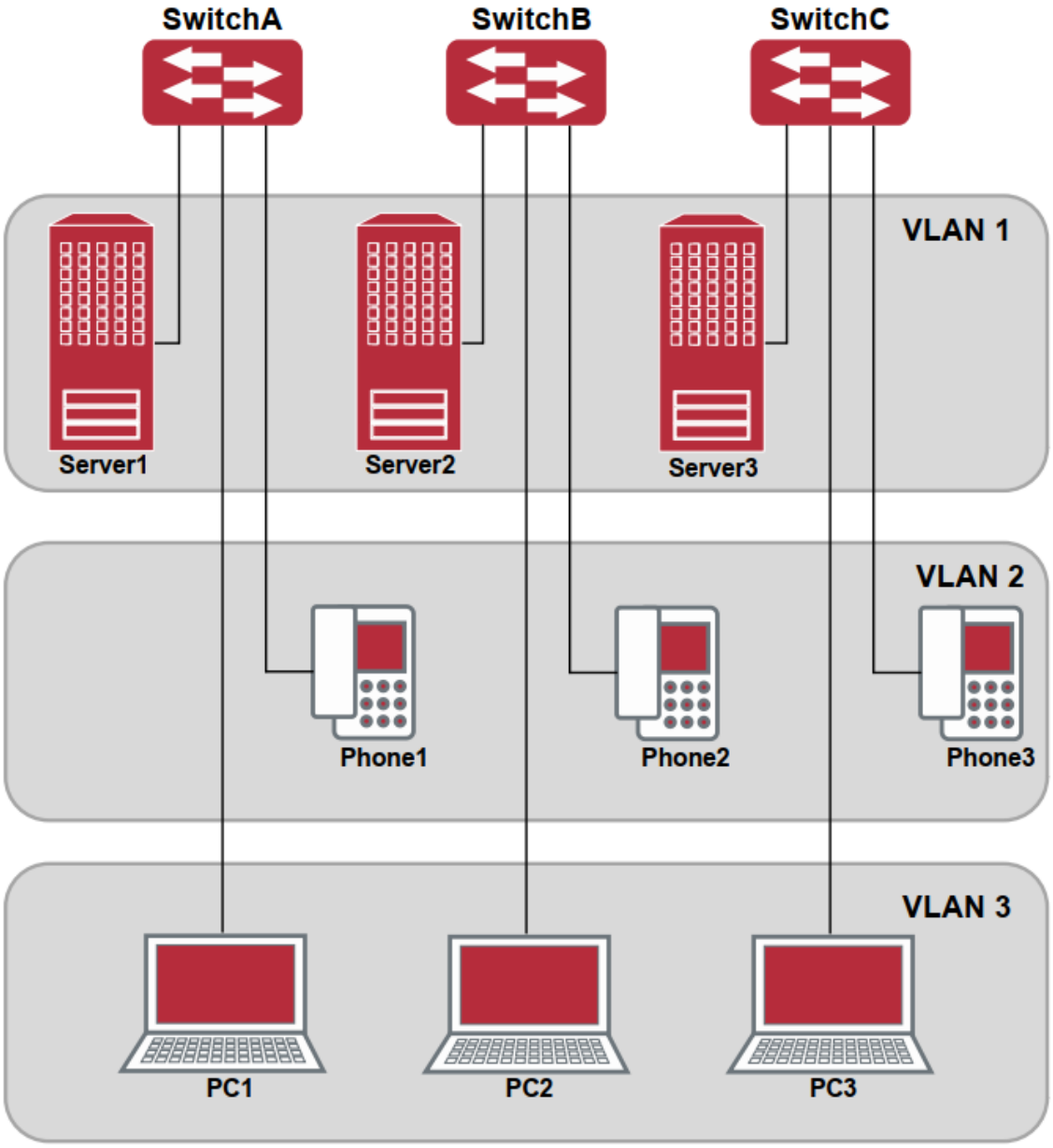


Рисунок 15. Логическое определение сети VLAN

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 маршрутизатора 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 маршрутизаторами или подключения пользовательских устройств.

Порты типа Hybrid также позволяют пересылать пакеты нескольких VLAN'ов. Они могут использоваться для соединения между маршрутизаторами 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 маршрутизаторе описывается в стандарте 802.1Q. Данная глава детально объясняет использование и конфигурацию VLAN'ов и GVRP.

9.1.2. Конфигурирование VLAN

1. Создание или удаление VLAN.
2. Установка или удаление имени VLAN'а.
3. Присоединение порта маршрутизатора к VLAN'у.
4. Установка типа порта маршрутизатора.
5. Настройка транкового порта.
6. Настройка порта доступа.
7. Настройка гибридного порта.

1. Создание или удаление VLAN.

Команда	**Описание**
Режим глобального конфигурирования	
vlan <1-4094> no vlan <1-4094>	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 маршрутизатора к VLAN’у.

Команда	Описание
VLAN Mode	
switchport interface { IFNAME | ethernet <IFNAME> | port-channel < IFNAME> } no switchport interface { IFNAME | ethernet < IFNAME> | port-channel < IFNAME> }	Назначение порта маршрутизатора VLAN’у

4. Установка типа порта маршрутизатора.

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

5. Настройка транкового порта.

Команда	Описание
Режим конфигурирования порта	
Switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD} no Switchport trunk allowed vlan	Установка/удаление VLAN’ов, приписанных к этому транку. Команда «no» восстанавливает значение по умолчанию.
Switchport trunk native vlan <vlan-id> no Switchport trunk native vlan	Установка/удаление PVID для транкового порта.

6. Настройка порта доступа.

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

7. Настройка гибридного порта.

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

9.1.3. Типичное применение VLAN'а

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 маршрутизатор, требования к связи между площадками удовлетворяются, если маршрутизаторы могут выполнять обмен трафиком VLAN.

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

Транковые порты с обеих сторон подключены к транковому каналу для передачи между узлами трафика VLAN'а. 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.

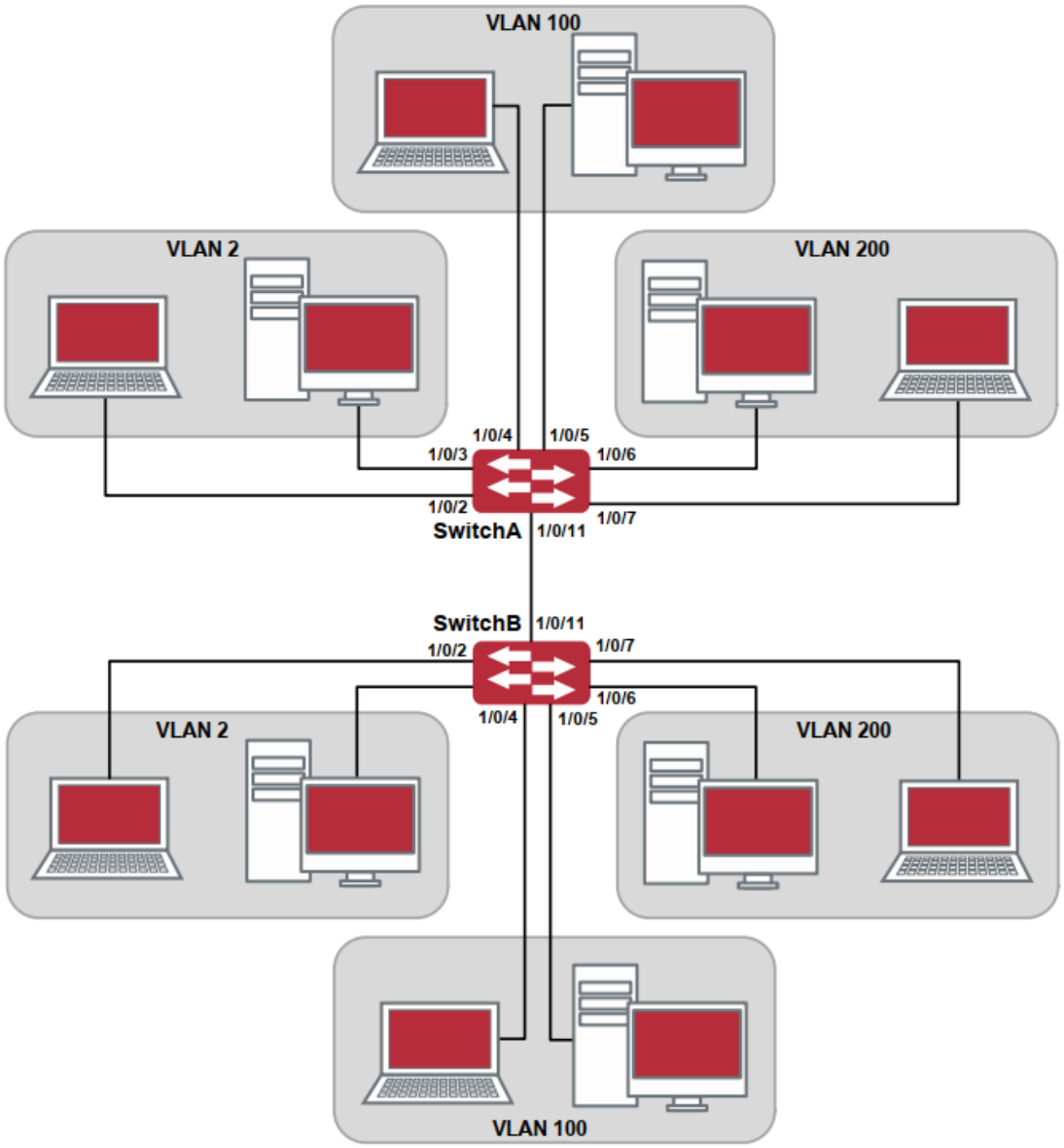


Рисунок 16. Типичная топология применения VLAN’a

Шаги конфигурации описаны ниже:

Маршрутизатор A:

Router(config)#vlan 2

Router(Config-Vlan2)#Switchport interface ethernet 1/0/2-3

Router(Config-Vlan2)#exit

Router(config)#vlan 100

Router(Config-Vlan100)#Switchport interface ethernet 1/0/4-5

Router(Config-Vlan100)#exit

Router(config)#vlan 200

```
Router(Config-Vlan200)#Switchport interface ethernet 1/0/6-7
Router(Config-Vlan200)#exit
Router(config)#interface ethernet 1/0/11
Router(Config-If-Ethernet1/0/11)#Switchport mode trunk
Router(Config-If-Ethernet1/0/11)#exit
Router(config)#
```

Маршрутизатор B:

```
Router(config)#vlan 2
Router(Config-Vlan2)#Switchport interface ethernet 1/0/2-3
Router(Config-Vlan2)#exit
Router(config)#vlan 100
Router(Config-Vlan100)#Switchport interface ethernet 1/0/4-5
Router(Config-Vlan100)#exit
Router(config)#vlan 200
Router(Config-Vlan200)#Switchport interface ethernet 1/0/6-7
Router(Config-Vlan200)#exit
Router(config)#interface ethernet 1/0/11
Router(Config-If-Ethernet1/0/11)#Switchport mode trunk
Router(Config-If-Ethernet1/0/11)#exit
```

9.1.4. Типичное применение гибридных портов

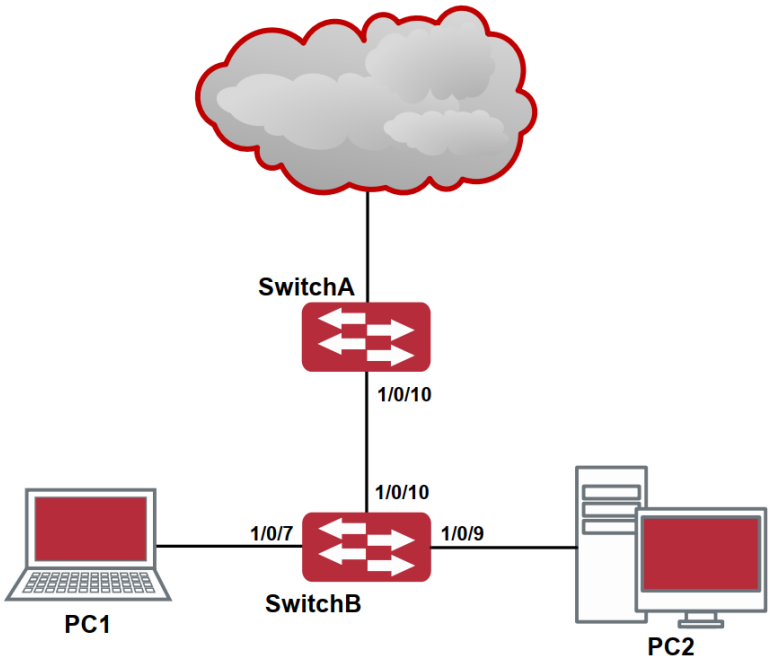


Рисунок 17. Типичное применение гибридного порта

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

Мы можем реализовать эту схему через гибридный порт.

Конфигурация объектов как описано ниже:

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

Шаги конфигурации описаны ниже:

Маршрутизатор A:

```
Router(config)#vlan 10
Router(Config-Vlan10)#Switchport interface ethernet 1/0/10
```

Маршрутизатор B:

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

```
Router(Config-If-Ethernet1/0/10)#exit
```

10. КОНФИГУРИРОВАНИЕ ФУНКЦИЙ 3-ГО УРОВНЯ

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

10.1. Интерфейс 3-го уровня

10.1.1. Начальные сведения об интерфейсах 3-го уровня

В маршрутизаторах 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). Маршрутизатор может использовать IP-адреса, установленные на интерфейсах 3-го уровня, для коммуникации с другими устройствами через IP-протокол. Маршрутизатор может пересылать IP-пакеты между разными интерфейсами 3-го уровня.

10.1.2. 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 маршрутизаторе.

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.

10.2. Настройка протокола IP

10.2.1. Введение в IPv4, IPv6

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

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

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

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

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

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

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

По сравнению с IPv4, конструкция заголовка IPv6 более совершенна. Заголовок содержит меньше полей данных, из него изъята контрольная сумма, что увеличивает скорость обработки основного заголовка IPv6. В заголовке IPv6 поле фрагмента может быть показано как дополнительное расширенное поле, поэтому больше не будет необходимости в фрагментации пакетных данных в процессе их передачи в

маршрутизаторе. Кроме того, эффективность работы маршрутизатора повышается за счет механизма обнаружения маршрута MTU (Path MTU Discovery Mechanism) работающего с источником пакетных данных.

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

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

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

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

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

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

10.2.2. Настройка IP-протокола

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

10.2.2.1. 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
Режим глобального конфигурирования	
ip route 0.0.0.0 0.0.0.0 <A.B.C.D> no ip route 0.0.0.0 0.0.0.0 <A.B.C.D>	Настройка статической маршрутизации. Команда «no» отменяет настройку.

10.2.2.2. Настройка адреса IPv6

Последовательность настройки адреса IPv6:

1. Базовая настройка IPv6.
   1.1. Настройка адреса IPv6-интерфейса.

1. Базовая настройка IPv6.
   1.1. Настройка адреса IPv6-интерфейса.

Команда	Описание
Режим конфигурирования интерфейса	
ipv6 address <ipv6-address/prefix-length> no ipv6 address <ipv6-address/prefix-length>	Настройка IPv6-адреса, включая объединяемые глобальные unicast-адреса, site-local-адреса. Команда «no ipv6 address <ipv6- address/prefix-length>» отменяет IPv6-адрес.

10.2.3. 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 маршрутизаторе (выключено по умолчанию).

10.3. ARP

10.3.1. Введение в ARP

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

10.3.2. Список задач конфигурации ARP

Список задач конфигурации ARP:

1. Настроить статический ARP.

Команда	Описание
Режим 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.

10.3.3. Поиск неисправностей ARP

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

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

11. КОНФИГУРАЦИЯ DHCP

11.1.1. 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:

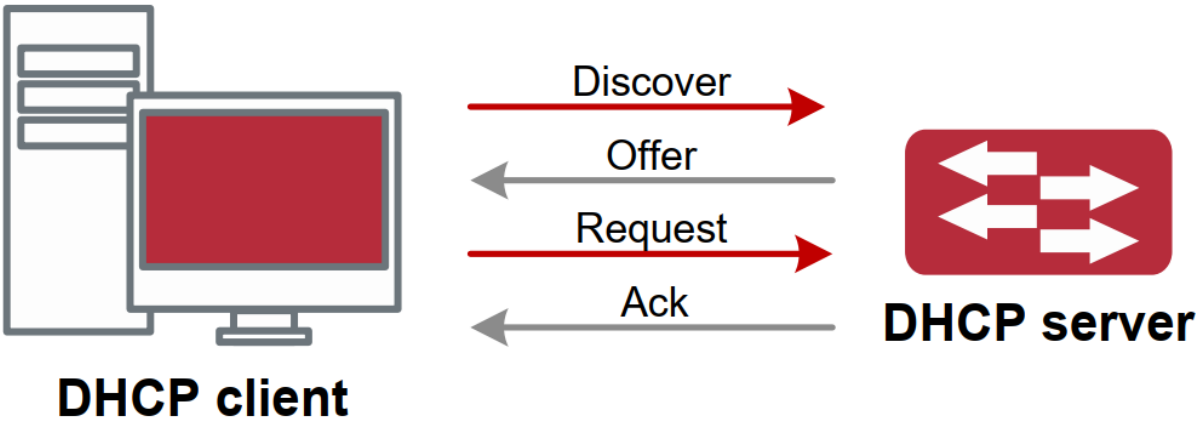


Рисунок 18. Взаимодействие протокола DHCP

Разъяснение:

DHCP-клиент рассылает в локальную подсеть широковещательные пакеты DHCPDISCOVER.

DHCP-сервер при получении пакета DHCPDISCOVER отправляет DHCP-клиенту пакет DHCPOFFER вместе с IP-адресами и другими сетевыми параметрами.

DHCP шлет широковещательный пакет DHCPREQUEST с информацией о DHCP-сервере, который он выбрал из DHCPOFFER-пакетов.

Выбранный клиентом DHCP-сервер отправляет пакет DHCPACK и клиент получает IP-адрес и другие параметры.

Эти четыре шага производят процесс динамической настройки хоста.

Однако, если DHCP-сервер и DHCP-клиент находятся в разных подсетях, сервер не получит широковещательные DHCP-пакеты, отправленные клиентом и не ответит ему. В этом случае необходим DHCP-ретранслятор (relay) для передачи таких DHCP-пакетов между клиентом и сервером.

Маршрутизатор 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.

11.2. 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**
Режим глобального конфигурирования	
service dhcp no service dhcp	Включить/выключить сервис DHCP.

2. Настроить адресный пул DHCP.
   2.1. Создать/удалить адресный пул DHCP.

Команда	**Описание**
Режим глобального конфигурирования	
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	

Команда	Описание
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 [<addresRouterA>[<addresRouterB>[…<address8>]]] no default-router	Настройка шлюза по умолчанию для DHCP-клиентов. Команда «no» отменяет шлюз по умолчанию.
dns-server [<addresRouterA>[<addresRouterB>[…<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.
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.
Режим глобального конфигурирования	
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	
host <address> [<mask> | <prefix-length>]	Задать/удалить IP-адрес, который будет назначен заданному клиенту.

Команда	Описание
no host	

11.3. Примеры конфигурации DHCP

Сценарий 1:

Чтобы упростить настройку, компания использует маршрутизатор в качестве DHCP-сервера. Адрес в VLAN-е управления - 10.16.1.2/16. Локальная сеть разделена на две сети – A и B, в соответствии с расположением офисов. Настройки сети для расположений A и B показаны ниже.

Пул A (сеть 10.16.1.0)		**Пул B (сеть 10.16.2.0)**	
Устройство	IP address	Устройство	IP address
Шлюз по умолчанию	10.16.1.200 10.16.1.201	Шлюз по умолчанию	10.16.1.200 10.16.1.201
DNS-сервер	10.16.1.202	DNS-сервер	10.16.1.202
WINS-сервер	10.16.1.209	WWW-сервер	10.16.1.209
Тип узла WINS	H-узел		
Время аренды	3 дня	Время аренды	1 день

В расположении A машине с MAC-адресом 08-c6-b3-23-dc-ab назначен фиксированный IP-адрес 10.16.1.210 и имя хоста «management».

```
Router(config)#service dhcp
Router(config)#interface vlan 1
Router(Config-Vlan-1)#ip address 10.16.1.2 255.255.0.0
Router(Config-Vlan-1)#exit
Router(config)#ip dhcp pool A
Router(dhcp-A-config)#network 10.16.1.0 24
Router(dhcp-A-config)#lease 3
Router(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201
Router(dhcp-A-config)#dns-server 10.16.1.202
Router(dhcp-A-config)#netbios-name-server 10.16.1.209
Router(dhcp-A-config)#netbios-node-type H-node
Router(dhcp-A-config)#exit
Router(config)#ip dhcp excluded-address 10.16.1.200 10.16.1.201
```

```
Router(config)#ip dhcp pool B
Router(dhcp-B-config)#network 10.16.2.0 24
Router(dhcp-B-config)#lease 1
Router(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201
Router(dhcp-B-config)#dns-server 10.16.2.202
Router(dhcp-B-config)#option 72 ip 10.16.2.209
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 10.16.2.200 10.16.2.201
Router(config)#ip dhcp pool A1
Router(dhcp-A1-config)#host 10.16.1.210
Router(dhcp-A1-config)#hardware-address 08-c6-b3-23-dc-ab
Router(dhcp-A1-config)#exit
```

Руководство по использованию: Когда DHCP/BOOTP-клиент подключается к VLAN1 порту маршрутизатора, 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 маршрутизатором.

11.4. 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-маршрутизатора, 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.

12. КОНФИГУРАЦИЯ DHCPV6

12.1. 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.

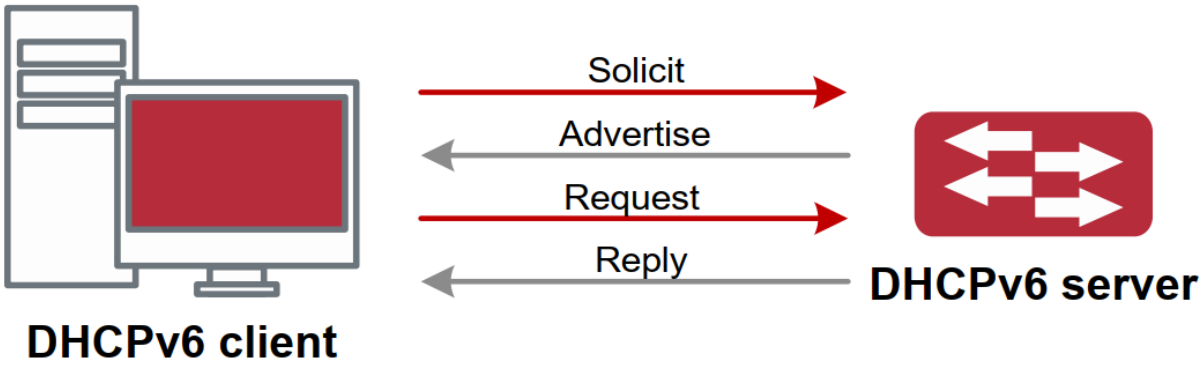


Рисунок 19. Согласование DHCPv6

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

маршрутизаторе 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.

12.2. 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.

4. Настроить адресный пул DHCPv6.
   4.1. Создать/удалить адресный пул DHCPv6.

Команда	**Описание**
Режим глобального конфигурирования	
ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>	Создать/удалить адресный пул DHCPv6.

4.2. Настроить параметры адресного пула DHCPv6

Команда	Описание
Режим конфигурации адресного пула DHCPv6	
network-address <ipv6-pool-start-address> {<ipv6-pool-end-address> | <prefix- length>} 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.
Lifetime {<valid-time> | infinity} {<preferred-time> | infinity} no lifetime	Настроить время действия или предпочтительное время адресного пула DHCPv6.

5. Включить функцию DHCPv6-сервера на порту.

Команда	Описание
Режим конфигурации интерфейса	
ipv6 dhcp server <poolname> [[rapid-commit] no ipv6 dhcp server <poolname>	Включить функцию DHCPv6-сервера на определенном порту и привязать используемый DHCPv6-адресный пул.

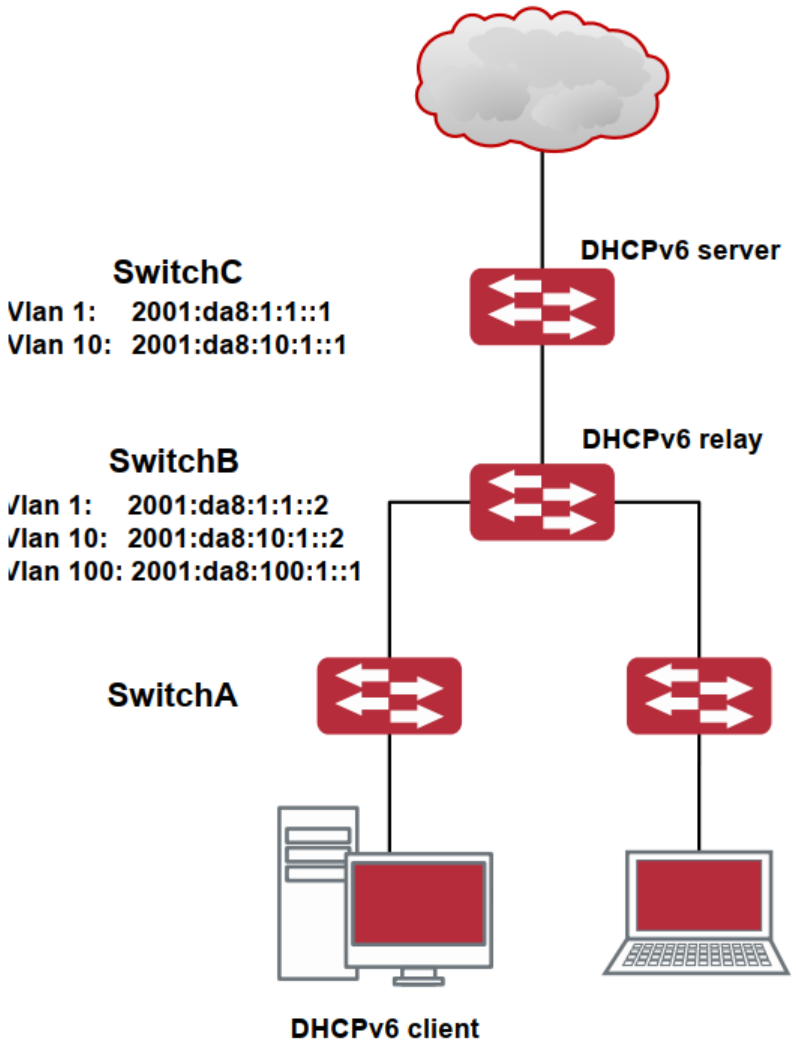
12.3. Примеры конфигурации DHCPv6

Пример 1:

При развертывании сетей IPv6 маршрутизаторы серии могут быть настроены в качестве DHPv6-серверов для управления распределением адресов IPv6. Поддерживаются оба режима DHCPv6 – с отслеживанием состояния и без него.

Топология:

На уровне доступа используется маршрутизатор 1 для подключения пользователей общежития. На первом уровне агрегации маршрутизатор 2 настроен как DHCPv6-ретранслятор. На втором уровне агрегации маршрутизатор 3 настроен как DHCPv6-сервер и соединен с магистральной сетью. На компьютерах должна быть установлена ОС не ниже Windows Vista, или любая другая в которой есть DHCPv6-клиент.



Конфигурация RouterC:

```
RouterC>enable
RouterC#config
RouterC(config)#service dhcpv6
RouterC(config)#ipv6 dhcp pool EastDormPool
RouterC(dhcpv6-EastDormPool-config)#network-address 2001:da8:100:1::1
2001:da8:100:1::100
RouterC(dhcpv6-EastDormPool-config)#excluded-address 2001:da8:100:1::1
RouterC(dhcpv6-EastDormPool-config)#dns-server 2001:da8::20
RouterC(dhcpv6-EastDormPool-config)#dns-server 2001:da8::21
RouterC(dhcpv6-EastDormPool-config)#domain-name dhcpv6.com
RouterC(dhcpv6-EastDormPool-config)#lifetime 1000 600
RouterC(dhcpv6-EastDormPool-config)#exit
RouterC(config)#interface vlan 1
RouterC(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::1/0/64
```

```
RouterC(Config-if-Vlan1)#exit
RouterC(config)#interface vlan 10
RouterC(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::1/0/64
RouterC(Config-if-Vlan10)#ipv6 dhcp server EastDormPool preference 80
RouterC(Config-if-Vlan10)#exit
RouterC(config)#
```

Конфигурация RouterB:

```
RouterB>enable
RouterB#config
RouterB(config)#service dhcpv6
RouterB(config)#interface vlan 1
RouterB(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::2/64
RouterB(Config-if-Vlan1)#exit
RouterB(config)#interface vlan 10
RouterB(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::2/64
RouterB(Config-if-Vlan10)#exit
RouterB(config)#interface vlan 100
RouterB(Config-if-Vlan100)#ipv6 address 2001:da8:100:1::1/0/64
RouterB(Config-if-Vlan100)#no ipv6 nd suppress-ra
RouterB(Config-if-Vlan100)#ipv6 nd managed-config-flag
RouterB(Config-if-Vlan100)#ipv6 nd other-config-flag
RouterB(Config-if-Vlan100)#ipv6 dhcp relay destination 2001:da8:10:1::1
RouterB(Config-if-Vlan100)#exit
RouterB(config)#
```

12.4. 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 маршрутизаторам со включенным DHCPv6, не могут получить IPv6-адрес. В этой ситуации в первую очередь необходимо проверить, подключены ли порты, к которым подключены хосты, к порту, к которому подключен DHCPv6-сервер. Если подключено напрямую, убедиться, что адресный пул IPv6 VLAN-а, к которому принадлежит порт, находится в одной подсети с адресным пулом, настроенным на DHCPv6-сервере. Если подключены не на прямую, и между хостом и сервером настроен DHCPv6-ретранслятор, необходимо в первую очередь проверить, настроен ли правильный IPv6-адрес на

интерфейсе маршрутизатора, 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.

13. ОПЦИИ 60 И 43 DHCP

13.1. 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.

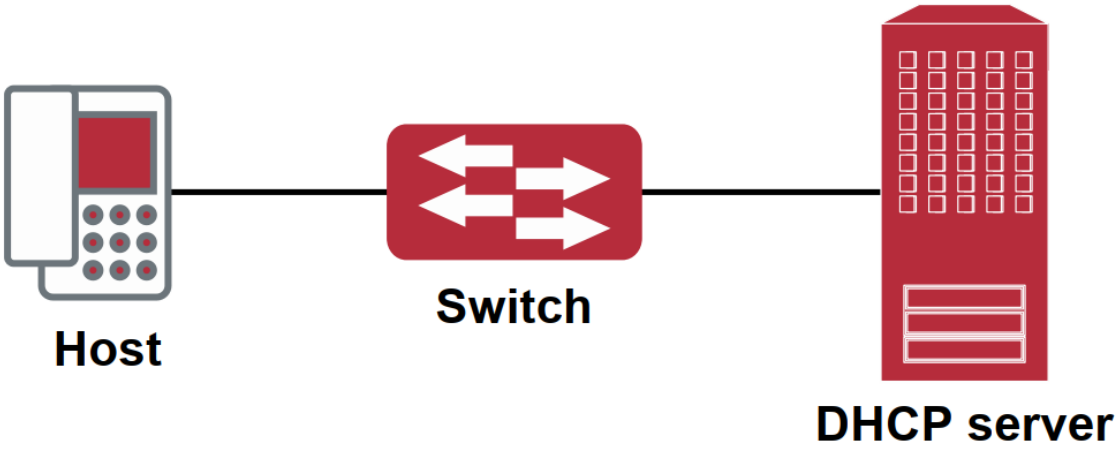
13.2. Настройка опций 60 и 43 на DHCP

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

Команда	Описание
option 43 ip A.B.C.D	Настройка опции 43 в символьной строке в формате IP в режиме ip-адресного пространства DHCP
no option 60	Удаление настроек опции 60 в режиме адресного пространства
no option 43	Удаление настроек опции 43 в режиме адресного пространства

13.3. Пример настройки опций 60 и 43 DHCPv6



Fit AP получает IP-адрес и опцию 43 – признак DHCP-сервера для отправки одноадресного discovery-запроса на беспроводый контроллер. DHCP-сервер настраивает опцию 60 в соответствии с опцией 60 Fit AP и возвращает 43 опцию FTP AP.

Настройка DHCP-сервера

```
router(config)#ip dhcp pool a
router (dhcp-a-config)#option 60 ascii AP1000
router (dhcp-a-config)#option 43 ascii 192.168.10.5,192.168.10.6
```

13.4. 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.

14. ОБЩАЯ ИНФОРМАЦИЯ

14.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

14.2. 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.

14.3. 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

14.4. Электронная версия документа

Дата публикации 16.05.2024

https://ftp.qtech.ru/Router/QSR-2200/Manual//QSR-2200_user_manual.pdf