QTECH
МИР ДОСТУПНЕЕ

ОСНОВНАЯ КОНФИГУРАЦИЯ

Коммутатор агрегации

СЕРИЯ QSW-8400

www.qtech.ru

Оглавление

1 УПРАВЛЕНИЕ КОММУТАТОРОМ

1.1 Варианты управления

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

1.1.1 Внеполосное управление

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

Процедура управления коммутатором через консольный интерфейс, описана ниже:

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

Подключение ПК к консольному порту коммутатора

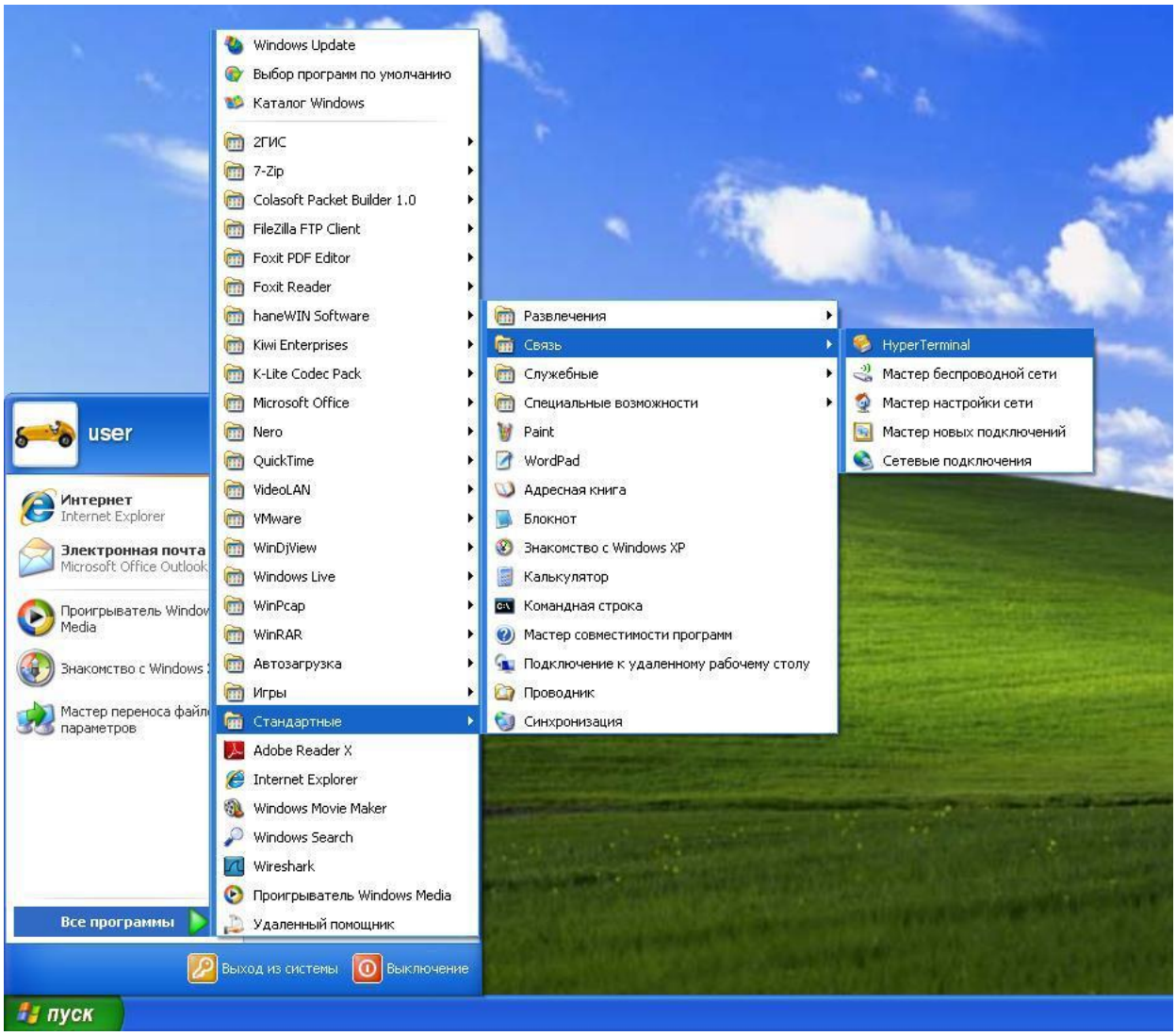
Как показано выше, серийный порт (RS-232) подключен к коммутатору через серийный кабель. В таблице ниже указаны все устройства, использующиеся в подключении.

Название устройства	Описание
Персональный компьютер (ПК)	Имеет функциональную клавиатуру и порт RS-232 с установленным эмулятором терминала, таким как HyperTerminal, входящий в ОС Windows

Кабель серийного порта	Один конец подключается к серийному порту, другой к порту консоли
Коммутатор	Требуется работающий консольный порт

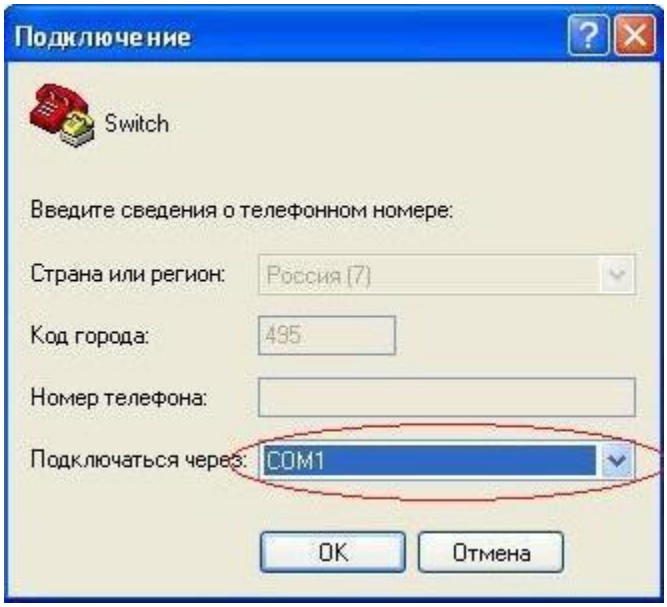
Шаг 2. Включение и настройка HyperTerminal. После установки соединения, запустите HyperTerminal, входящий в комплект Windows. Пример приведенный далее основан на HyperTerminal входящий в комплект Windows XP.

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

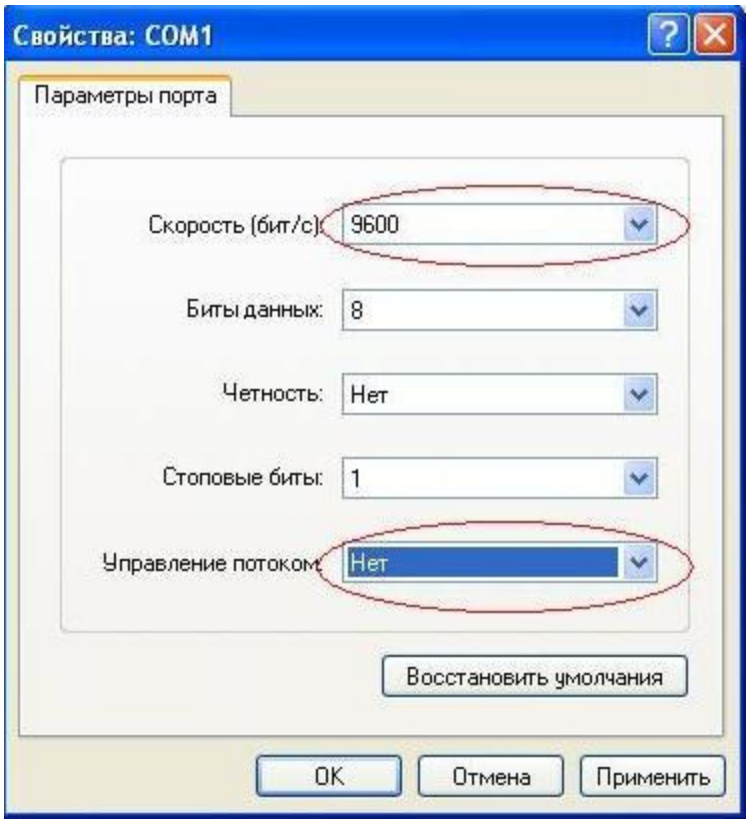


2. Наберите имя для запущенного HyperTerminal, например «Switch».

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



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



Шаг 3: Вызов командного интерфейса (CLI) коммутатора. Включите коммутатор, после чего следующие сообщения появятся в окне HyperTerminal – это режим конфигурации для коммутатора.

```
Testing RAM...
0x077C0000 RAM OK
Loading MiniBootROM...
Attaching to file system...
Loading nos.img ... done.
Booting......
Starting at 0x10000...
Attaching to file system...……
--- Performing Power-On Self Tests (POST) ---
DRAM Test.....................PASS!
PCI Device 1 Test.............PASS!
FLASH Test....................PASS!
FAN Test......................PASS!
Done All Pass.
------------------ DONE ---------------------
Current time is SUN JAN 01 00:00:00 2006
……
Switch>
```

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

1.1.2 Внутриполосное управление

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

1.1.2.1 Управление по Telnet

Чтобы управлять коммутатором по Telnet, должны выполняться следующие условия:

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

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

Управление коммутатором по Telnet

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

Первым делом идет настройка IP адреса хоста. Он должен быть в том же сегменте сети, что и IP адрес VLAN1 интерфейса коммутатора. Предположим что IP адрес интерфейса VLAN1 коммутатора 10.1.128.251/24. Тогда IP адрес хоста может быть

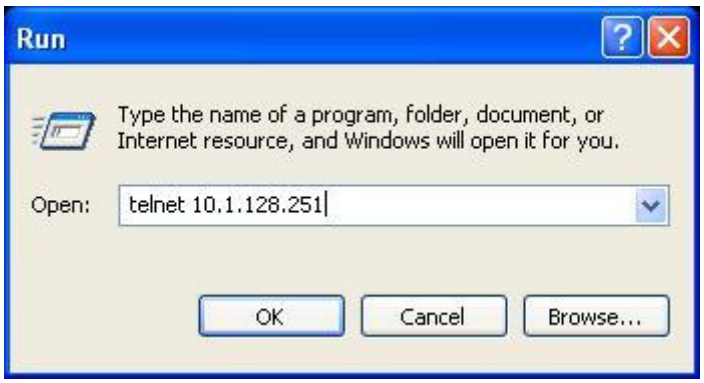
10.1.128.252/24. С помощью команды “ping 192.168.0.10” можно проверить, доступен коммутатор или нет.

Команды настройки IP адреса для интерфейса VLAN1 указаны ниже. Перед применением внутриполосного управления, IP-адрес коммутатора должен быть настроен посредством внеполосного управления (например, через порт Console). Команды конфигурирования следующие (Далее считается, что все приглашения режима конфигурирования коммутатора начинаются со слова “switch”, если отдельно не указано иного):

```
Switch>
Switch>enable
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.128.251 255.255.255.0
Switch(Config-if-Vlan1)#no shutdown
Для активации функции Telnet сервера пользователь должен включить её в режиме
глобального конфигурирования, как показано ниже:
Switch>enable
Switch#config
Switch(config)# telnet-server enable
```

Шаг 2. Запуск программы Telnet Client

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



Шаг 3. Получить доступ к коммутатору.

Для того, что бы получить доступ к конфигурации через интерфейс Telnet необходимо ввести достоверный логин (login) и пароль (password). В противном случае в доступе будет отказано. Этот метод помогает избежать неавторизованного получения доступа. Как результат, когда Telnet включен для настройки и управления коммутатора, имя пользователя (username) и пароль (password) для авторизованных пользователей

должны быть настроены следующей командой: `username <username> privilege<privilege> [password (0|7) <password>]`.

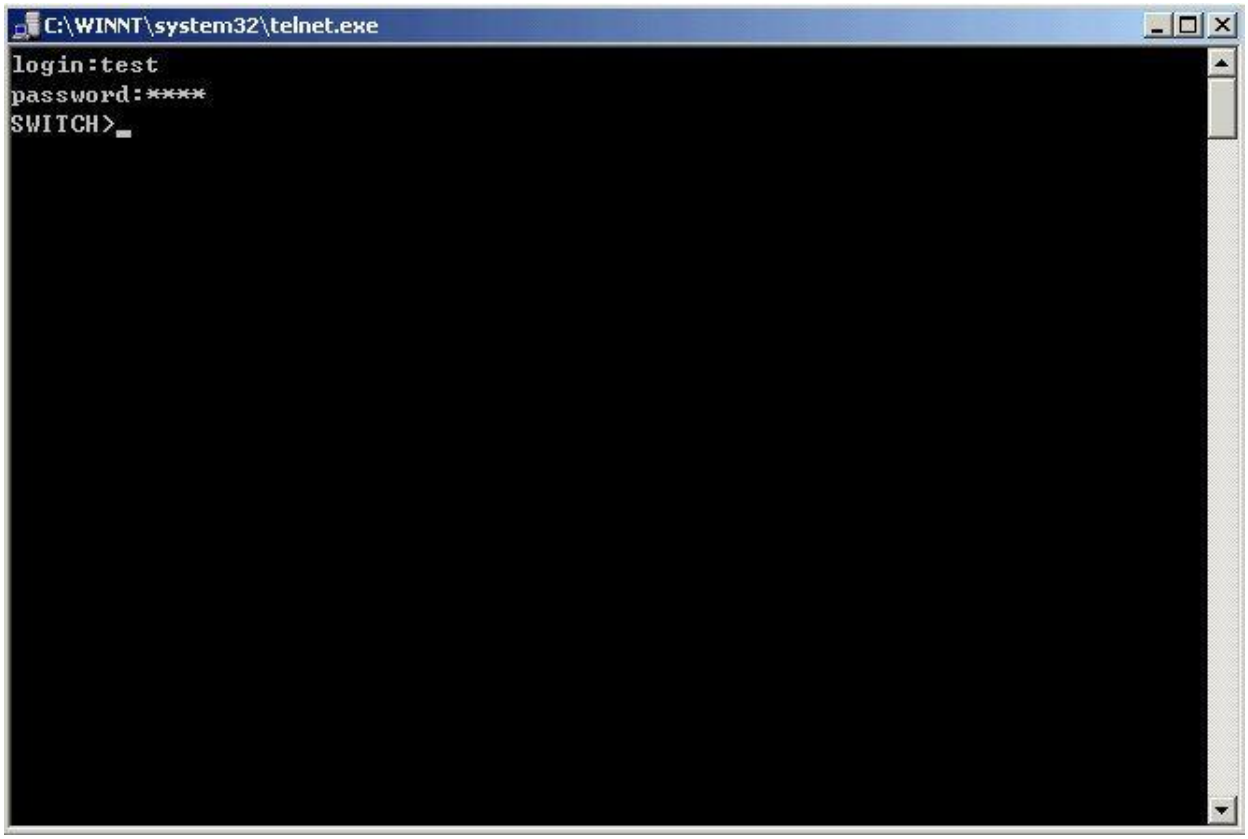
Для локальной аутентификации можно использовать следующую команду:

```
authentifcation line vty login local.
```

Для доступа в привилегированный режим необходимо и задан уровень привилегий 15. Допустим, авторизованный пользователь имеет имя “test” и пароль “test”, тогда процедура задания имени и пароля для доступа по Telnet:

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

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



1.1.2.2 Управление через HTTP

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

1. Коммутатор должен иметь сконфигурированный IPv4/IPv6 адрес.

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

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

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

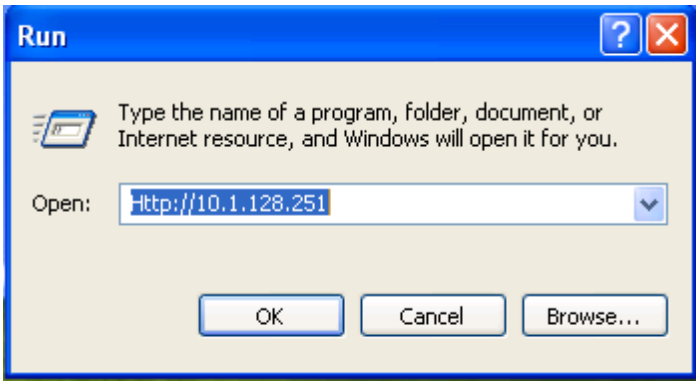
О настройке IP-адреса коммутатора с помощью внеполосного управления, смотри главу о настройке Telnet управления.

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

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

Шаг 2. Запуск Web-браузера на хосте.

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



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

Шаг 3. Получение доступа к коммутатору.

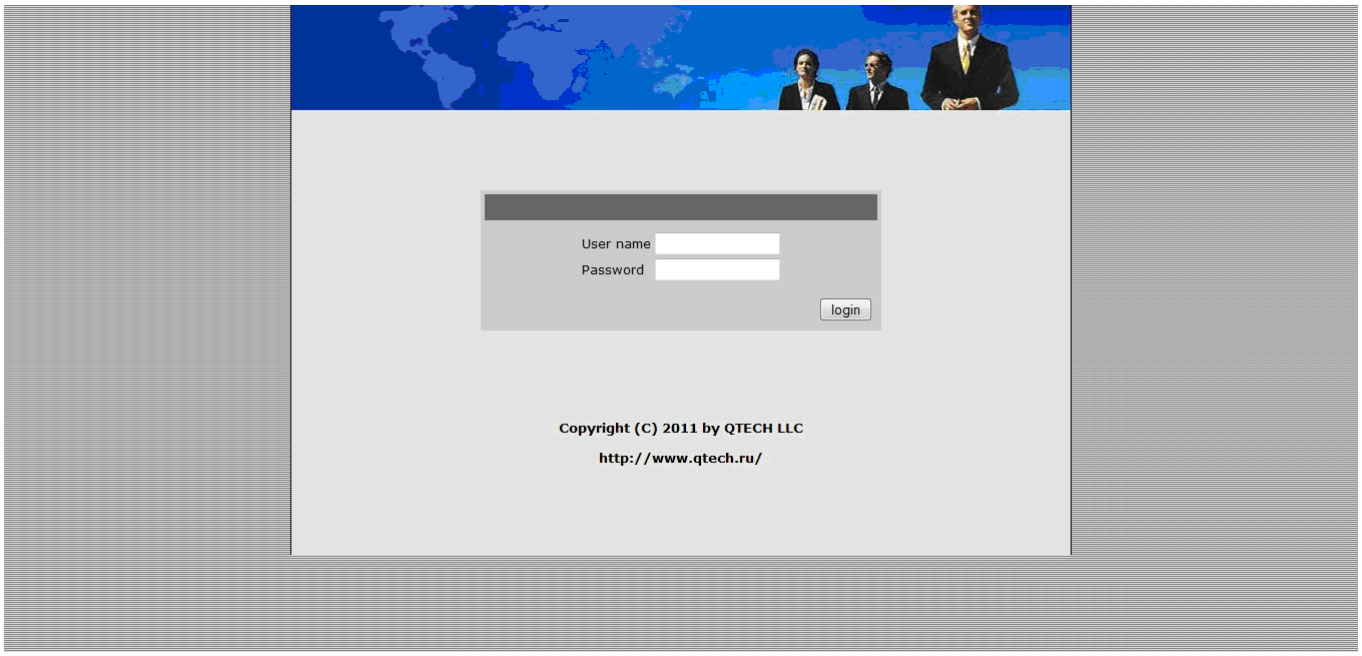
Для того чтобы получить доступ конфигурации с использованием WEB интерфейса, необходимо ввести достоверный логин (login) и пароль (password), в противном случае будет отказано в доступе. Этот метод помогает избежать неавторизованного доступа. Как результат, когда Telnet включен для настройки и управления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

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

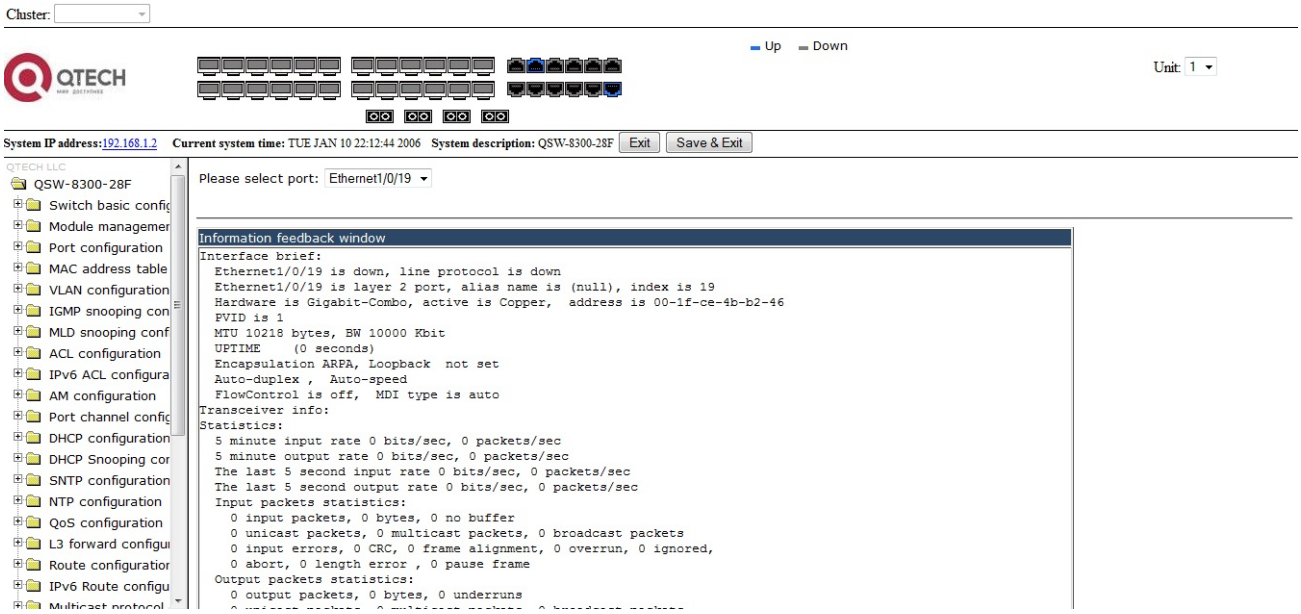
Для доступа в привилегированный режим необходимо и задан уровень привилегий 15.Допустим, авторизованный пользователь имеет имя «admin» и пароль «admin», тогда процедура настройки следующая:

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

Web интерфейс входа выглядит следующим образом:



Введите достоверные имя пользователя и пароль, затем вы попадете в главное меню настройки Web интерфейса, как это показано ниже:



1.1.2.3 Управление коммутатором через сетевое управление SNMP

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

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

1.2 CLI интерфейс

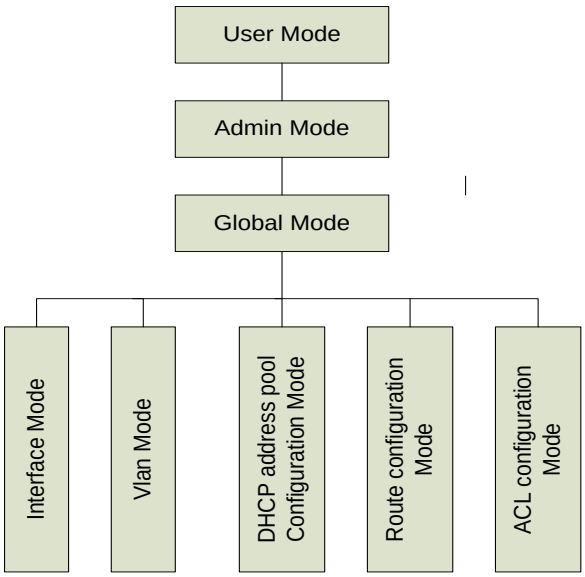
Коммутатор обеспечивает три интерфейса управления для пользователя: CLI (Command Line Interface) интерфейс, веб-интерфейс, сетевое управление программным обеспечением SNMP. Мы познакомим вас с CLI(Консолью), веб-интерфейсом и их конфигурациями в деталях, SNMP пока не будет рассматриваться. CLI интерфейс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

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

Возможности Shell для коммутаторов описаны ниже:

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

1.2.1 Режим настройки



1.2.1.1 Режим пользователя

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

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

1.2.1.2 Режим администратора

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

позволяет простым способом выйти в режим администратора из любого режима конфигурации (за исключением пользовательского).

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

1.2.1.3 Режим глобального конфигурирования.

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

Режим конфигурирования интерфейса

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

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

Режим VLAN

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

Режим DHCP Address Pool

Введите команду ip dhcp pool <name> в режиме глобального конфигурирования для входа в режим DHCP Address Pool. Приглашение этого режима «Switch(Config-<name>-dhcp)#». В этом режиме происходит конфигурирование DHCP Address Pool. Выполните команду выхода, чтобы выйти из режима конфигурирования DHCP Address Pool в режим глобального конфигурирования.

Режим роутера

Протоколы маршрутизации	Команда	Действие команды	Выход
Протокол маршрутизации RIP	Наберите команду **router rip** в режиме глобального конфигурирования	Настройка параметров RIP протокола	Используйте команду **exit** для возвращения в глобальный режим
Протокол маршрутизации OSPF	Наберите команду **router ospf** в режиме глобального конфигурирования	Настройка параметров OSPF протокола	Используйте команду **exit** для возвращения в глобальный режим
Протокол маршрутизации BGP	Наберите команду **router bgp <AS mumber>** в режиме глобального конфигурирования.	Настройка параметров BGP протокола	Используйте команду **exit** для возвращения в глобальный режим

ACL режим

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

1.2.2 Настройка синтаксиса

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

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

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

Вот примеры некоторых актуальных команды конфигурации:

- ❖ show version, параметры не требуется. Это команда, состоящая только из ключевых слов и без параметров.
- ❖ vlan <vlan-id>, необходим ввод значения параметров после ключевого слова.
- ❖ firewall {enable | disable}, этой командой пользователь может включить или выключить брандмауэр, следует лишь выбрать нужный параметр.
- ❖ snmp-server community {ro | rw} <string>,ниже приведены возможные варианты:
  - ✓ snmp-server community ro <string>
  - ✓ snmp-server community rw <string>

1.2.3 Сочетания клавиш

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

Клавиша (и)	Функция	
Back Space	Удалить символ перед курсором. Курсор перемещается назад.	
Вверх “↑”	Показать предыдущую введенную команду. Отображение до десяти недавно набранных команд.	
Вниз “↓”	Показать следующую введенную команду. При использовании клавиши вверх “↑”, вы получаете ранее введенные команды, при использовании клавиши вниз “↓”, вы возвращаетесь к следующей команде.	
Влево “←”	Курсор перемещается на один символ влево.	Вы можете использовать клавиши влево “←” и вправо “→” для изменения введенных команд.
Вправо“→”	Курсор перемещается на один	

	символ вправо.	
Ctrl +p	Такая же, как и у клавиши вверх “↑”.	
Ctrl +n	Такая же, как и у клавиши вниз “↓”.	
Ctrl +b	Такая же, как и у клавиши влево “←”.	
Ctrl +f	Такая же, как и у клавиши вправо “→”.	
Ctrl +z	Вернуться в Режим администратора непосредственно из других режимов настройки (за исключением пользовательского режима)	
Ctrl +c	Остановка непрерывных процессов команд, таких как пинг и т.д.	
Tab	В процессе ввода команды клавиша Tab может быть использована для ее завершения, если нет ошибок.	

1.2.4 Справка

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

Доступ к справке	Использование и функции
Help	Под любой командной строкой введите "help" и нажмите Enter, вы получите краткое описание из справочной системы.
“?”	1. Под любой командной строкой введите "?", чтобы получить список команд для текущего режима с кратким описанием. 2. Введите "?" после команды. Если позиция должна быть параметром, описание этого параметра типа, масштаба и т.д., будут отображены, если позиция должна быть ключевым словом, то будет отображен набор ключевых слов с кратким описанием, если вышло "<cr > ", то команда введена полностью, нажмите клавишу Enter, чтобы выполнить команду. 3. Введите "?" сразу после строки. Это покажет все команды, которые начинаются с этой строки.

1.2.5 Проверка ввода

1.2.5.1 Отображаемая информация: успешное выполнение (successfull)

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

1.2.5.2 Отображаемая информация: ошибочный ввод (error)

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

1.2.6 Поддержка языка нечеткой логики (Fuzzy math)

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

Например:

1. Команда “show interface ethernet status”, будет работать даже в том случае, если набрать “sh in ethernet status ”.
2. Однако, при наборе команды “show running-config” как “show r” система сообщит “> Ambiguous command!”, т.к. Shell будет не в состоянии определить, что имелось ввиду, “show radius” или “show running-config”. Таким образом, Shell сможет правильно распознать команду, только если будет набрано “sh ru”.

2 ОСНОВНЫЕ НАСТРОЙКИ КОММУТАТОРА

2.1 Основные настройки

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

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

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

2.2 Управление Telnet

2.2.1 Telnet

2.2.1.1 Введение в Telnet

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

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

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

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

2.2.1.2 Команды конфигурирования Telnet

1. Настройка Telnet сервера.

Команда	Описание
Режим глобального конфигурирования	
telnet-server enable **no telnet-server enable**	Активирует функцию Telnet сервера на коммутаторе, команда “**no**”

	деактивирует эту функцию.
username <*user-name*> [privilege <*privilege*>] [password [0 | 7] <*password*>] **no username <*username*>**	Настраивает имя пользователя и пароль для доступа по Telnet . Команда “**no**” удаляет данные авторизации выбранного пользователя.
authentication securityip <*ip-addr*> **no authentication securityip <*ip-addr*>**	Настраивает безопасность IP адресов для входа на коммутатор по Telnet: команда “**no**” отменяет предыдущую команду.
authentication securityipv6 <*ipv6-addr*> **no authentication securityipv6 <*ipv6-addr*>**	Настраивает безопасность IPv6 адресов для входа на коммутатор по Telnet: команда “**no**” отменяет предыдущую команду.
authentication ip access-class {<num-std>|<name>} **no authentication ip access-class**	Связывает стандартный IP ACL с Telnet / SSH /Web; команда “**no**” отменяет предыдущую команду.
authentication ipv6 access-class {<num-std>|<name>} **no authentication ipv6 access-class**	Связывает IPv6 ACL с Telnet / SSH /Web; команда “**no**” отменяет предыдущую команду.
authentication line {console | vty | web} login {local | radius | tacacs } **no authentication line {console | vty | web} login**	Настройка режима аутентификации Telnet.
authorization line {console | vty | web} exec {local | radius | tacacs} **no authorization line {console | vty | web} exec**	Настройка режима авторизации Telnet.
Режим администратора	
terminal monitor **terminal no monitor**	Отображение отладочной информации для входа на коммутатор через Telnet клиент; Команда “**no**” отключает отображение данной информации.

2. Использование Telnet для удаленного доступа к коммутатору.

Команда	Описание

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

2.2.2 SSH

2.2.2.1 Введение в SSH

SSH (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 коммутатору соответствующему требованиям SSH2.0, необходимо SSH2.0 клиентское программное обеспечение, такое, как SSH Secure Client и Putty. Пользователи могут запускать вышеперечисленное программное обеспечение для управления коммутатором удаленно. Коммутатор в настоящее время поддерживает аутентификацию RSA, 3DES и SSH шифрование протокола, пароль пользователя аутентификации и т.д.

2.2.2.2 Список команд для конфигурирования SSH сервера

Команда	Описание
Режим глобального конфигурирования	
ssh-server enable **no ssh-server enable**	Активация функции на коммутаторе; команда “**no**” отменяет предыдущую команду.
username <*username*> [privilege <*privilege*>] [password [0 | 7] <*password*>] **no username <*username*>**	Настраивает имя пользователя и пароль для доступа к коммутатору через SSH клиент . Команда “**no**” удаляет данные авторизации выбранного пользователя.
ssh-server timeout <*timeout*> **no ssh-server timeout**	Настройка таймаута для аутентификации SSH; Команда “**no**” восстанавливает значения по умолчанию таймаута для аутентификации SSH.
ssh-server authentication-retires <*authentication-retires*> **no ssh-server authentication-retries**	Настройка число повторных попыток SSH аутентификации; Команда “**no**” восстанавливает значения по умолчанию.
ssh-server host-key create rsa modulus <*moduls*>	Создание нового RSA ключа хоста на SSH сервере.

Режим администратора	
terminal monitor **terminal no monitor**	Показ отладочной информации SSH на стороне клиента; команда “**no**” отменяет предыдущую команду.

2.2.2.3 Пример настройки SSH сервера

Пример 1:

Задачи:

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

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

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

2.3 Настройка IP адресов коммутатора

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

- ❖ Ручной метод.
- ❖ BOOTP.
- ❖ DHCP.

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

В BOOTP/DHCP режиме коммутатор работает как BOOTP/DHCP клиент, отправляя широковещательные пакеты BOOTP запроса на BOOTP/DHCP-сервера. BOOTP/DHCP сервер назначает адрес отправителю запроса, кроме того, коммутатор может работать в качестве сервера DHCP и динамически назначать параметры сети, такие, как IP-адреса,

шлюз и адреса DNS-серверов DHCP клиентам, что подробно описано в последующих главах.

2.3.1 Список команд для настройки IP адресов

1. Включение VLAN режима.

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

2. Ручная настройка.

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

3. BOOTP конфигурация.

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

4. DHCP конфигурация.

Команда	Описание
VLAN режим	
ip dhcp-client enable **no ip dhcp-client enable**	Включение коммутатора как DHCP клиента для получения IP-адреса и адреса шлюза путем запросов DHCP. Команда “**no**” выключает DHCP клиент.

2.4 Настройка SNMP

2.4.1 Введение в SNMP

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

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

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

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

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

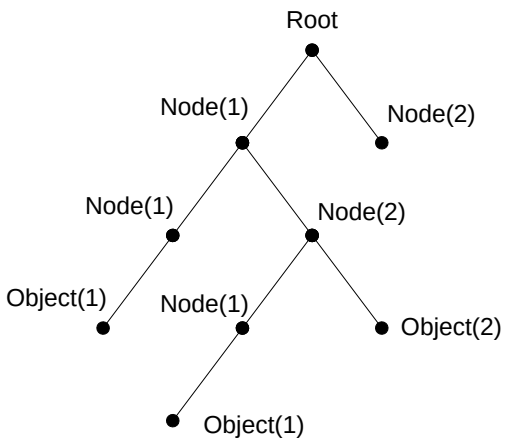
NMS связывается с агентом с помощью запросов: Get-Request, Get-Next-Request, Get-Bulk-Request and Set-Request, агент, при получении запросов, отвечает сообщением Get-Response. О некоторых специальных ситуациях, таких, как изменения статусов сетевых портов устройства или изменения топологии сети, агенты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

USM обеспечивает безопасную передачу, хорошо продуманное шифрование и аутентификацию. USM шифрует сообщения в зависимости от ввода пароля пользователя. Этот механизм гарантирует, что сообщения не могут быть просмотрены во время передачи. Также USM Аутентификация гарантирует, что сообщение не может быть изменено при передаче. USM использует DES-CBC криптографию. И HMAC-MD5 и HMAC-SHA используются для аутентификации.

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

2.4.2 Введение в MIB

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



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

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

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

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

2.4.3 Введение в RMON

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

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

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

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

2.4.4 Настройка SNMP

2.4.4.1 Список команд для настройки SNMP

1. Включение и отключение функции SNMP агента.

Команда	Описание
Режим глобального конфигурирования	
snmp-server enabled **no snmp-server enabled**	Включение функции SNMP агента на коммутаторе. Команда “**no**” выключает эту функцию.

2. Настройка строки сообщества в SNMP.

Команда	Описание
Режим глобального конфигурирования	
snmp-server community {ro|rw} *<string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}] [read *<read-view-name>*] [write *<write-view-name>*] **no snmp-server community *<string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**	Настройка строки сообщества в SNMP для коммутатора. Команда “**no**” удаляет эту строку.

3. Настройка IP-адреса станции управления SNMP.

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

4. Настройка engine ID.

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

5. Настройка пользователя.

Команда	Описание
Режим глобального конфигурирования	
snmp-server user *<use-string>* *<group-string>* [{authPriv | authNoPriv} auth {md5 | sha} *<word>*] [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}] **no snmp-server user *<user-string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**	Добавление пользователя в SNMP группу. Эта команда используется для настройки USM для SNMP v3.

6. Настройка группы.

Команда	Описание
Режим глобального конфигурирования	
snmp-server group *<group-string>* {noauthnopriv|authnopriv|authpriv} [[read *<read-string>*] [write *<write-string>*] [notify *<notify-string>*]] [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}] **no snmp-server group *<group-string>* {noauthnopriv|authnopriv|authpriv} [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**	Установка информации о группе на коммутаторе. Эта команда используется для настройки VACM для SNMP v3.

7. Настройка вида.

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

8. Настройка TRAP.

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

9. Включение/выключение RMON

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

2.4.5 Типичные примеры настройки SNMP

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

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

Конфигурация коммутатора, записана ниже:

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

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

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

Конфигурация коммутатора, изложена ниже:

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

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

Конфигурация коммутатора, изложена ниже:

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

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

Конфигурация коммутатора, изложена ниже:

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

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

Конфигурация коммутатора, изложена ниже:

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

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

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

Конфигурация коммутатора, изложена ниже:

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

2.4.6 Поиск неисправностей SNMP

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

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

- Если пользователь по-прежнему не может решить проблемы с SNMP, обращайтесь в технический центр.

2.5 Модернизация коммутатора

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

2.5.1 Системные файлы коммутатора

Системные файлы включают в себя файлы образа системы(image) и загрузочные(boot) файлы. Обновление системных файлов коммутатора 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”. IMG файл может быть сохранен только в FLASH с определенным названием nos.img.

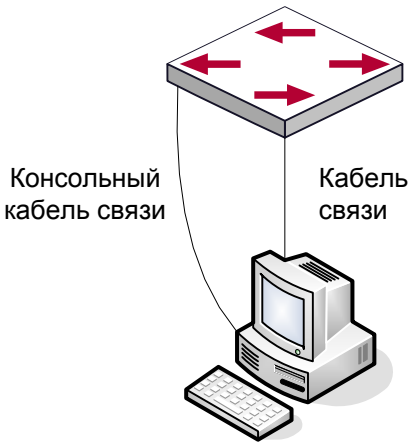
Загрузочные(boot) файлы необходимы для загрузки и запуска коммутатора, это то, что мы обычно называем “ROM file”(могут быть сжаты в IMG файлы, если они слишком больших размеров). В коммутаторе загрузочные файлы разрешено сохранять в только в ROM.

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

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

2.5.2 BootROM обновление

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



Процедура обновления перечислена ниже:

Шаг 1:

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

Шаг 2:

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

[Boot]:

Шаг 3:

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

```
[Boot]: setconfig
Host IP Address: [10.1.1.1] 192.168.1.2
Server IP Address: [10.1.1.2] 192.168.1.66
FTP(1) or TFTP(2): [1] 2
Network interface configure OK.
[Boot]
```

Шаг 4:

Включить FTP / TFTP сервер на ПК. Для TFTP запустите программу сервера TFTP, для FTP запустите программу FTP-сервер. Прежде, чем начать загрузку файла обновления на коммутатор, проверьте соединение между сервером и коммутатором с помощью пинга с сервера. Если пинг успешен, запустите команду "load" в BootROM режиме. Если это не удается, устранените неполадоки. Ниже показана конфигурация для обновления файла образа системы:

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

Шаг 5:

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

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

Шаг 6:

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

```
[Boot]: load boot.rom
Loading…
Loading file ok!
```

Шаг 7:

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

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

Шаг 8:

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

```
[Boot]: load config.rom
Loading...
Loading file ok!
```

Шаг 9:

Далее выполняем запись flash:/config.rom в режиме BootROM. Этот шаг позволяет сохранить обновленный файл.

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

Шаг 10:

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

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

Остальные команды в BootROM режиме.

Команда DIR – используется для вывода списка существующих файлов в FLASH.

```
[Boot]: dir
config.rom                              405,664 1980-01-01 00:00:00 --SH
boot.rom                              2,608,352 1980-01-01 00:00:00 --SH
```

```
boot.conf                              256 1980-01-01 00:00:00 ----
nos.img                              8,071,910 1980-01-01 00:00:00 ----
startup.cfg                            1,590 1980-01-01 00:00:00 ----
```

2.5.3 Обновление FTP/TFTP

2.5.3.1 Введение в FTP/TFTP

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

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

Существует два типа таких соединений: активные и пассивные соединения.

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

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

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

Коммутатор может работать как FTP/TFTP клиент или сервер. Когда коммутатор работает как FTP/TFTP клиент, файлы конфигурации и системные файлы можно загрузить с удаленного FTP/TFTP сервера (это могут быть как хосты, так и другие коммутаторы) без ущерба для его нормальной работы. И также может быть получен список файлов с сервера в режиме FTP клиента. Конечно, коммутатор может также загрузить текущие конфигурационные файлы и системные файлы на удаленный FTP/TFTP сервер (это могут

быть как хосты, так и другие коммутаторы). Когда коммутатор работает как FTP/TFTP сервер, он может обеспечить загрузку и выгрузку файлов для авторизованных FTP/TFTP клиентов.

Вот некоторые термины часто используемые в FTP/TFTP.

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

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

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

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

System image file: файл образа системы включает в себя сжатые файлы аппаратных драйверов, файлы программного обеспечения, это то, что мы обычно называем “IMG file”. IMG файл может быть сохранен только в FLASH. Коммутатор позволяет загрузить файл образа системы через FTP в режиме Shell только с определенным названием nos.img, другие файлы IMG будут отклонены.

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

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

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

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

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

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

2.5.3.2 Настройка FTP/TFTP

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

Настройка FTP/TFTP клиента

1. Загрузка файлов FTP/TFTP клиентом.

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

2. Просмотр доступных файлов на FTP сервере.

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

Настройка FTP сервера

1. Запуск FTP сервера.

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

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

Команда	Пояснение
Глобальный режим	
ip ftp username *<username>* password	Настройка имени пользователя и пароля для

[0 | 7] <*password*> **no ip ftp username<*username*>**	входа на FTP сервер. Команда “no” удалит имя пользователя и пароль

3. Изменение времени ожидания FTP сервера.

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

Настройка TFTP сервера

1. Запуск TFTP сервера

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

2. Изменение времени ожидания TFTP сервера.

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

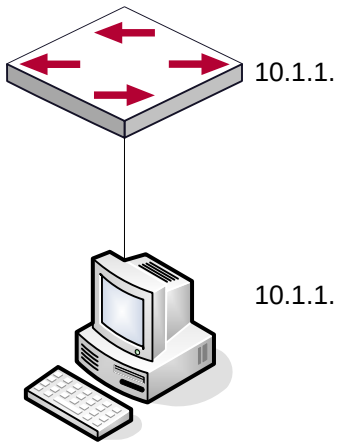
3. Настройка количества раз ретрансляции до таймаута для неповрежденных пакетов.

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

<number>	

2.5.3.3 Примеры настройки FTP/TFTP

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



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

Настройка FTP

Настройка компьютера:

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

Далее описана процедура настройки коммутатора:

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

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

Далее описана процедура настройки коммутатора:

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

Настройка компьютера:

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

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

Далее описана процедура настройки коммутатора:

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

Настройка компьютера:

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

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

Настройка TFTP:

Настройка компьютера:

Запустите FTP сервер на компьютере и установите имя пользователя “Switch”, и пароль “superuser”.

Настройка коммутатора:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch#copy ftp: //Switch: superuser@10.1.1.1
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
```

```
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
recv total = 480
nos.img
nos.rom
parsecommandline.cpp
position.doc
qmdict.zip
…(some display omitted here)
show.txt
snmp.TXT
226 Transfer complete.
```

2.5.3.4 Устранение неисправностей FTP/TFTP

Поиск неисправностей FTP

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

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

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

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

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
```

```
200 PORT Command successful.
recv total = 1526037
**********************
write ok
150 Opening ASCII mode data connection for nos.img (1526037 bytes).
226 Transfer complete.
```

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

Поиск неисправностей TFTP

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

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

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

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

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

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

3 ОПЕРАЦИИ С ФАЙЛОВОЙ СИСТЕМОЙ

3.1 Введение в Устройства хранения данных (File Storage Devices)

В качестве устройства для хранения данных в коммутаторах используются, в основном, flash-карты. Как наиболее распространённые устройства хранения, flash-карты используются для хранения образов системы (IMG files), файлов загрузки системы (ROM files) и файлов конфигурации системы (CFG files).

Файлы на flash-памяти можно копировать, удалять или переименовывать в режиме Shell или BootRom.

3.2 Список команд для конфигурирования файловой системы

1. Форматирование устройства хранения данных

Команда	Пояснение
Режим администратора	
format <*device*>	Форматирование устройства хранения данных

2. Создание подкаталогов

Команда	Пояснение
Режим администратора	
mkdir <*directory*>	Создание подкаталога в указанной директории текущего устройства.

3. Удаление подкаталогов

Команда	Пояснение
Режим администратора	
rmdir <*directory*>	Удаление подкаталога в указанной директории текущего устройства.

4. Изменение текущего рабочего каталога для устройства хранения данных.

Команда	Пояснение
Режим администратора	
cd <*directory*>	Изменяет текущий рабочий каталог на указанный.

5. Отображение текущего рабочего каталога.

Команда	Пояснение
Режим администратора	
pwd	Отображет текущий рабочий каталог

6. Отображение информации об указанных файлах и каталогах.

Команда	Пояснение
Режим администратора	
dir [WORD]	Отображение информации об указанном файле или каталоге.

7. Удаление указанного файла из файловой системы.

Команда	Пояснение
Режим администратора	
delete <*file-url*>	Удаляет указанный файл из системы

8. Переименовывание файлов.

Команда	Пояснение
Режим администратора	
rename <*source-file-url*> <*dest-file*>	Переименовывает указанный файл.

9. Копирование файлов.

Команда	Пояснение
Режим администратора	
copy <*source-file-url* > <*dest-file-url*>	Копирует указанный файл в указанное место

3.3 Типичные области применения

Копирование IMG файла flash:/nos.img, хранящегося на FLASH-памяти, установленной на материнской карте в cf:/nos-6.1.11.0.img.

Настройки коммутатора выглядят следующим образом:

```
Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img
Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y:N] y
Copyed file flash:/nos.img to flash:/nos-6.1.11.0.img.
```

3.4 Поиск проблем

Если возникают ошибки, когда пользователи пытаются осуществить операции с файловой системой, пожалуйста, проверьте, могут ли они быть вызваны следующими причинами:

- Правильно ли введены имена файлов или пути.
- Правильно ли переименованы файлы, будь то использование или создание нового имени файла, который уже используется в данном файле или каталоге.

4 НАСТРОЙКА КЛАСТЕРА

4.1 Введение в управление кластерами сети

Настройка кластеров осуществляется при помощи внутриполосного управления конфигурацией. В отличие от CLI, SNMP и веб-конфигурации, которые осуществляют непосредственное управление целевых коммутаторов через управляющую рабочую станцию, управление кластерной сетью реализуется путем настройки целевых коммутаторов (коммутаторы-члены) через промежуточный коммутатор (главный коммутатор). Таким образом, главный коммутатор может управлять несколькими коммутаторами. Как только будет настроен публичный IP адрес в главном коммутаторе, управление всеми коммутаторами, которые настраиваются с частным IP-адресом, происходит дистанционно. Эта функция экономит публичные IP-адреса, которых осталось не так много. Обнаружение новых коммутаторов может происходить динамически, если на коммутаторе включена функция кластера (коммутатор-кандидат) либо сетевые администраторы могут статически добавлять коммутаторы-кандидаты в кластер, который уже установлен. Соответственно, они могут настраивать и управлять коммутаторами через главный коммутатор. Когда коммутаторы члены расположены в различных физических местах (например, на разных этажах одного и того же здания), управление сетевым кластером имеет очевидные преимущества, нет необходимости для создания специальной сети для управления сетью.

Кластер сетевого управления имеет следующие возможности:

- Сохранение IP-адресов;
- Упрощение задач конфигурирования;
- Топология сети и расстояния не имеют значения;
- Автоматическое обнаружение и автоматическая настройка;
- Несколько коммутаторов могут управляться с помощью кластера управления сетью с заводскими настройками;
- Главный коммутатор может модернизировать и настраивать любой коммутатор-член в кластере.

4.2 Список команд для конфигурирования кластера управления сети:

1. Включение или отключение функции кластера.
2. Создание кластера.
   - ✓ Настройка пула частных IP-адресов для коммутаторов-членов кластера;
   - ✓ Создание или удаление кластера;
   - ✓ Добавление или удаление коммутатора-члена.
3. Настройка атрибутов кластера в главном коммутаторе.
   - ✓ Включение или отключение автоматического добавления коммутаторов в кластер;
   - ✓ Установка автоматически добавленных членов как добавленных вручную;
   - ✓ Установка или изменение временного интервала сообщений проверки активности (keep-alive) на коммутаторах в кластере.

- ✓ Установка максимально допустимого количества потерянных “Keep-Alive” сообщений;
- ✓ Очистка списка коммутаторов-кандидатов, поддерживаемых коммутатором.

4. Настройка атрибутов кластера в коммутаторах-кандидатах.
   - ✓ Установка интервала времени “Keep-Alive” сообщений кластера;
   - ✓ Установка максимального количества потерянных “Keep-Alive” сообщений, которое может быть допустимо в кластере.
5. Удаленное управление кластерной сетью.
   - ✓ Удаленное управление конфигурацией;
   - ✓ Удаленное обновление коммутаторов-членов;
   - ✓ Перезагрузка коммутатора-члена.
6. Управление кластерной сетью через Web.
   - ✓ Enable http.
7. Управление кластерной сетью через snmp.
   - ✓ Enable snmp server.

1. Включение или отключение кластера.

Команда	Пояснение
Режим глобального конфигурирования	
cluster run [key <*WORD*>] [vid <*VID*>] **no cluster run**	Включить или выключить функцию кластера в коммутаторе.

2. Создание кластера.

Команда	Пояснение
Режим глобального конфигурирования	
cluster ip-pool <*commander-ip*> **no cluster ip-pool**	Настройка пула частных IP-адресов для устройств кластера.
cluster commander [<*cluster_name*>] **no cluster commander**	Создание или удаление кластера.
cluster member {candidate-sn <*candidate-sn*> | mac-address <*mac-addr*> [id <*member-id*>]} **no cluster member {id <*member-id*> | mac-address <*mac-addr*>}**	Добавить или удалить коммутатор-участник.

3. Настройка атрибутов кластера в главном коммутаторе.

Команда	Пояснение
Режим глобального конфигурирования	
cluster auto-add **no cluster auto-add**	Включение или отключение добавления новых обнаруженных коммутаторов-кандидатов в кластер.
cluster member auto-to-user	Установка автоматически добавленных членов как добавленных вручную
cluster keepalive interval <*second*> **no cluster keepalive interval**	Установка интервала проверки активности кластера
cluster keepalive loss-count <*int*> **no cluster keepalive loss-count**	Установка максимального количества потерянных Keep-Alive сообщений, которые допускаться в кластере.
Режим администратора	
clear cluster nodes [nodes-sn <*candidate-sn-list*> | mac-address <*mac-addr*>]	Очистить список коммутаторов-кандидатов, поддерживаемый коммутатором.

4. Настройка атрибутов кластера в коммутаторе кандидате.

Команда	Пояснение
Глобальный режим	
cluster keepalive interval <*second*> **no cluster keepalive interval**	Установка интервала проверки активности кластера.
cluster keepalive loss-count <*int*> **no cluster keepalive loss-count**	Установка максимального количества потерянных Keep-Alive сообщений, которые допускаются в кластере.

5. Удаленное управление кластерной сетью.

Команда	Пояснение
Режим администратора	
rcommand member <*member-id*>	В главном коммутаторе эта команда используется для настройки и управления коммутаторами-членами.
rcommand commander	В коммутаторе члене эта команда используется для настройки главного коммутатора.
cluster reset member [id <*member-id*> | mac-address <*mac-addr*>]	В главном коммутаторе эта команда используется для восстановления настроек для коммутатора–члена.
cluster update member <*member-id*> <*src-url*> <*dst-filename*>[ascii | binary]	В главном коммутаторе эта команда используется для удаленного обновления коммутатора-члена, обновляется только файл nos.img.

6. Управление кластерной сетью через web.

Команда	Пояснение
Режим глобального конфигурирования	
ip http server	Включение функции HTTP в главном коммутаторе и коммутаторах-членах. Примечание: необходимо убедиться, что HTTP функция активна в коммутаторах-членах, когда главный коммутатор посещает коммутатор-член через web.

7. Управление кластерной сетью через snmp.

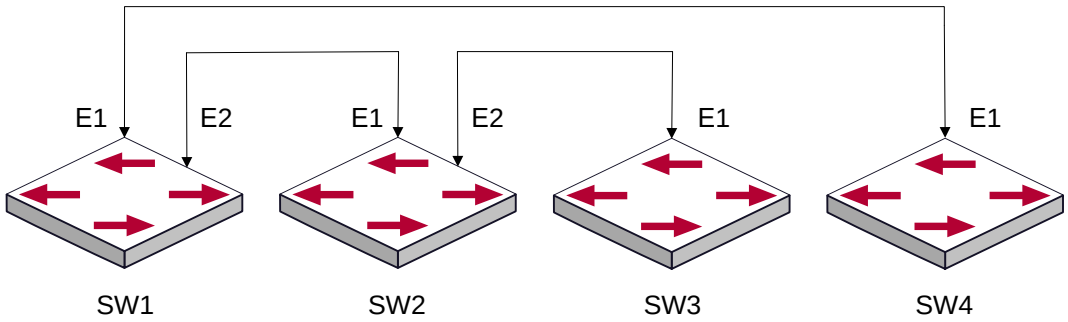
Команда	Пояснение
Режим глобального конфигурирования	
snmp-server enable	Включение функции SNMP сервера в главном коммутаторе и коммутаторах-членах. Примечание: необходимо убедиться, что функция SNMP сервера активна в коммутаторах-членах, когда

	главный коммутатор посещает их через SNMP. Главный коммутатор посещает коммутатор-член через настройки командной строки <commander-community>@sw<member id>

4.3 Примеры администрирования кластера

Сценарий:

Имеется четыре коммутатора SW1-SW4, среди них SW1 является главным коммутатором, а другие коммутаторами-членами и SW2 и SW4 напрямую подключены с главным, SW3 подключается к коммутатору через SW2.



Процедура настройки:

1. Настройка главного коммутатора.

Настройки SW1:

```
Switch(config)#cluster run
Switch(config)#cluster ip-pool 10.2.3.4
Switch(config)#cluster commander 5526
Switch(config)#cluster auto-add
```

2. Настройка коммутатора-члена.

Настройки SW2-SW4

```
Switch(config)#cluster run
```

4.4 Поиск проблем в администрировании кластерами

При возникновении проблем в применении кластерного управления, пожалуйста, проверьте следующие настройки:

Проверьте, что главный коммутатор настроен правильно и включена функция автоматического добавления. Главный коммутатор и коммутаторы члены относятся к кластерной VLAN.

После назначения кластерной VLAN в главном коммутаторе не включайте протоколы маршрутизации (RIP, OSPF, BGP) в этой VLAN сети для того, чтобы предотвратить образование петель маршрутизации.

Проверьте, есть ли связь между главным коммутатором и коммутаторами-членами, правильно ли она настроена. Необходимо проверить могут ли главный коммутатор и коммутаторы-члены получать и обрабатывать пакеты, связанные с администрированием кластера.