Руководство пользователя

Ethernet-маршрутизаторы
Серия QSR-2200

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.

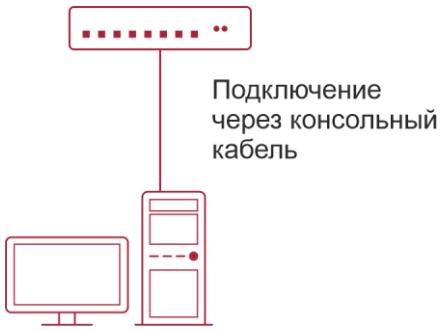

Рисунок 1-1. Подключение ПК к консольному порту маршрутизатора

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) — 115 200 бит/с.

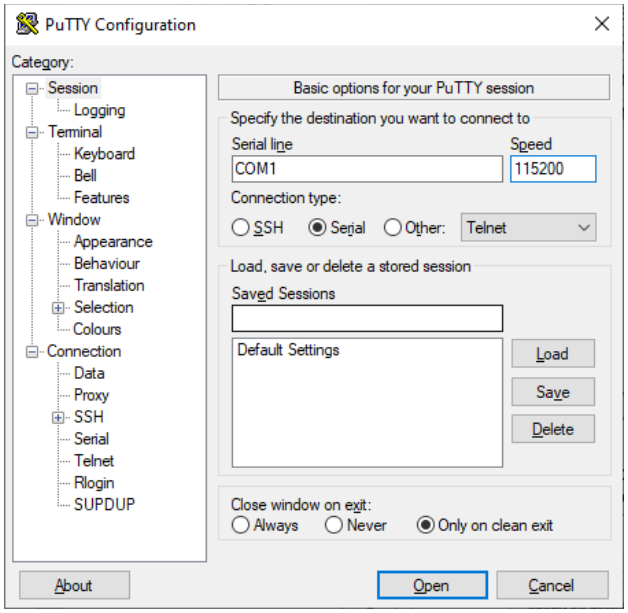

Рисунок 1-2. Основные настройки PuTTY

В настройках Connection настроить пункт Flow Control выставить в значение None:

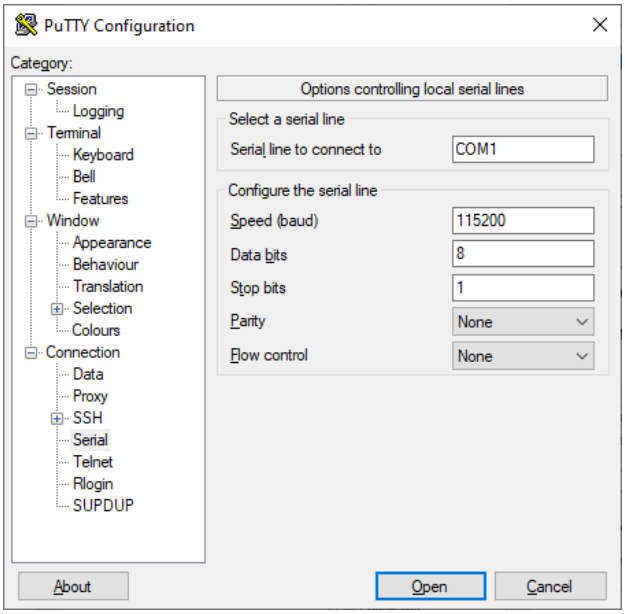

Рисунок 1-3. Настройки Connection

2. Для облегченного повторного подключения с использованием PuTTY, следует сохранить настройки сессии. Для этого необходиомо в поле «Saved Session» ввести название сессии (например, QSR-2200-10TBX-AC1) и нажать кнопку «Save».

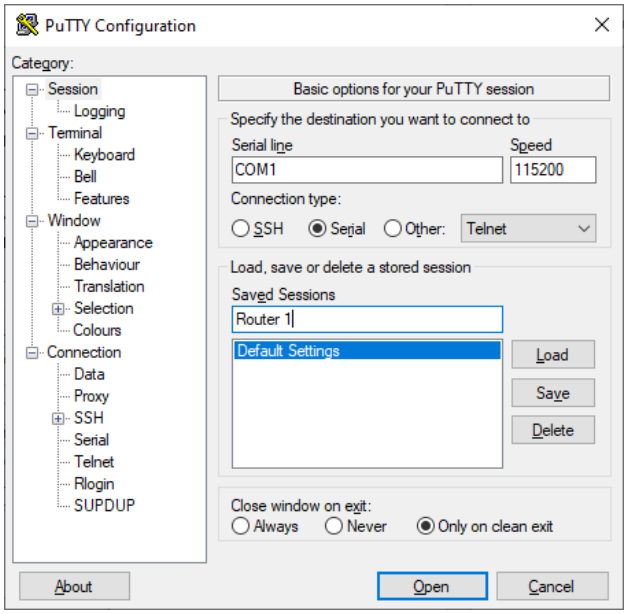

Рисунок 1-4. Сохранение сессии в PuTTY

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

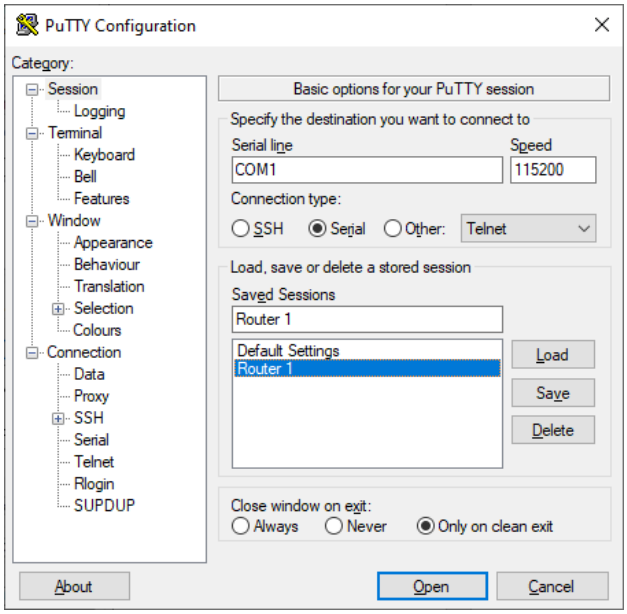

Рисунок 1-5. Запуск сохраненной сессии

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.

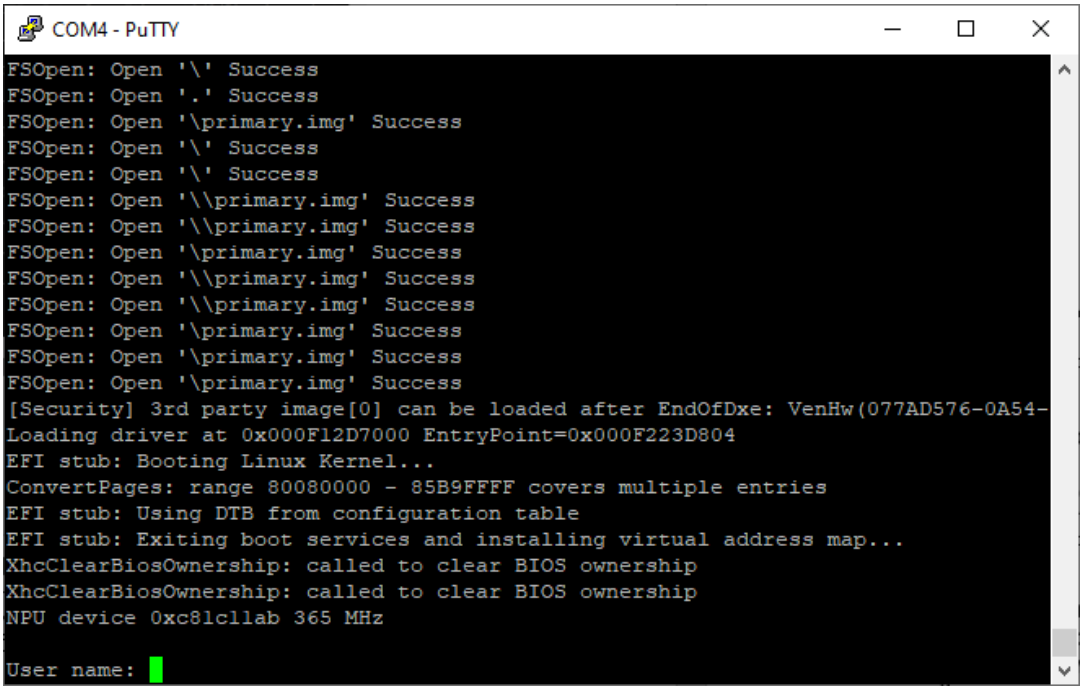

Рисунок 1-6. Маршрутизатор загрузился

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 1-7. 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 «QSR-2200-10TBX-AC», 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:

```
QSR-2200-10TBX-AC#config
QSR-2200-10TBX-AC(config)#interface vlan 1
QSR-2200-10TBX-AC(config-vlan)# no shutdown
QSR-2200-10TBX-AC(config-vlan)# ip address 192.168.0.1/24
```

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:

```
QSR-2200-10TBX-AC#config
QSR-2200-10TBX-AC(config)# service telnet
QSR-2200-10TBX-AC(config-service-telnet)# run
```

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.

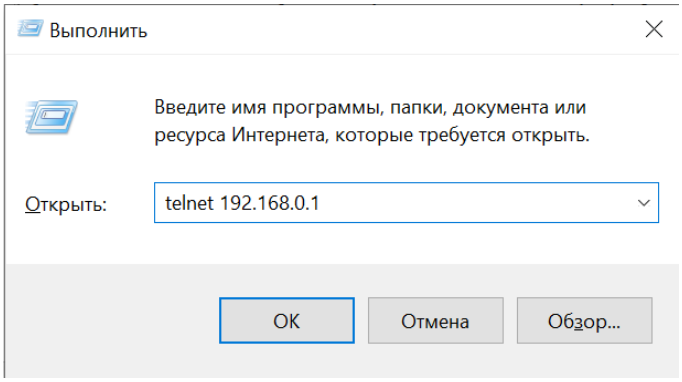

Рисунок 1-8. Запуск программы Telnet-клиент в Windows

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 следующими командами:

```
QSR-2200-10TBX-AC(config)# username qtech
QSR-2200-10TBX-AC(config-user)# privilege 15
QSR-2200-10TBX-AC(config-user)# password
QSR-2200-10TBX-AC(config-user)# password ascii-text qtech
```

По умолчанию логин (login) — admin, пароль (password) — admin.

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 1-9. 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

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 «QSR-2200-10TBX-AC#», 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 глобального конфигурирования

Наберите команду «QSR-2200-10TBX-AC# configure» 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, STP, и т. д. Также пользователь может войти в режим конфигурирования порта для настройки всех интерфейсов.

1.2.1.2.1. Режим конфигурирования интерфейса

Использование команды интерфейса в режиме глобального конфигурирования позволяет входить в режим конфигурирования указанного интерфейса. Маршрутизатор поддерживает несколько типов интерфейсов: 1. VLAN; 2. Ethernet-порт; 3. Tunnel и т.д.

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 VLAN-интерфейсов 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

1.2.1.2.2. 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.

1.2.1.2.3. Режим DHCP Address Pool

Введите команду ip dhcp pool <name> в режиме глобального конфигурирования для входа в режим DHCP Address Pool. Приглашение этого режима «QSR-2200-10TBX(config-dhcp)#». В этом режиме происходит конфигурирование DHCP Address Pool. Выполните

команду выхода, чтобы выйти из режима конфигурирования DHCP Address Pool в режим глобального конфигурирования.

1.2.1.2.4. ACL-режим

Тип ACL	Команда	Действие команды	Выход
Расширенный режим IP ACL	Наберите команду ip access-list <name> 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.

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

server community public ro

server community private rw

1.2.3. Сочетания клавиш

Маршрутизатор поддерживает множество сочетаний клавиш для облегчения ввода конфигурации пользователем.

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 +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 «Tab» и «?».

Доступ к справке	Использование и функции
«Tab»	Для получения списка всех доступных команд в данном режиме
«?»	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 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: QSR-2200-10TBX-AC # show mac mac-address-table - MAC table info

Доступ к справке	Использование и функции
«Tab»	Нажмите Tab после ввода команды для получения списка доступных параметров

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
unknown command	Введенной команды не существует или есть ошибка в параметре масштаба, типа или формата

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 switchport status»**, будет работать даже в том случае, если набрать **«sh int switchport status»**.
2. Однако, при наборе команды **«show running-config»** как **«show r»** система сообщит «unknown 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	
commit	Применение введенных ранее команд конфигурации на время confirm-timeout
confirm	Подтверждение примененных при помощи команды commit команд
Режим администратора	
configure	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

Команда	Пояснение
copy default-config startup-config	Возвращает заводские настройки
copy running-config startup-config	Сохраняет текущую конфигурацию на Flash-память
reload	Перезагрузка маршрутизатора
system config [on-demand | by-commit]	Применение конфигурации: - после ввода команды - в режиме commit/confirm

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

2.2.1.2.1. Настройка Telnet-сервера

Команда	Описание
Режим глобального конфигурирования	
service telnet run no run	Активирует функцию Telnet-сервера на маршрутизаторе, команда «no» деактивирует эту функцию
username <username> privilege [<1-15>] password [ascii-text | encrypted] <password> no username <username>	Настраивает имя пользователя и пароль для доступа по Telnet. Команда «no» удаляет данные авторизации выбранного пользователя
aaa authentication login <name> login {local | radius | tacacs} no authentication <name>	Настройка режима аутентификации для подключения к маршрутизатору. Команда «no» удаляет команду
aaa authentication active-login-list <name> no authentication active-login-list	Настройка включения списков методов аутентификации. Команда «no» отменяет применение методов аутентификации

2.2.1.2.2. Использование Telnet для удаленного доступа к маршрутизатору

Команда	Описание
Режим администратора	
telnet [vrf <vrf-name>] {<ip-addr> | host <hostname>} [<port>]	Подключения с маршрутизатора к другим устройствам по протоколу telnet

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	
service ssh generate ssh-host-key {rsa [<1024-8192> bit size] | ecdsa [<any number> bit size of 256, 384 or 521] | ed25519} run no run	Активация функции на маршрутизаторе; команда «no» отменяет предыдущую команду
username <username> privilege [<1-15>] password [ascii-text | encrypted] <password> no username <username>	Настраивает имя пользователя и пароль для доступа к маршрутизатору через SSH-клиент. Команда «no» удаляет данные авторизации выбранного пользователя

2.2.2.2.1. Пример настройки SSH-сервера

Пример:

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.

```
QSR-2200-10TBX-AC # configure
QSR-2200-10TBX-AC (config)# service ssh
QSR-2200-10TBX-AC (config-service-ssh)# run
QSR-2200-10TBX-AC (config-service-ssh)# exit
QSR-2200-10TBX-AC (config)# interface vlan 1
QSR-2200-10TBX-AC (config-vlan)# ip address 10.10.254.29/24
QSR-2200-10TBX-AC (config-vlan)# exit
QSR-2900-30TX(config)# username qtech
QSR-2900-30TX(config-user)# privilege 15
```

```
QSR-2900-30TX(config-user)# password ascii-text qtech
```

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 LAN Ethernet-порты маршрутизатора по умолчанию являются портами доступа для канального уровня и работают на втором уровне, но могут быть сконфигурированы в L3 интерфейсы. Все WAN Ethernet-порты по умолчанию являются L3 интерфейсами, но могут быть сконфигурированы как L2 интерфейсы. L3 интерфейсы, а так же VLAN-интерфейсы представляет собой интерфейс третьего уровня с функциями, для которых может быть назначен IP-адрес, который будет IP-адресом маршрутизатора. Все сети VLAN, связанные с интерфейсом, и их конфигурация могут быть настроены в подрежиме конфигурирования VLAN. Маршрутизатор предоставляет два метода конфигурации IP-адреса:

- Статический
- DHCP

Статическа 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

2.3.1.1. 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

2.3.1.2. Ручная настройка

Команда	Описание
ip address <ip_address>/<mask> [secondary] no ip address {<ip_address>/<mask> | dhcp | all} [secondary]	Настройка IP-адреса VLAN-интерфейса; команда «no» удаляет IP-адрес VLAN-интерфейса

Команда	Описание
ipv6 address <ipv6-address/prefix-length> [eui-64] no ipv6 address <ipv6-address/prefix-length>	Настройка IPv6-адресов. Команда «no» удаляет IPv6-адреса

2.3.1.3. DHCP конфигурация

Команда	Описание
ip address dhcp no ip address dhcp	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.

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:

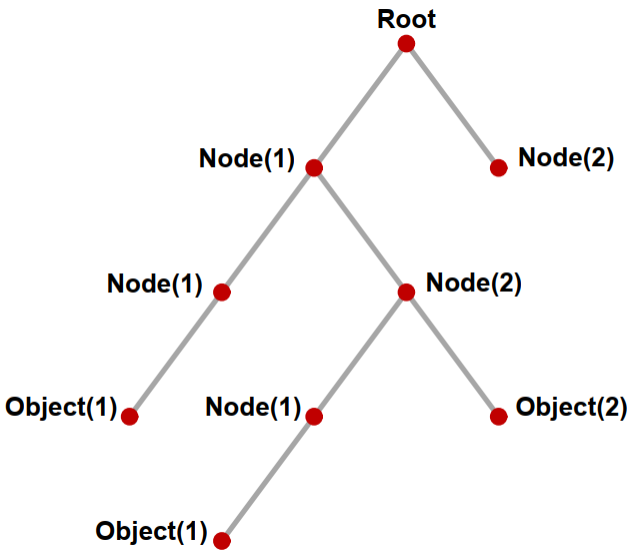

Рисунок 2-1. Пример дерева ASN.1

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

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

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

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.

2.4.3. Настройка SNMP

2.4.3.1. Список команд для настройки SNMP

2.4.3.1.1. Включение и отключение функции SNMP-агента

Команда	Описание
Режим глобального конфигурирования	
service snmp	Переход в режи конфигурации SNMP
Режим конфигурирования SNMP	
run no run	Включение функции SNMP-агента на маршрутизаторе. Команда «no» выключает эту функцию

2.4.3.1.2. Настройка строки сообщества в SNMP

Команда	Описание
Режим конфигурирования SNMP	
server community <string> {ro|rw} [view view-name>] no server community	Настройка строки сообщества в SNMP для маршрутизатора. Команда «no» удаляет эту строку

2.4.3.1.3. Настройка безопасного IP-адреса станции управления SNMP

2.4.3.1.3.1. Настройка TRAP

Команда	Описание
Режим глобального конфигурирования	
service snmp server enable traps [config | dying-gasp | transceiver-monitor] no server enable traps [config | dying-gasp | transceiver-monitor]	Включить отправку Trap-сообщений. Эта команда используется для SNMP v1/v2/v3. Команда «no» удаляет конфигурацию
server host [oob | vrf <name>] <ip address> no server host [oob | vrf <name>] <ip address> community <name> no community	Установка IPv4/IPv6-адреса хоста, который используется для получения информации SNMP Trap. Для SNMP v1/v2, эта команда также настраивает строку сообщества для Trap. 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:

```
QSR-2200-10TBX-AC(config)#  service snmp
QSR-2200-10TBX-AC(config-service-snmp)# server host 1.1.1.5
QSR-2200-10TBX-AC(config-snmp-host)# community public
QSR-2200-10TBX-AC(config-snmp-host)# exit
QSR-2200-10TBX-AC(config-service-snmp)# server enable traps
QSR-2200-10TBX-AC(config-service-snmp)# server community public rw
QSR-2200-10TBX-AC(config-service-snmp)# server enable traps dying-gasp
QSR-2200-10TBX-AC(config-service-snmp)# run
```

NMS может использовать private строку сообщества(rw) для доступа к маршрутизатору для чтения и записи или использовать public строку сообщества(ro) для доступа к маршрутизатору только для чтения.

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 "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 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.

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.

2.5.2.2.1. Настройка FTP/TFTP-клиента

2.5.2.2.1.1. Загрузка файлов FTP/TFTP-клиентом

Команда	Пояснение
Режим администратора	
copy ftp://user[:password]@<host>[:port][active_mode_flag]/<remote-filename>.bzimage flash:image/ tftp://<host>[:port]:/<remote-filename>.bzimage flash:image/	Загрузка файлов FTP/TFTP-клиентом

2.5.2.3. Примеры настройки FTP/TFTP

Пример показан только для IPv4-адреса.

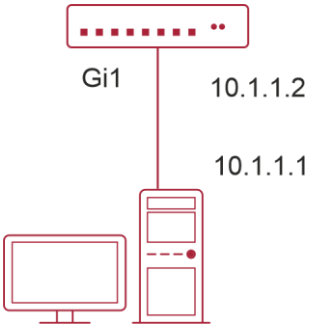

Рисунок 2-2. Загрузка nos.img файла FTP/TFTP-клиентом

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 "QSR-2200-10TBX-AC_ 1.0.755.bzimage" 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 "QSR-2200-10TBX-AC _1.0.755.bzimage" в соответствующий каталог FTP-сервера на компьютере.

Далее описана процедура настройки маршрутизатора:

```
QSR-2200-10TBX-AC(config)#interface vlan 1
QSR-2200-10TBX-AC(Config-if-Vlan1)#ip address 10.1.1.2/24
```

```
QSR-2200-10TBX-AC(Config-if-Vlan1)#exit
QSR-2200-10TBX-AC(config)#exit
QSR-2200-10TBX-AC#copy tftp://10.1.1.1:/QSR-2200-10TBX-AC_1.0.755.bzimage flash:image/
```

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 флеш-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	
system boot <filename>.bzimage primary-image	Выставление парметров загрузки IMG-файла в качестве основного ПО, которое будет загружаться в первую очередь
system boot <filename>.bzimage backup-image	Выставление параметров загрузки IMG-файла, который будет выступать в роли резервного ПО и загружаться если загрузка основного ПО не удалась

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 пинг-тестирование неудачно, следует устранить неполадки с соединением.

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.

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 транспортировки на флеш-память маршрутизатора. Также необходимо свободное место на флеш-накопителе USB для выгрузки файлов из флеш-памяти маршрутизатора. Флеш-накопитель должен быть установлен в USB-разъем.

Установите флеш-накопитель USB в USB-разъем. Система автоматически выполнит поиск USB.

Команды для работы с флеш-накопителем USB.

2.5.3.1.1. Команды просмотра и перехода по разделам

Команда	Пояснение
dir usb://<раздел> dir usb://sda1/	Просмотр содержимого USB флеш-накопителя
umount usb://sda1/	Отключение USB-накопителя

2.5.3.1.2. Команды транспортировки файлов с использованием флеш-накопителя

Команда	Пояснение
Режим администратора	
copy usb://sda1/<file name> flash:image/	Копирование ПО (IMG-файла) с USB флеш-накопителя на флеш-память маршрутизатора
delete usb://sda1/<file name>	Удаление файла с флеш-накопителя USB

После копирования IMG-файлов в флеш-память маршрутизатора необходимо выставить параметры загрузки файлов (см. п. 2.5.2.4).

3. КОНФИГУРИРОВАНИЕ ПОРТОВ

3.1. Введение

Если пользователь хочет сконфигурировать сетевой порт, он может ввести команду «interface <interface-type> <interface-list>» для входа в соответствующий режим конфигурации порта. 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

3.2.1. Вход в режим конфигурации Ethernet-порта

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

3.2.1.1. Конфигурация параметров сетевого порта

Команда	Описание
Режим конфигурации порта	
sfp mode {copper | fiber}	Установка режима SFP+-портов
shutdown no shutdown	Включение/выключение указанного порта
description <string> no description	Назначение или отмена имени порта
speed {auto | 10 | 100 | 1G | 2.5G | 5G | 10G {full | half} no speed	Установка скорости и дуплекса на порту. С оператором «no» данная команда восстанавливает параметры порта по умолчанию, то есть автоматическое определение скорости и дуплекса
loopback-detection enable no loopback-detection enable	Включение/выключение функции петли для указанных портов
loopback-detection specified-vlans <VLAN ID> no loopback-detection specified-vlans	Выбор VLAN для работы loopback-detection. Команда no для отключения

Команда	Описание
loopback-detection trap no loopback-detection trap	Включение отправки SNMP Trap для событий обнаружения петель. Команда no для отключения
storm-control {unicast-unknown | broadcast | multicast-unregistered} {kbps <Kbits> | pps <packet>} no storm-control {unicast-unknown | broadcast | multicast-unregistered}	Включение функции контроля штормов для широковещательных, многопользовательских и персональных пакетов с неизвестным адресом назначения (коротких для широковещательного) и установка допустимого числа широковещательных пакетов; формат NO данной команды отключает функцию контроля широковещательных штормов

3.2.1.2. Виртуальный тест кабеля

Команда	Описание
Режим администратора	
virtual-cable-test <interface-type> <interface-list>	Виртуальный тест кабеля на порте

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 Ethernet-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

4.2.1. Конфигурирование временного интервала распознавания петли

Команда	Описание
Режим глобального конфигурирования	
loopback-detection interval <1-300> {<1-300>} no interval	Конфигурирование временного интервала распознавания петли

4.2.2. Включение функции распознавания петли

Команда	Описание
Режим конфигурирования порта	
loopback-detection enable no loopback-detection enable	Включение и выключение функции распознавания петли
loopback-detection specified-vlans <VLAN ID> no loopback-detection specified-vlans	Выбор VLAN для работы loopback-detection. Команда no для отключения
loopback-detection trap no loopback-detection trap	Включение отправки SNMP Trap для событий обнаружения петель. Команда no для отключения

4.2.3. Вывод отладочной информации по распознаванию петли

Команда	Описание
Режим администратора	
show loopback-detection	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

4.2.4. Конфигурирование режима восстановления при распознавании петли

Команда	Описание
Режим глобального конфигурирования	
loopback-detection recovery recovery <1-300> s no recovery	Конфигурирование режима восстановления при распознавании петли (автоматическое восстановление или нет) или времени восстановления

4.3. Примеры функции распознавания петли на порту

Рисунок 4-1. 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:

```
QSR-2200-10TBX-AC(config)# loopback-detection
QSR-2200-10TBX-AC(config-lbd)# interval 35 15
QSR-2200-10TBX-AC(config-lbd)# recovery
QSR-2200-10TBX-AC(config-lbd)# recovery 60
QSR-2200-10TBX-AC(config-lbd)# exit
QSR-2200-10TBX-AC(config)# interface gigabitethernet0/1/1
QSR-2200-10TBX-AC(config-if-gi)# loopback-detection
QSR-2200-10TBX-AC(config-if-gi)# loopback-detection enable
QSR-2200-10TBX-AC(config-if-gi)# loopback-detection specified-vlans 1-3
```

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 Ethernet-устройствам, таким, как маршрутизаторы, маршрутизаторы и точки доступа уведомлять о своем существовании другие узлы сети и сохранять информацию обо всех соседних устройствах. Как следсвие, детальная информация о конфигурации устройства и о найденных соседях может объявляться посредством данного протокола.

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

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

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

Информация, собранная на 2 уровне, содержит сведения об устройствах, их портах и о том какие 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

5.2.1. Включение LLDP на устройстве

Команда	Описание
Режим глобального конфигурирования	
service lldp run no run	Общее включение/выключение

5.2.2. Включение функции LLDP на порту

Команда	Описание
Режим конфигурирования порта	
lldp receive lldp transmit no lldp receive no lldp transmit	Включение/выключение получения и отправки пакетов LLDP на порту

5.2.3. Конфигурация интервала обновления сообщений LLDP

Команда	Описание
Режим глобального конфигурирования	
service lldp timer interval <1-65535> s no timer	Конфигурация интервала отправки сообщений LLDP

5.2.4. Отображение отладочной информации по функции LLDP

Команда	Описание
Режим администратора	
show lldp settings	Отображение текущей конфигурации функции LLDP

Команда	Описание
show lldp interface info	Отображение информации о конфигурации LLDP на конкретном порту
show lldp statistics	Отображение информации обо всех счетчиках
show lldp neighbors	Отображение информации о LLDP соседях на данном порту

5.3. Типовой пример функции LLDP

Рисунок 5-1. Типовой пример конфигурации функции LLDP

На схеме сетевой топологии, приведенной выше, порт 0/1/1 на маршрутизаторе B подключен к порту 0/1/1 маршрутизатора A. Порт маршрутизатора B сконфигурирован в режиме приема пакетов. Опция TLV на порту маршрутизатора A сконфигурирована как portDes и SysCap.

Маршрутизатор A. Последовательность команд конфигурации:

```
QSR-2200-10TBX-AC_A (config)# service lldp
QSR-2200-10TBX-AC_A (config-service-lldp)# run
QSR-2200-10TBX-AC_A (config-service-lldp)# exit
QSR-2200-10TBX-AC_A (config)# interface gigabitethernet0/1/1
QSR-2200-10TBX-AC_A (config-if-gi)# lldp transmit
QSR-2200-10TBX-AC_A (config-if-gi)# lldp port description TEST
QSR-2200-10TBX-AC_A (config-if-gi)# exit
```

Маршрутизатор B. Последовательность команд конфигурации:

```
QSR-2200-10TBX-AC_B (config)# service lldp
QSR-2200-10TBX-AC_B (config-service-lldp)# run
QSR-2200-10TBX-AC_B (config-service-lldp)# exit
QSR-2200-10TBX-AC_B (config)# interface gigabitethernet0/1/1
QSR-2200-10TBX-AC_B (config-if-gi)# lldp receive
```

5.4. Устранение неисправностей функции LLDP

Функция LLDP по умолчанию выключена. 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

Команда	Описание
Режим конфигурирования интерфейса	
mtu <68-10278> байт	Настройка максимального размера пакета на интерфейсе

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

7.2.1. Просмотр информации контроля в реальном масштабе времени

Команда	Описание
Режим конфигурирования порта, режим администратора или режим глобального конфигурирования	
show transceiver detail	Просмотр мониторинга состояния трансивера

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

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

7.2.3. Настройка состояния мониторинга трансивера

7.2.3.1. Настройка интервала мониторинга трансивера

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

7.2.3.2. Настройка состояния включения мониторинга трансивера

Команда	Описание
Режим конфигурирования порта	
transceiver-monitoring disable no transceiver-monitoring 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:

В интерфейс tengigabitethernet0/1/10 включен оптический модуль с DDM, в интерфейс tengigabitethernet0/1/9 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:

```
QSR-2200-10TBX-AC# show transceiver detail
```

Interface	Temp (°C)	Voltage (V)	Bias (mA)	RX Power (dBM)	TX Power (dBM)
0/1/10	43,82	3,29	23,34	−3,75	−0,79

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 установлен в порт, иначе конфигурация DDM не будет показана.
- Убедитесь, что конфигурация SNMP работает, иначе оповещение о событии не сможет оповестить систему сетевого управления.
- Использование команды show transceiver detail может занять много времени, так как маршрутизатор будет проверять все порты.

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

8.2.1. Базовая конфигурация

Команда	Описание
Режим конфигурирования	
service lldp med network policy profile <profile id> type <raffic type name> vlan <id> cos <0-7> dscp <0-63>	Настройка профиля сетевой политики, включающая VLAN ID, поддерживаемые приложения (такие как голос и видео), приоритет приложений и политика использования, и так далее
Режим конфигурирования порта	
lldp med enable lldp med network policy profile <profile id>	Настройка профиля сетевой политики на интерфейсе. Команда no для отмены конфигурации
Режим администратора	
show lldp med network policy profiles	Показывает настройки LLDP-MED профилей

8.3. Пример настройки LLDP-MED

Рисунок 8-1. Топология базовой конфигурации LLDP-MED

1. Настройка QSR-2200-10TBX-AC:

```
QSR-2200-10TBX-AC(config)# vlan 10,20
QSR-2200-10TBX-AC(config)# service lldp
QSR-2200-10TBX-AC(config-service-lldp)# run
QSR-2200-10TBX-AC(config-service-lldp)# med
QSR-2200-10TBX-AC(config-service-lldp-med)# network policy profile 1
QSR-2200-10TBX-AC(config-service-lldp-med-network-policy-profile)# type voice
QSR-2200-10TBX-AC(config-service-lldp-med-network-policy-profile-type)# vlan 10
QSR-2200-10TBX-AC(config-service-lldp-med-network-policy-profile-type)# cos 5
QSR-2200-10TBX-AC(config-service-lldp-med-network-policy-profile-type)# dscp 46
QSR-2200-10TBX-AC(config-service-lldp-med-network-policy-profile-type)# exit
QSR-2200-10TBX-AC(config-service-lldp-med-network-policy-profile)# exit
QSR-2200-10TBX-AC(config-service-lldp-med)# exit
QSR-2200-10TBX-AC(config-service-lldp)# exit
QSR-2200-10TBX-AC(config)# interface gigabitethernet0/1/1
QSR-2200-10TBX-AC(config-if-gi)# lldp receive
QSR-2200-10TBX-AC(config-if-gi)# lldp transmit
QSR-2200-10TBX-AC(config-if-gi)# lldp med network policy profile 1
QSR-2200-10TBX-AC(config-if-gi)# no shutdown
QSR-2200-10TBX-AC(config-if-gi)# switchport mode hybrid
QSR-2200-10TBX-AC(config-if-gi)# switchport hybrid allowed tagged vlan 10
QSR-2200-10TBX-AC(config-if-gi)# switchport hybrid native vlan 20
```

Просмотр глобального статуса и статуса интерфейса на QSR-2200-10TBX-ACA

```
QSR-2200-10TBX-AC# show lldp med network policy profiles
LLDP MED network policy profiles:
Profile 1:
    Traffic type: voice
        DSCP: 46
```

Tagged: true

Vlan: 10

COS: 5

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.
- 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.

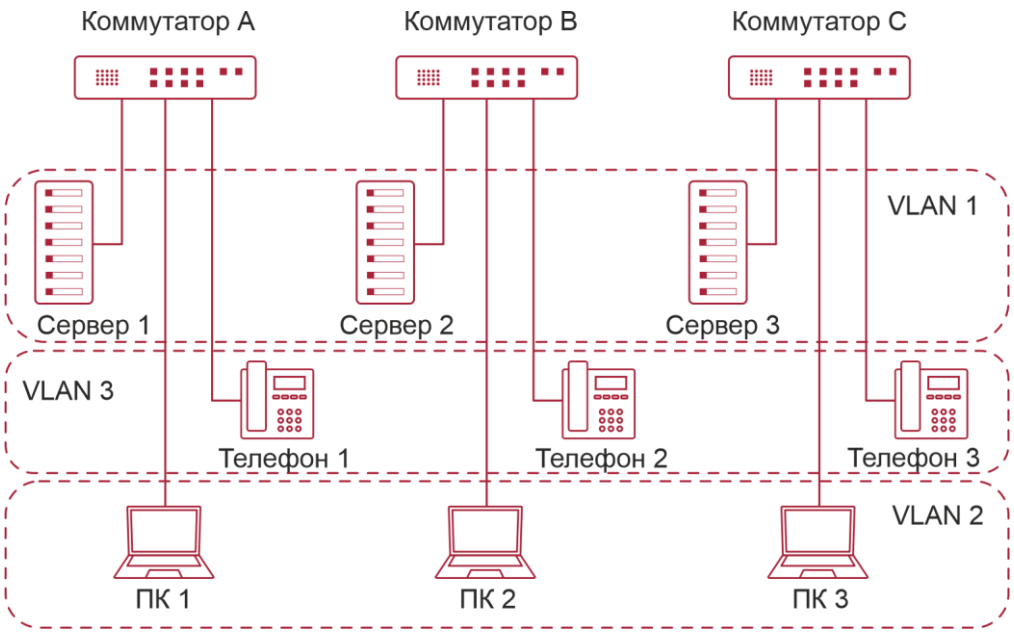

Рисунок 9-1. Логическое определение сети VLAN

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

Благодаря вышеперечисленным особенностям, технология VLAN обеспечивает следующие преимущества:

- улучшается производительность сети;
- экономятся сетевые ресурсы;

- упрощается управление сетью;
- снижается стоимость сети;
- улучшается безопасность сети.

Ethernet-порты 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

9.1.2.1. Создание или удаление VLAN

Команда	Описание
Режим глобального конфигурирования	
vlan <1-4094> no vlan <1-4094>	Создание/удаление VLAN-а

9.1.2.2. Настройка имени VLAN

Команда	Описание
Режим глобального конфигурирования	
interface vlan <1-4094> name <VLAN_name> no name	Изменение имени VLAN. no для возврата к имени по умолчанию

9.1.2.3. Установка типа порта маршрутизатора

Команда	Описание
Режим конфигурирования порта	
switchport mode {trunk | access | hybrid}	Настройка режима порта

9.1.2.4. Настройка транкового порта

Команда	Описание
Режим конфигурирования порта	
switchport trunk allowed vlan {<vlan-id> | all | add <vlan-id> | remove <vlan-id>} 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

9.1.2.5. 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

9.1.2.6. Настройка гибридного порта

Команда	Описание
Режим конфигурирования порта	
switchport hybrid allowed tagged vlan {<vlan-id> | all | add <vlan-id> | remove <vlan-id>} switchport hybrid allowed untagged vlan {<vlan-id> | all | add <vlan-id> | remove <vlan-id>} no switchport hybrid allowed tagged no switchport hybrid allowed untagged	Установка/удаление VLAN'а, приписанного к гибридному порту с режимом метки или без нее

Команда	Описание
switchport hybrid native vlan <vlan-id> no Switchport hybrid native vlan	Установка/удаление PVID на порту

10. КОНФИГУРИРОВАНИЕ ФУНКЦИЙ 3-ГО УРОВНЯ

10.1. Интерфейс 3-го уровня

10.1.1. Начальные сведения об интерфейсах 3-го уровня

В маршрутизаторах могут быть физические и виртуальные интерфейсы 3-го уровня. Интерфейс 3 уровня, основанный на VLAN называется SVI. SVI 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.

10.1.2.1. Создание интерфейса 3-го уровня

Команда	Описание
Режим глобального конфигурирования	
interface vlan <vlan-id> no interface vlan <vlan-id>	Создание VLAN-интерфейса (SVI); команда «no» удаляет VLAN-интерфейс, созданный на маршрутизаторе
interface <interface-type> <interface-list> no switchport	Изменение режима работы физического порта на 3 уровень

10.1.2.2. Настройка описания интерфейса

Команда	Описание
Режим конфигурирования L3 интерфейса	
description <text> no description	Настройка описания интерфейса. Команда «no» уберет описание 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 Интернета. Однако по мере роста инфраструктуры Интернета и услуг, использующих интернет-приложения, выявляются и некоторые недостатки протокола IPv4, связанные с масштабом и сложностью сегодняшнего Интернета.

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

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

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

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

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

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

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

счет механизма обнаружения маршрута MTU (Path MTU Discovery Mechanism) работающего с источником пакетных данных.

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

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

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

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

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

10.2.2. Настройка IP-протокола

Интерфейс 3-го уровня может быть настроен как IPv4-интерфейс и(или) как IPv6-интерфейс.

10.2.2.1. Настройка адреса IPv4

10.2.2.1.1. 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 интерфейса; команда no отменяет настройки

10.2.2.1.2. Настройка шлюза по умолчанию

Команда	Описание
Режим глобального конфигурирования	
ip route 0.0.0.0/0 <A.B.C.D> no ip route 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.

10.2.2.2.1. Базовая настройка IPv6

10.2.2.2.1.1. Настройка адреса IPv6-интерфейса

Команда	Описание
Режим конфигурирования интерфейса	
ipv6 enable ipv6 address {X:X::X:X/M | dhcp} no ipv6 address {X:X::X:X/M | dhcp | all}	Настройка IPv6-адреса. Команда no отменяет настройки

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).

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 11-1. 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. Настройка сервера DHCP

11.2.1. Включить/выключить сервис DHCP

Команда	Описание
Режим глобального конфигурирования	
service dhcps no service dhcps	Включить/выключить сервис DHCP

11.2.2. Настроить адресный пул DHCP

11.2.2.1. 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

11.2.2.2. Настроить параметры адресного пула DHCP

Команда	Описание
Режим адресного пула DHCP	
network A.B.C.D/M no network-address	Настройка области адресов, которые могут быть выделены адресному пулу. Команда «no» отменяет выделение адресного пула
default-router <address> no default-router	Настройка шлюза по умолчанию для DHCP-клиентов. Команда «no» отменяет шлюз по умолчанию
dns-server <addres> no dns-server <addres>	Настройка DNS-сервера для DHCP-клиентов. Команда «no» отменяет настройку DNS-сервера

Команда	Описание
domain-name <domain> no domain-name <domain>	Настройка доменного имени для DHCP-клиентов. Команда «no» отменяет доменное имя
option <code> {ascii <string> | hex <hex> | address <ipaddress>} no option <code> {ascii <string> | hex <hex> | address <ipaddress>}	Настройка сетевого параметра, определенного кодом опции. Команда «no» удаляет сетевой параметр
lease {days [hours][minutes]} no lease	Настройка времени аренды адресов пула. Команда «no» удаляет настройку времени аренды
exclude-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
Режим конфигурирования интерфейса	
ip dhcp-server	Включение DHCP-сервера на L3-интерфейсе

11.2.2.3. Настроить параметры статического адресного пула DHCP

Команда	Описание
Режим адресного пула DHCP	
host <address> mac <address> no host <address> mac <address>	Задать/удалить IP-адрес, который будет назначен заданному клиенту

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. Настройки сети для расположений A показаны ниже.

Пул A (сеть 10.16.1.0)	
Устройство	IP address
Шлюз по умолчанию	10.16.1.200

Пул A (сеть 10.16.1.0)	
DNS-сервер	10.16.1.202
WINS-сервер	10.16.1.209
Тип узла WINS	H-узел
Время аренды	3 дня

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».

```
QSR-2200-10TBX-AC(config)# service dhcps
QSR-2200-10TBX-AC(config)# interface vlan 1
QSR-2200-10TBX-AC(config-vlan)# ip address 10.16.1.2/24
QSR-2200-10TBX-AC(config-vlan)# ip dhcp-server
QSR-2200-10TBX-AC(config-vlan)# exit
QSR-2200-10TBX-AC(config)# ip dhcp pool A
QSR-2200-10TBX-AC(config-dhcp)# network 10.16.1.0/24
QSR-2200-10TBX-AC(config-dhcp)# lease 3
QSR-2200-10TBX-AC(config-dhcp)# default-router 10.16.1.200
QSR-2200-10TBX-AC(config-dhcp)# dns-server 10.16.1.202
QSR-2200-10TBX-AC(config-dhcp)# option  44 address 10.16.1.209
QSR-2200-10TBX-AC(config-dhcp)# option 46 ascii H-node
QSR-2200-10TBX-AC(config-dhcp)# exclude-address 10.16.1.200 10.16.1.201
QSR-2200-10TBX-AC(config-dhcp)# host 10.16.1.210 mac 08-c6-b3-23-dc-ab
QSR-2200-10TBX-AC(dhcp-A1-config)#exit
```

Руководство по использованию: когда DHCP/BOOTP-клиент подключается к порту маршрутизатора, клиент может получить адрес из сети 10.16.1.0/24. 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.

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.

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.

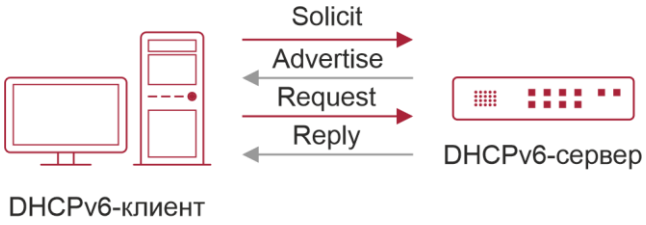

Рисунок 12-1. Согласование DHCPv6

Когда DHCPv6-клиент пытается запросить у DHCPv6-сервера IPv6-адрес и другие параметры, клиент должен сначала найти DHCPv6-сервер, затем уже запросить конфигурация у сервера.

Для обнаружения сервера DHCP-клиент рассылает пакеты SOLICIT (запрос) на широковещательный адрес FF02::1:2.

Каждый DHCP-сервер, получивший запрос, ответит клиенту сообщением ADVERTISE (предложение), которое содержит идентификатор сервера (DIUD) и его приоритет.

Возможно, что клиент получит несколько сообщений ADVERTISE. Клиент должен выбрать один сервер и ответить ему сообщением REQUEST (заявка), чтобы запросить адрес, предложенный в сообщении ADVERTISE.

Затем выбранный DHCPv6-сервер сообщением REPLY (ответ) подтверждает назначение клиенту IPv6-адреса и других настроек.

Данные четыре шага завершают процесс динамической настройки хоста. Тем не менее, если DHCPv6-сервер и DHCPv6-клиент не находятся в одной сети, сервер не получит широковещательный запрос от клиента и не ответит ему. В этом случае необходим DHCPv6-ретранслятор (relay), чтобы пересылать запросы между клиентом и сервером. В 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

12.2.1. Включить/выключить сервис DHCPv6

Команда	Описание
Режим глобального конфигурирования	
service dhcps no service dhcps	Включение/выключение сервиса DHCP
ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>	Создать/удалить адресный пул DHCPv6

12.2.2. Настроить параметры адресного пула DHCPv6

Команда	Описание
Режим конфигурации адресного пула DHCPv6	
address prefix <ipv6-pool-start-address>/<prefix-length> [lifetime <seconds> | infinite] no address prefix <ipv6-pool-start-address>/<prefix-length> [lifetime <seconds> | infinite]	Настроить диапазон IPv6-адресов, назначаемый пулом
dns-server <ipv6-address> no dns-server <ipv6-address>	Настроить адрес DNS-сервера для DHCPv6-клиента

Команда	Описание
domain-name <domain-name> no domain-name <domain-name>	Настроить доменное имя DHCPv6-клиента

12.2.3. Включить функцию DHCPv6-сервера на порту

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

12.2.4. Просмотр информации о клиентах

show ipv6 dhcp binding	Посмотреть список DHCPv6-клиентов

12.3. Примеры конфигурации DHCPv6

Пример:

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 коммутатор для подключения пользователей. На маршрутизаторе настроен DHCPv6-сервер и соединен с магистральной сетью. На компьютерах DHCPv6-клиент.

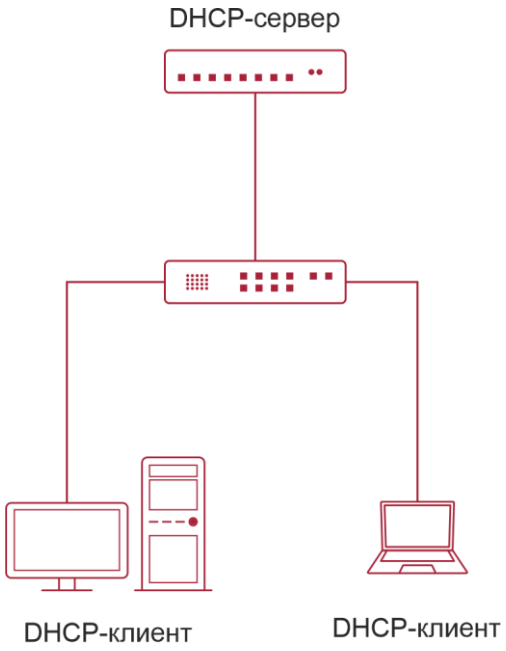

Рисунок 12-2. Схема DHCPv6

Конфигурация QSR-2200-10TBX-ACC:

```
QSR-2200-10TBX-AC# configure
QSR-2200-10TBX-AC(config)# service dhcps
QSR-2200-10TBX-AC(config)# ipv6 dhcp pool B
QSR-2200-10TBX-AC(config-dhcp6)# address prefix 2001:da8:100:1::1/64
QSR-2200-10TBX-AC(config-dhcp6)# dns-server 2001:da8::20
QSR-2200-10TBX-AC(config-dhcp6)# dns-server 2001:da8::21
QSR-2200-10TBX-AC(config-dhcp6)# domain-name QTECH
 QSR-2200-10TBX-AC(config-dhcp6)# exit
QSR-2200-10TBX-AC(config)# interface vlan 1
QSR-2200-10TBX-AC(config-vlan)# ipv6 enable
QSR-2200-10TBX-AC(config-vlan)# ipv6 address 2001:da8:1:1::1/64
QSR-2200-10TBX-AC(config-vlan)# ipv6 dhcp server B
```

12.4. Поиск неисправностей 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. ОБЩАЯ ИНФОРМАЦИЯ

13.1. Гарантия и сервис

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

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

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

13.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться разделом технической поддержки пользователей QTECH на нашем сайте www.qtech.ru/support/.

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

Центральный офис +7 (495) 477-81-18

13.3. Электронная версия документа

Дата публикации 29.04.2025

https://files.qtech.ru/upload/routers/QSR-2200/QSR-2200_user_manual.pdf