Зелакс ZES

Руководство по настройке
ZES-2026C

Декларация о соответствии: Д-СПД-2592

Редакция 01 от 21.09.2009 г.
ПО 6.0.74.100

Россия, 124681 Москва, г. Зеленоград, ул. Заводская, дом 1Б, строение 2
Телефон: +7 (495) 748-71-78 (многоканальный) • http://www.zelax.ru
Отдел технической поддержки: tech@zelax.ru • Отдел продаж: sales@zelax.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 порт описана ниже:

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

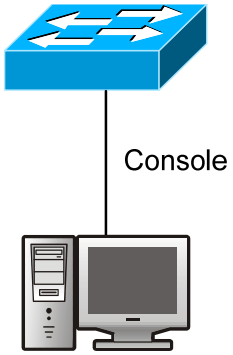

Рис. 1. Подключение ПК к консольному порту коммутатора

Подключитесь к порту RS-232 коммутататора, используя консльный кабель, входящий в комплект поставки.

Персональный компьютер должен иметь порт RS-232 и иметь установленную терминальную программу, например, HyperTerminal, являющаяся стандартной программой операционных систем Windows 9x/NT/2000/XP

Шаг 2: Загрузка программы HyperTerminal.

После того, как соединение будет установлено, загрузите программу HyperTerminal. Ниже приведена процедура настройки, когда используется программа HyperTerminal из стандартного набора программ Windows XP.

1. Загрузите программу HyperTerminal.
2. В открывшемся окне HyperTerminal введите имя, например “Switch_A” (Рис. 2).

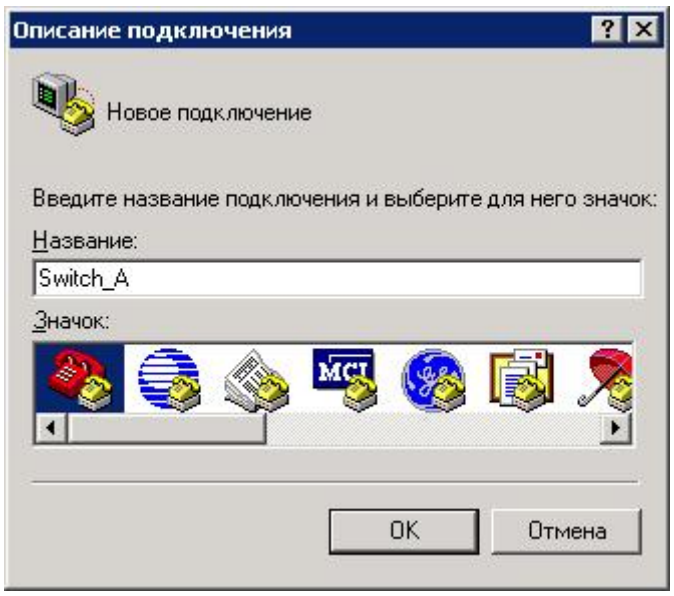

Рис. 2. Окно программы HyperTerminal

3. В раскрывающемся списке “Подключится через”, выберите последовательный порт RS-232, который использует ПК, например COM1, затем нажмите “OK” (Рис. 3)

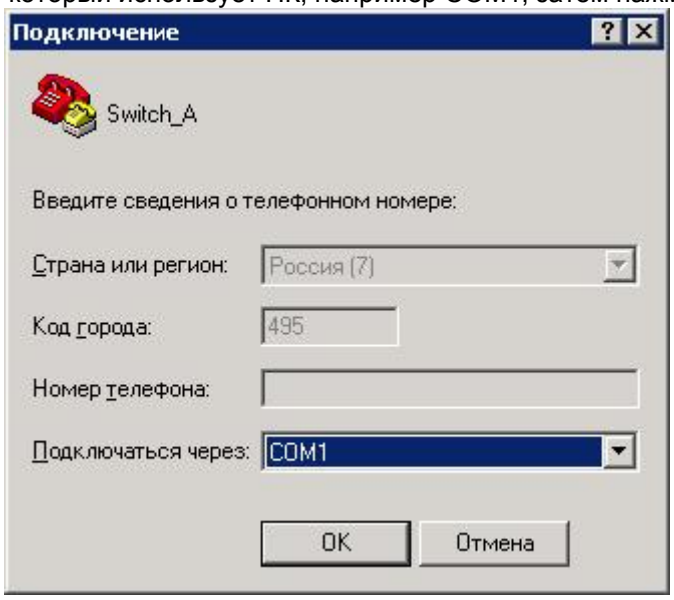

Рис. 3. Окно программы HyperTerminal

4. На открывшейся вкладке свойств порта COM1 выберите Скорость 9600, 8 бит данных, четность отсутствет, 1 стоповый биты и управление потоком отсутствует, затем нажмите “OK” (Рис. 4).

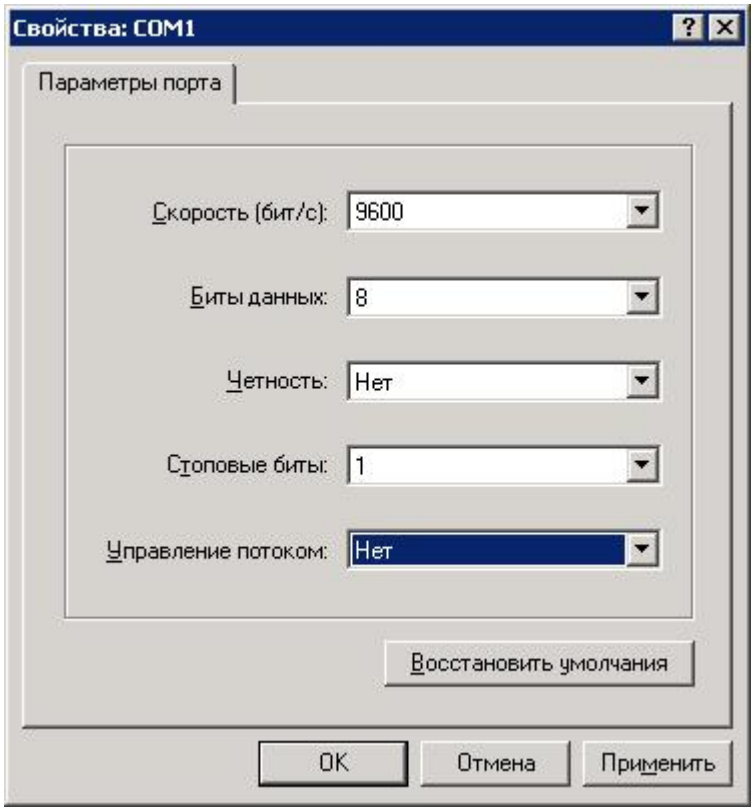

Рис. 4. Окно программы HyperTerminal

Шаг 3: Вызов командного интерфейса (CLI) коммутатора Включите напряжение питания коммутатора. В окне HyperTerminal появится информация о вызове режима CLI-конфигурирования.

```
Testing RAM...
0x03E80000 RAM OK
Initializing...OK
Checking ECC of config.rom...OK

Safe-Block-Write restoring...OK
Booting IMG from FLASH...OK
Checking ECC of IMG...OK

Starting at 0x10000...



Current time is Sun Jan 01 00:00:00 2006

ZES-2026C Series Switch Operating System
Software Version ZES-2026C_6.0.74.100
Compiled Aug 14 15:00:44 2009

Mac Addr 00-1a-81-00-18-9d
ZES-2026C>
```

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

1.1.2 Внутриполосное управление

Внутриполосное управление сетью осуществляется путем доступа к коммутатору по Telnet или HTTP, либо с помощью ПО управления по протоколу 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

Для управления коммутатором по Telnet необходимо подключится к коммутатору (Рис. 5) и должны выполняться следующие условия:

1. Настроен IP-адрес коммутатора для управления;
2. IP-адреса хоста (клиента Telnet) и интерфейса VLAN коммутатора должны находиться в одном и том же сегменте сети.
3. Если условие 2 не выполнено, клиент Telnet может быть подключен к IP-адресу коммутатора через другие устройства, например, через маршрутизатор.

В следующем примере предполагается, что коммутатор еще не использовался и имеет настройки по умолчанию, при этом в системе существует только VLAN1.

Ниже рассмотрены шаги, которые необходимо предпринять для подключения к интерфейсу VLAN1 коммутатора по Telnet.

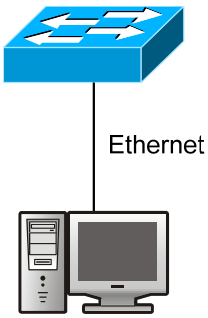

Рис. 5. Управление коммутатором по Telnet

Шаг 1: Настройте IP-адрес коммутатора и включение на коммутаторе функции Telnet-сервера.

Сначала необходимо настроить IP-адрес хоста, который должен находиться в том же сегменте сети, что и IP-адрес интерфейса VLAN1 коммутатора. Предположим, что IP-адрес интерфейса VLAN1 коммутатора 192.168.0.10/24, тогда IP-адрес хоста может быть 192.168.0.20/24. С помощью команды “ping 192.168.0.10” можно проверить, доступен коммутатор или нет.

Команды конфигурирования IP-адреса для интерфейса VLAN1 коммутатора перечислены 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 192.168.0.10 255.255.255.0
Switch(config-if-vlan1)#no shutdown
```

Для того чтобы конфигурирование с помощью Telnet-сервера стало возможным, пользователи должны в глобальном режиме конфигурирования ввести следующую команду:

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

Шаг 2: Запустите Telnet-клиент

Шаг 3: Регистрация на коммутаторе

Зарегистрируйтесь в интерфейсе конфигурирования Telnet. Для этого требуется указать правильное имя и пароль, в противном случае коммутатор будет отвергать доступ по Telnet. Это

сделано для защиты коммутатора от попыток несанкционированного доступа. Поэтому, когда Telnet доступен для конфигурирования коммутатора и управления им, необходимо с помощью команды, приведенной ниже, задать имя и пароль для авторизованных пользователей Telnet: **username** <username> **privilege** <privilege> [**password** (**0**|**7**) <**password**>].

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

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

```
Switch>enable
Switch#config
Switch(config)#username admin privilege 15 password 0 admin
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 (Рис. 6).

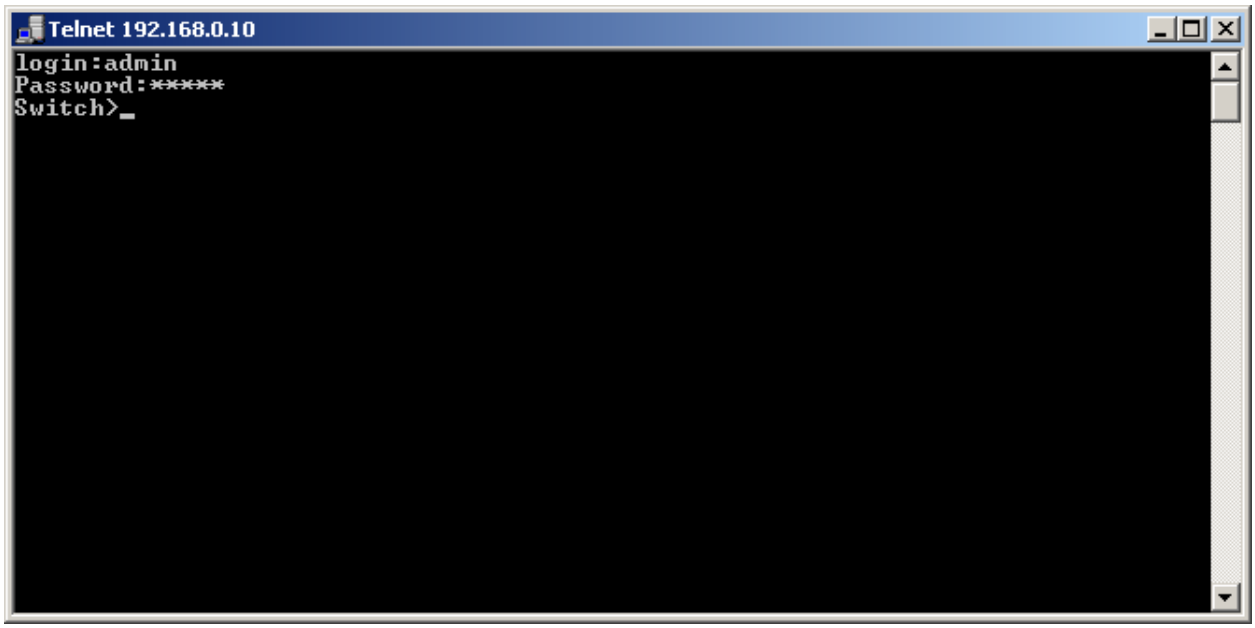

Рис. 6. Интерфейс конфигурирования Telnet

1.1.2.2 Управление через Web-интерфейс

Для управления коммутатором через Web-интерфейс должны выполняться следующие условия:

1. Настроен IP-адрес коммутатора для управления.
2. IP-адреса хоста (клиента HTTP) и интерфейса VLAN коммутатора должны находиться в одном и том же сегменте сети.
3. Если условие 2 не выполнено, пользователя (клиента HTTP) можно подключить к IP-адресу коммутатора через другие устройства, например, через маршрутизатор.

Подобно управлению по Telnet, как только с хоста будет успешно проходить команда ping до IP-адреса коммутатора, введя правильное имя и пароль можно получить доступ к Web-интерфейсу коммутатора. Процедура конфигурирования следующая:

Шаг 1: Настройте IP-адреса коммутатора и запустите на нём функцию HTTP-сервера.

О настройке IP-адреса коммутатора с помощью внеполосного управления см. п. 1.1.2.1.

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: Запустите протокол Web-браузер на хосте.

Откройте на хосте Web-браузер и введите IP-адрес коммутатора, либо запустите HTTP-протокол непосредственно из Windows. Пусть, например, IP-адрес коммутатора 192.168.0.10.

Шаг 3: Регистрация на коммутаторе

Зарегистрируйтесь в Web-интерфейсе конфигурирования. Для доступа к Web-интерфейсу коммутатора необходимо ввести имя пользователя и пароль, в противном случае в доступе будет отказано. Это сделано для защиты коммутатора от попыток несанкционированного доступа. Поэтому, когда Telnet доступен для конфигурирования коммутатора и управления им, необходимо с помощью команды, приведенной ниже, задать имя и пароль для авторизованных пользователей Telnet: **username** <username> **privilege** <privilege> [**password** (**0**|**7**) <**password**>]. Для локальной аутентификации можно использовать следующую команду: **authentication line vty login local**. Для доступа в привелигерованный режим необходимо и задан уровень привилегий 15.Допустим, авторизованный пользователь имеет имя “admin” и пароль “admin”, тогда процедура настройки следующая:

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

Окно для входа в Web-интерфейс коммутатора ZES показано на Рис. 7:

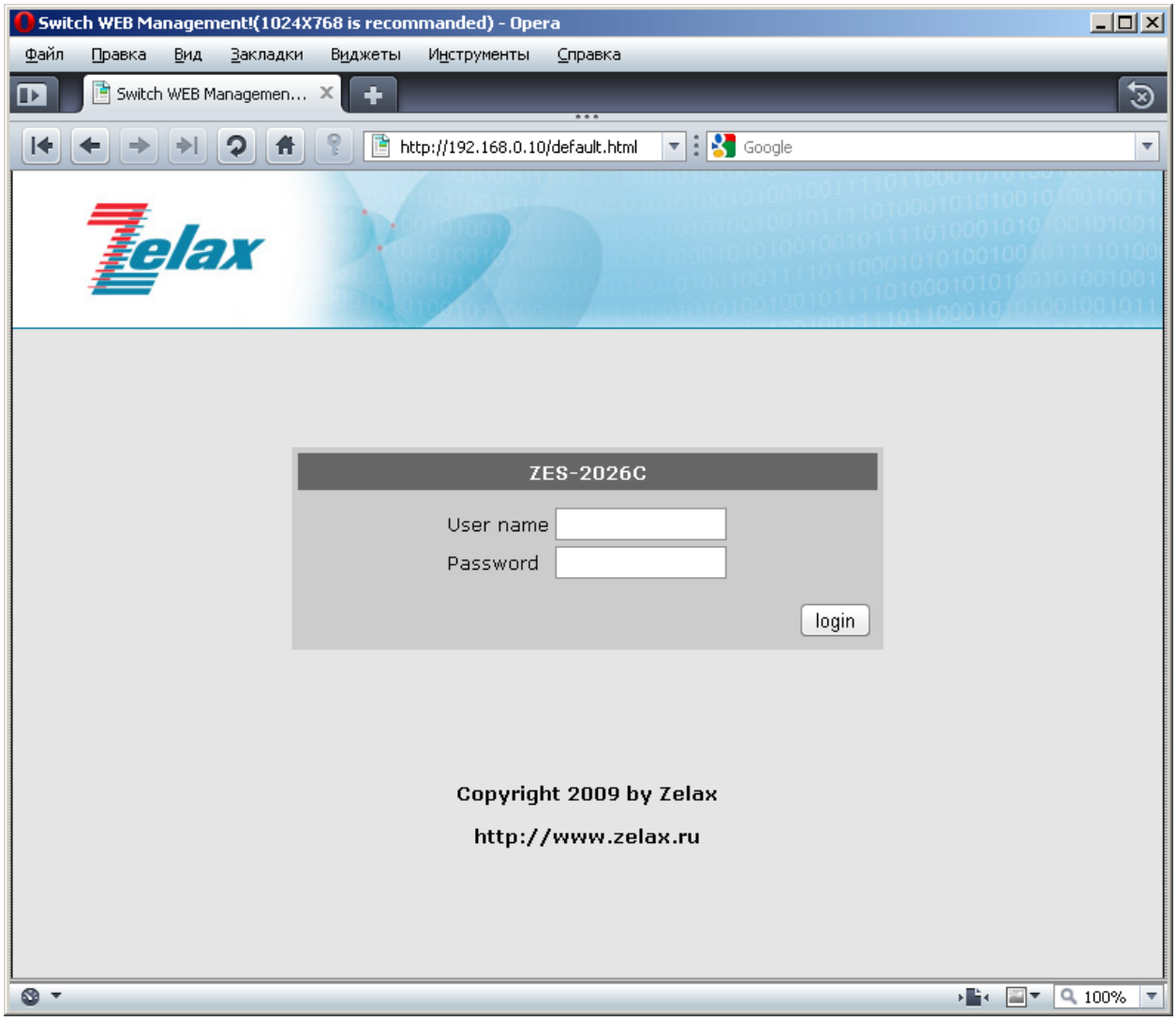

Рис. 7. Окно для входа в Web-интерфейс

Окно входа в Web-интерфейс. Введите имя и пароль, откроется окно Web-интерфейса для настройки коммутатора (см. Рис. 8).

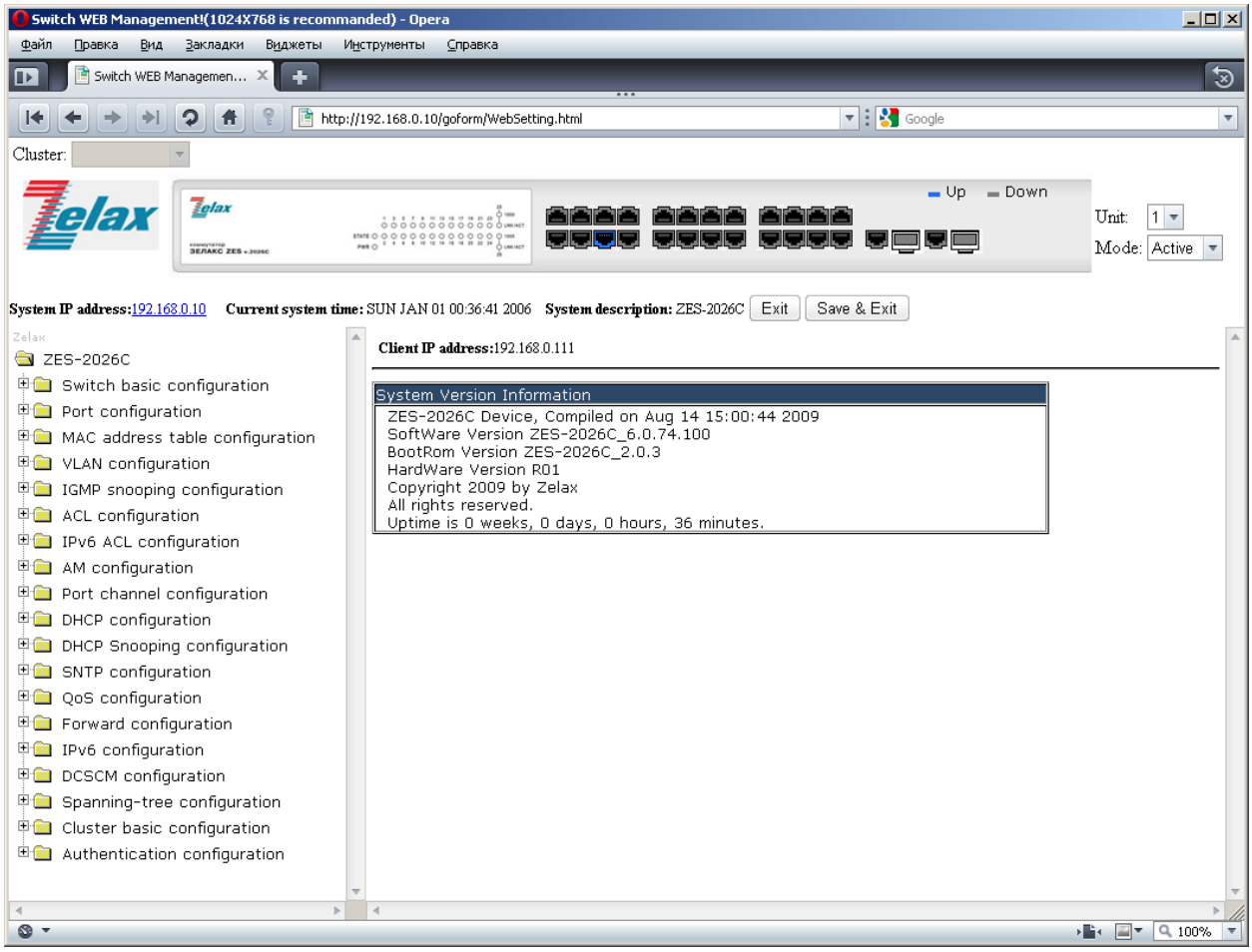

Рис. 8. Главное окно Web-интерфейса настройки коммутатора

1.1.2.3 Управление коммутатором с помощью по протоколу SNMP

Для управления коммутатором по протоколу SNMP должны выполняться следующие условия:

1. Настроен IP-адреса коммутатора;
2. IP-адреса хоста (с SNMP-менеджером) и интерфейса VLAN коммутатора должны находиться в одном и том же сегменте сети;
3. Если условие 2 не выполнено, клиент можно подключить к IP-адресу коммутатора через другие устройства, например, через маршрутизатор;
4. Должен быть включен протокол SNMP.

1.2 Интерфейс командной строки (CLI)

Интерфейс CLI уже знаком большинству пользователей. Как отмечалось выше, внеполосное управление и регистрация по Telnet для управления коммутатором выполняется посредством CLI.

Для управления коммутатором с помощью CLI имеется набор команд. Для управления и настройки коммутатора эти команды объединены в категории в соответствии с выполняемыми функциями. Каждой категории соответствует свой режим конфигурирования. Ниже рассмотрены команды для коммутатора:

- Режимы конфигурирования
- Синтаксис команд
- «Горячие» клавиши
- Контекстная справка
- Проверка вводимых команд
- Поддержка доопределения команд

1.2.1 Режимы конфигурирования

На Рис. 9 приведены режимы конфигурации коммутатора.

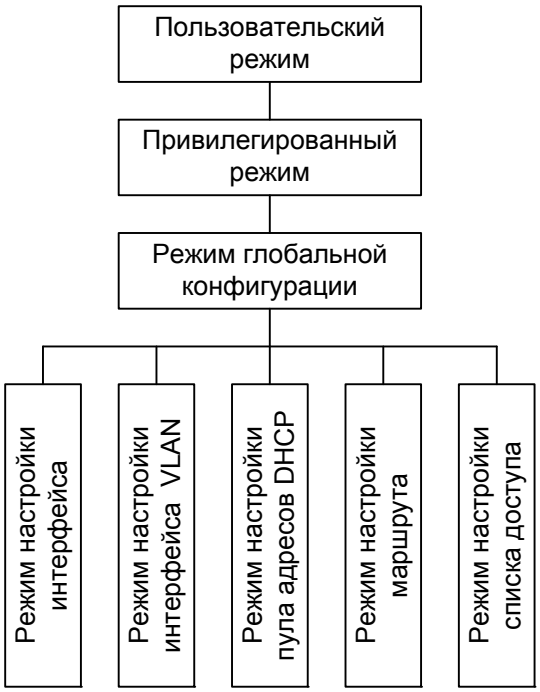

Рис. 9. Режимы конфигурирования коммутатора

1.2.1.1 Пользовательский режим

При вызове интерфейса CLI сначала вызывается система регистрации пользователя. По умолчанию включен пользовательский режим. На экране появляется приглашение “Switch>“, символ “>“ указывает, что включен пользовательский режим. Если в привилегированном режиме ввести команду **exit** (выход), то выход произойдет также в пользовательский режим.

В пользовательском режиме конфигурирование коммутатора запрещено, по запросам выдается только информация о времени и версии коммутатора.

1.2.1.2 Привилегированный режим

Приглашение в привилегированном режиме имеет вид “Switch#”. В привилегированный режим можно войти из пользовательского режима, введя команду **enable**, а затем — имя и пароль администратора. Если в глобальном режиме конфигурирования (Global Mode) ввести команду **exit** (выход), то выход произойдет также в привилегированный режим. Для коммутатора также работает клавиатурная команда "Ctrl+z” — она выполняет выход из любого режима (кроме пользовательского) в привилегированный режим.

В привилегированном режиме пользователь может запрашивать информацию о конфигурировании коммутатора, статусе соединения и статистике трафика для всех портов; находясь в привилегированном режиме, пользователь может входить в глобальный режим конфигурирования и изменять всё конфигурирование коммутатора. По этой причине для входа в привилегированный режим должен быть установлен пароль, предотвращающий несанкционированный доступ.

1.2.1.3 Глобальный режим конфигурирования

При вводе в привилегированном режиме команды config произойдет переключение в глобальный режим конфигурирования, появится приглашение “Switch(Config)#” при использовании команды **exit** в других режимах конфигурирования (интерфейсный режим, режим VLAN), произойдет возврат в глобальный режим конфигурирования.

В глобальном режиме конфигурирования пользователь может вводить настройки, например, задавать таблицу MAC-адресов, зеркалирование портов, создавать VLAN, запускать IGMP Snooping, GVRP, STP и т. п.

Затем пользователь может, например, включить режим настройки интерфейсов.

1.2.1.4 Режим настройки интерфейсов

Для входа в режим настройки интерфейсов: в глобальном режиме конфигурирования введите команду interface. Коммутатор поддерживает три типа интерфейса:

1. Интерфейс VLAN;
2. Интерфейс Ethernet;
3. Интерфейс port-channel.

Соответственно имеются три режима конфигурирования интерфейсов.

Тип интерфейса	Вводимая команда	Выполняемые операции	Выход
VLAN	В глобальном режиме конфигурирования введите команду **interface vlan** <vlan-id>	Настройка IP-адресов коммутатора и т. д.	Для возврата в глобальный режим конфигурирования введите команду exit
Ethernet	В глобальном режиме конфигурирования введите команду **interface ethernet** <interface-list>	Настройка поддержки режима дуплекса, скорости Ethernet-порта и т. д.	Для возврата в глобальный режим конфигурирования введите команду exit
port-channel	В глобальном режиме конфигурирования введите команду **interface port-channel** <port-channel-number>	Конфигурирование интерфейса port-channel, задание таких настроек как режим дуплекса, скорость и т. д.	Для возврата в глобальный режим конфигурирования введите команду exit

1.2.1.5 Режим настройки интерфейсов VLAN

При вводе в глобальном режиме конфигурирования команды **vlan** <vlan-id> , будет включен режим настройки интерфейсов VLAN для соответствующей VLAN. В режиме настройки интерфейсов VLAN пользователь может сконфигурировать все порты членов соответствующей VLAN. Для выхода из режима настройки интерфейсов VLAN в глобальный режим конфигурирования, введите команду **exit**.

1.2.1.6 Режим настройки пула адресов DHCP

При вводе в глобальном режиме конфигурирования команды **ip dhcp pool** <name> будет включен режим настройки пула адресов DHCP, появится приглашение этого режима "**Switch(Config**-<name>-**dhcp**)#" В режиме настройки пула адресов DHCP можно сконфигурировать свойства пула адресов DHCP. Для выхода из режима настройки пула адресов DHCP в глобальный режим конфигурирования введите команду **exit**.

1.2.1.7 Режим настройки списков доступа ACL

Тип ACL	Вводимая команда	Выполняемые операции	Выход
Режим стандартного ACL	В глобальном режиме конфигурирования введите **команду ip access-list standard**	Конфигурирование параметров для стандартного ACL	Для возврата в глобальный режим конфигурирования введите команду **exit**
Режим расширенного ACL IP	В глобальном режиме конфигурирования введите команду **ip access-list extanded**	Конфигурирование параметров для расширенного ACL	Для возврата в глобальный режим конфигурирования введите команду **exit**

1.2.2 Синтаксис команд

Коммутатор поддерживает различные команды конфигурирования. Хотя все команды разные, все они поддерживают синтаксис команд конфигурирования коммутатора. Общий формат команд коммутатора приведен ниже:

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

cmdtxt — строго заданная последовательность символов, определяющая дальнейшие параметры.

<**variable**> — обозначает переменный параметр;

{**enum1** | … | **enumN**} —обозначает штатный параметр, значения которого лежат в пределах **enum1** — **enumN**;

квадратные скобки ([ ]) в [**option**] обозначают опцию — дополнительный параметр. В командной строке могут присутствовать и комбинации этих обозначений, например “< >“, “{ }” и “[ ]”. Пример комбинации [<**variable**>] , {**enum1** <**variable**>| **enum2**}, [**option1** [**option2**]], и т. п.

Ниже приведены примеры некоторых актуальных команд конфигурирования:

show version, параметры не требуются. Эта команда состоит из одного ключевого слова и не имеет параметров. Для ее выполнения просто введите ее.

vlan <vlan-id>, после ключевого слова должны быть заданы значения параметра.

firewall {**enable** | **disable**}, позволяет включить или выключить межсетевой экран.

snmp-server community {**ro** | **rw**} <string>, возможны следующие варианты команды:

snmp-server community ro <string>

snmp-server community rw <string>

1.2.3 «Горячие» клавиши

Для обслуживания операций конфигурирования, выполняемых пользователем, коммутатор поддерживает несколько «горячих» клавиш (например, команды назначены на клавиши перемещения курсора (вверх, вниз, влево, вправо) и пробел. Если терминал не распознает клавиши Up (вверх) и Down (вниз), вместо них можно использовать сочетания клавиш ctrl+p и ctrl+n.

Клавиши	Функция	
Пробел	Удаляет символ перед курсором, курсор перемещается назад на одну позицию	
Up “↑”	Отображает предыдущую введенную команду. Может быть показано до 10 последних введенных команд	
Down “↓”	Отображает следующую введенную команду. Если клавиша Up уже использовалась для отображения ранее введенных команд, можно использовать клавишу Down для просмотра следующей команды	
Left “←”	Курсор перемещается на один символ влево	Клавиши Left и Right можно использовать для редактирования команды на экране
Right “→”	Курсор перемещается на один символ вправо	
Ctrl+p	Выполняет те же функции, что и клавиша Up “↑”	
Ctrl+n	Выполняет те же функции, что и клавиша Down “↓”	
Ctrl+b	Выполняет те же функции, что и клавиша Left “←”	
Ctrl+f	Выполняет те же функции, что и клавиша Right “→”	

Ctrl +z	Выход в привилегированный режим из других режимов конфигурирования (за исключением пользовательского)
Ctrl +c	Прерывание процесса выполнения команды, например, прерывание ping или другой команды
Клавиша табуляции (Tab)	Если введена строка команды или ее ключевого слова, клавишу Tab можно использовать для дополнения этой команды или ее ключевого слова до полной формы (если это не приводит к конфликту имен)

1.2.4 Контекстная справка

Пользователь может получить доступ к справочной информации по командам коммутатора двумя способами: введя команду “help” или нажав клавишу “?”.

Доступ к справке	Использование и способ ввода
Команда Help	В любом месте командной строки введите “help” и нажмите Enter. Коммутатор выведет краткое описание команды
“?”	1. В любом месте командной строки введите “?”. Будет выведен список команд текущего режима и краткое их описание. 2. Введите “?” после ключевого слова команды (через пробел). Если в этой позиции должен быть параметр, будет выведено описание типа параметра, области его применения и т. п. Если в этой позиции должно быть ключевое слово, будет выведен набор ключевых слов и краткое описание этих команд. Если ответом на ввод является “<cr>“, команда имеет полную форму — нажмите Enter и введите команду. 3. Знак “?” введен сразу после строки (без пробела) Будут отображены все команды, начинающиеся с этой строки

1.2.5 Проверка вводимых команд

1.2.5.1 Ответ системы: success (выполнена успешно)

Все введенные с клавиатуры команды проходят проверку на правильность синтаксиса. Если пользователь ввел команду правильно, в соответствующем режиме и она успешно выполнена, то никакого ответа системы не последует. Ответ системы: error (ошибка)

Сообщение об ошибке, отображаемое на экране	Описание
Unrecognized command or illegal parameter!	Введенная команда не существует, либо ошибка в области значений параметра, его формате или типе
Ambiguous command	Возможны не менее двух интерпретаций введенной команды
Invalid command or parameter	Команда распознана, однако не найдено правильной записи параметра
This command is not exist in current mode	Команда распознана, однако такая команда не может использоваться в текущем режиме
Please configure precursor command "*" at first !	Команда распознана, однако предварительные условия, необходимые для выполнения этой команды еще не созданы
syntax error: missing "" before the end of command line!	Знаки двойных кавычек не образуют пару

1.2.6 Поддержка доопределения команд

Программное обеспечение коммутатора поддерживает доопределение вводимых команд. ПО будет распознавать введенные команды и ключевые слова правильно, даже если команды введены не полностью, но введенная строка однозначно интерпретируется. Например:

Для команды “show interfaces status ethernet0/0/1” можно ввести “sh in status ethernet0/0/1” и команда будет правильно распознана.

1. Однако, если ввести “sh r” для команды “show running-config”, система выдаст сообщение об ошибке “> Ambiguous command!” (Нераспознанная команда!), так как ПО неспособно распознать команду. Под командой “show r” могут подразумеваться команды “show run” и “show running-config”. Поэтому ПО распознает команду только в том случае, если введена команда “sh ru”.

2 Основная настройка коммутатора

2.1 Команды основной настройки коммутатора

Командами основной настройки коммутатора являются следующие: команды входа в привилегированный режим и выхода из него, команды входа в режим настройки интерфейсов и выхода из него, команды настройки и отображения даты и времени коммутатора, команды для просмотра версии программного обеспечения коммутатора и т. п.

Команда	**Описание**
Пользовательский режим или привилегированный режим	
enable disable	Команда **enable** используется для входа в привилегированный режим (из пользовательского режима). Команда **disable** используется для выхода из привилегированного режима
Привилегированный режим	
config [terminal]	Используется для входа в глобальный режим конфигурирования (из привилегированного режима)
Разные режимы	
exit	Используется для выхода из текущего режима в предыдущий режим. Например, ввод этой команды в глобальном режиме конфигурирования приведет к возврату в привилегированный режим. Ввод этой команды в привилегированном режиме конфигурирования приведет к возврату в пользовательский режим
Привилегированный режим	
clock set <HH:MM:SS> [YYYY.MM.DD]	Используется для установки даты и времени
show version	Используется для отображения информации о версии ПО коммутатора
set default	Используется для восстановления заводских настроек
write	Используется для сохранения текущих значений параметров настройки во флэш-памяти
reload	Перезагрузка коммутатора

2.2 Управление по Telnet

2.2.1 Протокол Telnet

2.2.1.1 Начальные сведения о Telnet

Telnet — это протокол простого терминального удаленного доступа. Используя Telnet, пользователь может зарегистрироваться со своей рабочей станции на удаленном хосте с определенным IP-адресом и именем хоста. По Telnet пользователь может посылать коды нажимаемых клавиш клавиатуры на удаленный хост и по TCP-соединению получать ответы хоста, которые отображаются на дисплее рабочей станции пользователя. Это служба с прозрачным интерфейсом — у пользователя создается полное ощущение, что его клавиатура и монитор подключены напрямую к удаленному хосту.

В протоколе Telnet используется режим Клиент-Сервер; локальная система является Telnet-клиентом, а удаленный хост — Telnet-сервером. Коммутатор может функционировать либо как Telnet-сервер, либо как Telnet-клиент.

Если коммутатор используется в качестве Telnet-сервера, пользователь для регистрации на коммутаторе может использовать программу Telnet-клиента, входящую в комплект программ Windows, либо другой операционной системы (см. раздел, посвященный внутриполосному управлению). Когда коммутатор используется в качестве Telnet-сервера, он поддерживает до 5 Telnet-клиентов, использующих TCP-соединения.

Когда коммутатор работает как Telnet-клиент, используя команду **telnet** в привилегированном режиме, пользователь может регистрироваться на других удаленных хостах. Коммутатор может устанавливать TCP-соединение только с одним удаленным хостом. Если

требуется соединение с другим удаленным хостом, текущее TCP-соединение должно быть закрыто.

2.2.1.2 Список команд для настройки Telnet

1. Настройка Telnet-сервера
2. Доступ к коммутатору по Telnet с удаленного хоста.

Настройка Telnet-сервера

Команда	Описание
Глобальный режим конфигурирования	
telnet-server enable **no telnet-server enable**	Включает функцию Telnet-сервера на коммутаторе: Отмена команды: “**no telnet-server enable**” выключает функцию Telnet-сервера
username <username> [**privilege** <privilege>] [**password** {**0** | **7**} <password>] **no username** <username>	Задает имя пользователя и пароль для регистрации на коммутаторе по Telnet. Отмена команды: **no username** <username> отключает пользователя, подключенного по Telnet с определенным именем и паролем
authentication securityip <ip-addr> **no authentication securityip** <ip-addr>	Задает безопасный IP-адрес для регистрации на коммутаторе по Telnet: Отмена команды “**no authentication securityip** <ip-addr>“ удаляет авторизованный безопасный адрес Telnet
authentication securityipv6 <ipv6-addr> **no authentication securityipv6** <ipv6-addr>	Задает безопасный IPv6-адрес для регистрации на коммутаторе по Telnet. Отмена команды: “**no authentication securityipv6** <ipv6-addr>“ удаляет авторизованный безопасный адрес Telnet
authentication line {**console** | **vty** | **web**} **login** {**local** | **radius** | **tacacs**} **no authentication line** {**console** | **vty** | **web**} **login**	Позволяет настроить режим аутентификации telnet
Admin Mode	
terminal monitor terminal no monitor	Отображает отладочную информацию для Telnet-клиента, зарегистрированного на коммутаторе. Отмена команды: “**no monitor**” отключает вывод отладочной информации

Доступ к коммутатору по Telnet с удаленного хоста:

Команда	Описание
Привилегированный режим	
telnet {<ip-addr>| <ipv6-addr> <hostname>} [<port>]	Регистрация с удаленного хоста с помощью Telnet-клиента, имеющегося на коммутаторе

2.2.2 SSH

2.2.2.1 Начальные сведения о SSH

SSH (Secure Shell) — это протокол, гарантирующий безопасное удаленное соединение с сетевыми устройствами. Безопасное соединение между SSH-сервером и SSH-клиентом устанавливается с использованием механизма распределения ключей, аутентификации и шифрования. Информация, передаваемая по этому соединению, защищена от перехвата и дешифрирования. Коммутатор удовлетворяет требованиям SSH2.0. Он поддерживает клиентское программное обеспечение SSH2.0, например, SSH Secure Client и PuTTY. Пользователи могут запускать это программное обеспечение для удаленного управления коммутатором.

В настоящее время коммутатор поддерживает аутентификацию RSA, криптографический протокол 3DES, аутентификацию паролей SSH и т. д.

2.2.2.2 Типовая настройка сервера SSH

Настройка сервера SSH:

Команда	Описание
Глобальный режим конфигурирования	
ssh-server enable **no ssh-server enable**	Включает функцию SSH коммутатора; команда “**no ssh-server enable**” выключает функцию SSH
ssh-user <user-name> **password** {**0** | **7**} <password> **no ssh-user** <user-name>	Задает имя пользователя и пароль клиентского программного обеспечения SSH для регистрации на коммутаторе. Отмена команды “**no ssh-user** <user-name>“ удаляет имя пользователя
ssh-server timeout <timeout> **no ssh-server timeout**	Позволяет задать время таймера аутентификации SSH. Отмена команды: “**no ssh-server timeout**” восстанавливает время таймера аутентификации SSH, используемое по умолчанию
ssh-server authentication-retires <authentication-retires> **no ssh-server authentication-retries**	Задает число попыток аутентификации SSH; Отмена команды “**no ssh-server authentication-retries**” восстанавливает число попыток аутентификации SSH, используемое по умолчанию
ssh-server host-key create rsa modulus <moduls>	Генерирует новый ключ хоста RSA на сервере SSH
Привилегированный режим	
terminal monitor terminal no monitor **no terminal monitor**	Отображает отладочную информацию SSH на стороне SSH-клиента. Отмена команды: “**no terminal monitor**” прекращает отображение отладочной информации SSH на стороне SSH-клиента

Пример 1:

Требуется: Включить на коммутаторе SSH-сервер, на терминале — запустить клиентское программное обеспечение SSH2.0: Secure shell или PuTTY. Зарегистрируйтесь на коммутаторе, используя клиентское имя пользователя и пароль.

Сконфигурируйте IP-адрес, добавьте пользователя SSH и включите услуги SSH на коммутаторе. Клиент SSH2.0 может зарегистрироваться на коммутаторе, используя имя пользователя и пароль и затем сконфигурировать коммутатор.

```
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)#ssh-user test password 0 test
```

В сетях IPv6 на терминале должно функционировать клиентское ПО SSH, поддерживающее IPv6, например putty6. Пользователи не должны изменять настройки коммутатора за исключением IPv6-адреса, выделенного локальному хосту.

2.3 Настройка IP-адресов коммутатора

По умолчанию все Ethernet-порты коммутатора являются портами уровня линий передачи данных и поддерживают передачу пакетов уровня 2. Интерфейс VLAN — это интерфейсная функция уровня 3, с помощью нее можно присвоить IP-адрес, который будет также и IP-адресом коммутатора. Все команды настройки интерфейса VLAN могут использоваться в режиме настройки интерфейсов VLAN. Коммутатор поддерживает три метода конфигурирования IP-адресов:

- Вручную
- В режиме загрузки (BOOTP)
- По DHCP

При конфигурировании вручную IP-адрес присваивается коммутатору вручную.

В режимах BootP и DHCP, коммутатор функционирует, как BootP/DHCP-клиент и посылает широковещательные пакеты с запросами BootPRequest на серверы BootP или DHCP, которые присваивают адреса на основе принятых запросов. Кроме того, коммутатор может функционировать как DHCP-сервер, динамически распределяя сетевые параметры: IP-адреса, адреса шлюзов, адреса DNS-сервера для DHCP-клиентов. Конфигурирование сервера DHCP детально рассмотрено в последующих главах.

2.3.1 Список команд для настройки IP-адресов коммутатора

1. Включение режима настройки интерфейсов VLAN
2. Настройка вручную
3. Настройка с использованием BootP
4. Настройка с использованием DHCP

1. Включение режима настройки интерфейсов VLAN:

Команда	Описание
Глобальный режим конфигурирования	
interface vlan <vlan-id> **no interface vlan** <vlan-id>	Позволяет создать интерфейс VLAN (интерфейс 3-го уровня). Отмена команды: “**no interface vlan** <vlan-id>” удаляет указанный интерфейс VLAN

2. Настройка вручную:

Команда	Описание
Режим настройки портов VLAN	
ip address <ip-address> <mask> [secondary] **no ip address** <ip-address> <mask> [secondary]	Позволяет настроить IP-адрес интерфейса VLAN; Отмена команды “**no ip address** <ip_address> <mask> [secondary]” удаляет IP-адрес интерфейса VLAN
ipv6 address <ipv6-address / prefix-length> [eui-64] **no ipv6 address** <ipv6-address / prefix-length>	Позволяет задать IPv6–адрес, в том числе глобальный адрес агрегации одноадресного трафика, адрес локального сайта и адрес локальной линии. Отмена команды: удаляет IPv6–адрес

3. Настройка с использованием BootP:

Команда	Описание
Режим настройки портов VLAN	
ip bootp-client enable **no ip bootp-client enable**	Включает коммутатор, как BootP-клиент, при этом получение IP-адреса и адреса шлюза выполняется через механизм переговоров BootP. Отмена команды: “**no ip bootp-client enable**” выключает функцию BootP-клиента

4. Настройка с использованием DHCP:

Команда	Описание
Режим настройки портов VLAN	
ip bootp-client enable **no ip bootp-client enable**	Включает коммутатор, как DHCP-клиент, при этом получение IP-адреса и адреса шлюза выполняется через механизм переговоров DHCP. Отмена команды “**no ip dhcp-client enable**” выключает функцию DHCP-клиента

2.4 Настройка SNMP

2.4.1 Начальные сведения о SNMP

Протокол SNMP (Simple Network Management Protocol) является простым протоколом управления сетью, он широко используется для управления компьютерными сетями. SNMP — это развивающийся протокол.

Первой версией SNMP была версия SNMP v1 [RFC1157], она нашла применение у множества производителей, выбравших этот протокол из-за его простоты и легкости реализации. SNMP v2c — улучшенная версия SNMP v1, она поддерживает управление сетью на разных уровнях; в версии SNMP v3 улучшена безопасность за счет добавления режима USM (User-based Security Mode) и модели управления доступом VACM (View-based Access Control Model).

Протокол SNMP обеспечивает простой способ обмена сетевой управляющей информацией между двумя точками сети. При SNMP применяется механизм опроса очереди сообщений и передача сообщений по протоколу UDP (протокол транспортного уровня, не требующий установления соединения). Поэтому он хорошо поддерживается существующими компьютерными сетями.

При протоколе SNMP применяется режим станции-агента. В этой структуре имеется две части: NMS (Network Management Station — Станция управления сетью) и Агент. NMS — это

рабочая станция, на которой функционирует программа-клиент SNMP. Для управления сетью она является ядром. Агент — это серверное программное обеспечение, функционирующее на устройствах, которыми требуется управлять. NMS управляет всеми объектами управления через Агентов. Коммутатор поддерживает функции Агента.

Связь между NMS и Агентом осуществляется в режиме Клиент/Сервер путем обмена стандартными сообщениями. NMS посылает запрос, а Агент отвечает на него. Существует семь типов сообщений SNMP:

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

NMS посылает запросы Агенту при помощи сообщений Get-Request, Get-Next-Request, Get-Bulk-Request и Set-Request. Агент, приняв эти запросы отвечает на них сообщением Get-Response. В некоторых специальных ситуациях, например, когда порты сетевых устройств находятся в состоянии включения или выключения (Up/Down), либо при изменении топологии сети, Агенты могут посылать на NMS сообщения Trap, чтобы информировать ее о нештатных событиях. Кроме того, на NMS может быть задан режим оповещения о нештатных событиях путем включения функции RMON. При наступлении нештатного события Агенты будут посылать сообщения Trap, либо создавать отчет о событии (в зависимости от настроек). Для связи между NMS при многоуровневом управлении сетью в основном используются сообщения Inform-Request.

Режим USM гарантирует безопасную передачу за счет применения эффективного алгоритма шифрования и аутентификации. В режиме USM осуществляется шифрование сообщений в соответствии с паролем, введенным пользователем. Этот механизм гарантирует невозможность просмотра сообщения в процессе передачи. Аутентификация в режиме USM гарантирует невозможность изменения сообщения в процессе передачи. В режиме USM применяется криптозащита DES-CBC. При аутентификации используются алгоритмы шифрования HMAC-MD5 и HMAC-SHA.

Для классификации прав доступа пользователей используется модель VACM. В соответствии с этой моделью пользователи с одинаковыми правами доступа объединяются в одну группу. Пользователи не могут выполнять операции, которые им не разрешены.

2.4.2 Начальные сведения о MIB

Информация управления сетью, становящаяся доступной от NMS структурируется и организуется в базе данных управляющей информации (MIB — Management Information Base). В MIB определена информация, которая может быть доступна протоколам управления сетью. Информация классифицирована по уровням и структурам. Предопределенная управляющая информация может быть получена из мониторинга сетевых устройств. В стандарте ISO ASN.1 (Abstract Syntax Notation One) для MIB определена древовидная структура. Каждая MIB организует всю доступную информацию в этой древовидной структуре. Каждый узел дерева имеет OID (Object Identifier — идентификатор объекта) и краткое описание узла. OID представляет собой набор целых чисел, разделенных точками. Он определяет узел и может использоваться для поиска узла в древовидной структуре MIB (см. Рис. 10).

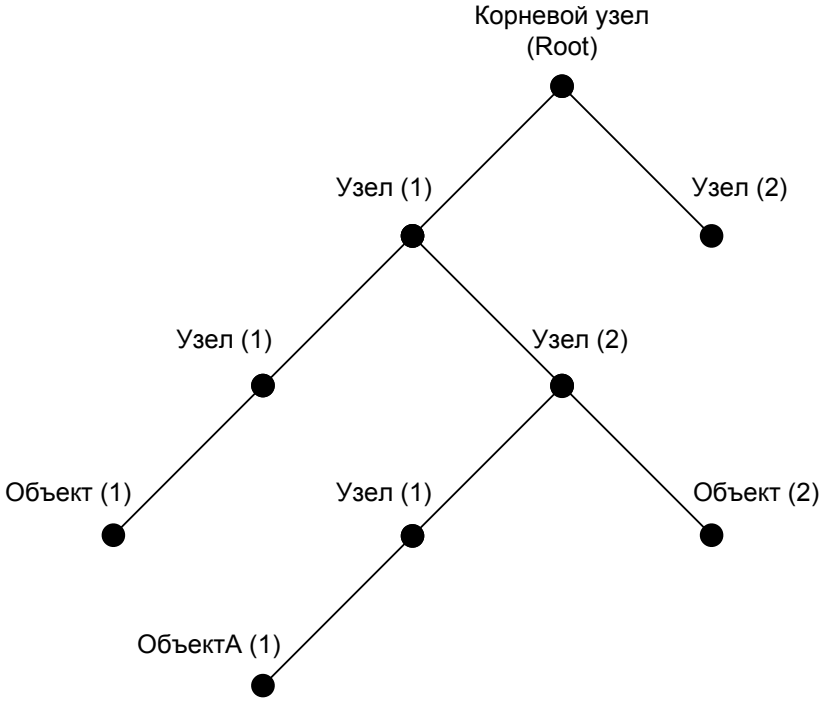

Рис. 10. Дерево объектов ASN.1.

На этом рисунке OID объекта A является 1.2.1.1. NMS может отыскать этот объект по его уникальному OID и получить стандартные переменные объекта. MIB определяет набор стандартных переменных для контролируемых сетевых устройств следуя этой структуре.

Если необходим просмотр информации переменных Агента MIB, в NMS должно функционировать программное обеспечение просмотра MIB. MIB в Агенте обычно состоит из общедоступной MIB и частной MIB. Общедоступная MIB обычно содержит общедоступную управляющую информацию сети, доступную всем NMS. Частная MIB содержит специальную информацию, которая может просматриваться и контролироваться изготовителями.

MIB-I [RFC1156] была первой реализацией общедоступной MIB протокола SNMP, впоследствии она была заменена на MIB-II [RFC1213]. MIB-II является расширением MIB-I, поддерживает OID дерева MIB в MIB-I. MIB-II поддерживает суб-деревья, называемые группами. Объекты в этих группах охватывают все области функционала сетевого управления. NMS получает управляющую информацию сети, посещая MIB Агента SNMP.

Коммутатор может функционировать, как Агент SNMP и поддерживать как SNMP v1/v2c, так и SNMP v3. Коммутатор поддерживает базовую MIB-II, RMON общедоступной MIB и другие общедоступные MIB, такие как BRIDGE MIB. Кроме того, коммутатор поддерживает частные MIB, созданные путем самоопределения.

2.4.3 Начальные сведения о RMON

RMON — это наиболее важное расширение стандарта SNMP. RMON — это набор определений MIB, используемый для определения стандартных функций мониторинга сети и интерфейсов. Он делает возможной связь между терминалами управления SNMP и удаленными мониторами. RMON обеспечивает высокоэффективный метод мониторинга операций, выполняемых в подсетях.

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

Statistics: Обслуживает статистики использования и ошибок для каждой подсети, контролируемой Агентом.

Alarm: Позволяет пользователям задать с консоли любой счетчик или целое число для интервалов выборки и порогов сигнализации при сохранениях RMON, выполняемых Агентом.

Event: Список всех событий, генерируемых Агентом RMON.

Сигнализация определяется конкретным событием. Statistics и History обеспечивают вывод на дисплей текущей статистики подсети и истории статистики подсети. Alarm и Event обеспечивают метод мониторинга изменений любых целых данных в сети и сигнализацию о

некоторых нештатных событиях (посылают сообщение Trap (Особая ситуация) или создают запись в отчетах).

2.4.4 Настройка SNMP

2.4.4.1 Последовательность настройки SNMP

1. Включить или выключить SNMP-агент
2. Настроить SNMP-community
3. Установить IP-адрес станции управления SNMP
4. Задать ID вычислительной подсистемы коммутатора
5. Сконфигурировать пользователя
6. Сконфигурировать группу
7. Сконфигурировать вид сводной информации о коммутаторе
8. Сконфигурировать TRAP
9. Включить или выключить RMON

1. Включить или выключить SNMP-агент

Команда	Описание
Глобальный режим конфигурирования	
snmp-server enabled **no snmp-server enabled**	Включает функцию Агента SNMP на коммутаторе. Отмена команды “**no snmp-server enabled**” выключает функцию Агента SNMP на коммутаторе

2. Настроить SNMP community

Команда	Описание
Глобальный режим конфигурирования	
snmp-server community {ro|rw} <string> **no snmp-server community** <string>	Позволяет настроить строку community для коммутатора. Команда “**no snmp-server community** <string>“ удаляет настроенную строку community

3. Установить IP-адрес станции управления SNMP

Команда	Описание
Глобальный режим конфигурирования	
snmp-server securityip <ip-addr> **no snmp-server securityip** <ip-addr>	Позволяет задать безопасный адрес IPv4/IPv6, разрешающий доступ к коммутатору по NMS. Отмена команды: “**no snmp-server securityip** <ip-addr> “удаляет настроенный безопасный адрес
snmp-server securityip enable **snmp-server securityip disable**	Включает или выключает функцию проверки безопасного IP-адреса на NMS

4. Задать ID вычислительной подсистемы коммутатора

Команда	Описание
Глобальный режим конфигурирования	
snmp-server engineid <engine-string> **no snmp-server engineid**	Позволяет задать ID локальной вычислительной подсистемы коммутатора. Эта команда используется при SNMP v3

5. Сконфигурировать пользователя

Команда	Описание
Глобальный режим конфигурирования	
snmp-server user <use-string> <group-string> {encrypted | noencrypted} **auth** {md5 | sha} <word> **no snmp-server user** <user-string>	Добавляет пользователя в группу SNMP. Эта команда используется для конфигурирования USM при SNMP v3

6. Сконфигурировать группу

Команда	Описание
Глобальный режим конфигурирования	
snmp-server group <group-string> {noauthnopriv|authnopriv|authpriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]] **no snmp-server group** <group-string> {noauthnopriv|authnopriv|authpriv}	Задает на коммутаторе информацию о группе. Эта команда используется для конфигурирования VACM при SNMP v3

7. Сконфигурировать вид сводной информации о коммутаторе

Команда	Описание
Глобальный режим конфигурирования	
snmp-server view <view-string> <oid-string> {include|exclude} **no snmp-server view** <view-string>[<oid-string>]	Конфигурирует вид сводной информации коммутатора. Эта команда используется при SNMP v3

8. Сконфигурировать TRAP

Команда	Описание
Глобальный режим конфигурирования	
snmp-server enable traps **no snmp-server enable traps**	Включает на коммутаторе отправку сообщения Trap. Эта команда используется при 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-addr> } {v1 | v2c | {v3 {Noauthnopriv | Authnopriv | Authpriv}}} <user-string>	Задает адрес IPv4/IPv6 для хоста, который используется для приема информации SNMP Trap. При SNMP v1/v2 эта команда, кроме того, конфигурирует строку Trap community; при SNMP v3 эта команда также конфигурирует имя пользователя Trap и уровень безопасности. Отмена команды (с no): отменяет этот IPv4- или IPv6-адрес

9. Включить или выключить RMON

Команда	Описание
Глобальный режим конфигурирования	
rmon enable **no rmon enable**	Включает или выключает RMON

2.4.5 Примеры типового конфигурирования SNMP

IP-адрес NMS — 1.1.1.5; IP-адрес коммутатора (Агента) — 1.1.1.9

Пример 1: Для получения данных коммутатора используется SNMP-менеджер. Конфигурация коммутатора приведена 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
```

Для доступа к коммутатору по чтению/записи NMS может использовать строку community “private”, а для доступа к коммутатору только по чтению — строку community “public”.

Пример 2: NMS будет принимать сообщения Trap от коммутатора (NMS может осуществлять проверку строки community для сообщений Trap. В этом случае NMS использует проверку пользовательских сообщений Trap строки community Trap). Конфигурация коммутатора приведена ниже:

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

Пример 3: NMS использует протокол SNMP v3 для получения информации от коммутатора. Конфигурация коммутатора приведена ниже:

```
Switch(config)#snmp-server
Switch(config)#snmp-server user tester UserGroup encrypted auth md5 hellotst
```

```
Switch(config)#snmp-server group UserGroup AuthPriv read max write max notify max
Switch(config)#snmp-server view max 1 include
```

Пример 4: На NMS требуется принимать сообщения v3Trap, посылаемые коммутатором. Конфигурация коммутатора приведена ниже:

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

2.4.6 Устранение неполадок при SNMP

После того, как пользователи сконфигурируют SNMP, SNMP-сервер может давать сбои из-за отсутствия соединений, неправильной настройки т. д. Пользователи могут выявить причины возникших проблем, руководствуясь принципами, перечисленными ниже:

Необходимо обеспечить хорошее состояние физических соединений

Должны быть включены интерфейс и протокол канального уровня передачи данных (используйте команду “**show interface**”). Соединение между коммутатором и хостом можно проверить командой “**ping**”.

На коммутаторе должна быть активирована серверная функция Агента SNMP (используйте команду “**snmp-server**”)

Для NMS должны быть правильно сконфигурированы безопасный IP-адрес и строка community (используйте команду “**snmp-server community**”). Если какой-либо из этих параметров задан неправильно, SNMP не будет правильно связываться с NMS.

Если требуется функция Trap, не забудьте включить ее (командой “**snmp-server enable traps**”). Не забудьте, что необходимо правильно настроить IP-адрес станции мониторинга и строку community для Trap (командой “**snmp-server host**”), — только в этом случае сообщения Trap будут посылаться на станцию мониторинга.

Если требуется функция RMON, ее необходимо сначала включить (командой “**rmon enable**”).

Используйте команду “**show snmp**” для проверки посланных и принятых сообщений SNMP. Используйте команду “**show snmp status**” для проверки информации о конфигурации SNMP. Используйте команду “**debug snmp packet**” для включения функции отладки SNMP и проверки отладочной информации. Если пользователи не могут самостоятельно разрешить проблемы с SNMP, пожалуйста, обратитесь в службу технической поддержки.

2.5 Обновление программного обеспечения коммутатора

Коммутатор поддерживает два способа обновления ПО: Обновление BootROM и обновление по протоколу TFTP/FTP.

2.5.1 Системные файлы коммутатора

Системные файлы следующие: файл образа системы, загрузочный файл. Обновление ПО коммутатора состоит в обновлении этих двух файлов — замене старых версий на новые.

Файл образа системы — это сжатый файл для драйвера аппаратных средств коммутатора и программы поддержки программного обеспечения, обычно обозначается как файл обновления IMG. Файл IMG может быть сохранен только во флэш-памяти и с определенным именем: nos.img.

Файл загрузки — это файл, инициализирующий коммутатор, также называемый файлом обновления ROM (большой по размеру файл, который при сжатии дает файл IMG). Файл загрузки может быть сохранен только в ROM с именем boot.rom.

Метод обновления файла с образом системы и файла загрузки — один и тот же. Коммутатор поддерживает два режима обновления, выполняемого пользователем: 1. Режим обновления BootROM; 2. Обновление по TFTP и FTP с помощью ПО. Эти два метода обновления будут детально рассмотрены в последующих двух разделах.

2.5.2 Обновление BootROM

Существует два метода обновления BootROM: по протоколу TFTP или по протоколу FTP, соответствующий метод можно выбрать настройками команды BootROM. Типичная схема подключения оборудования при обновлении ПО коммутатора в режиме BootROM приведена на Рис. 11.

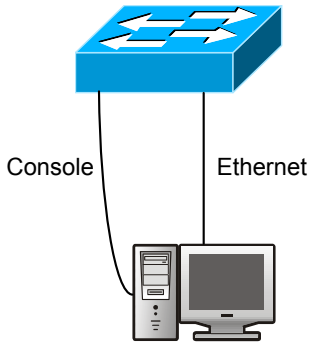

Рис. 11. Типичная схема подключения оборудования при обновлении ПО коммутатора в режиме BootROM

Процедура обновления описана ниже:

1. В качестве терминала для коммутатора используется ПК. Подключите ПК консольным кабелем к порту управления коммутатора. На ПК должно быть установлено программное обеспечение FTP/TFTP — сервера, должен иметься файл img, необходимый для обновления.
2. Во время загрузки коммутатора нажимайте на клавиатуре “ctrl+b” до тех пор, пока коммутатор не переключится в режим монитора BootROM. Информация на дисплее приведена ниже:

```
[Boot]:
```

3. В режиме BootROM введите команду “**setconfig**”, чтобы задать IP-адрес и маску коммутатора в режиме BootROM, IP-адрес и маску сервера. Выберите обновление по протоколу TFTP или по протоколу FTP. Предположим, адрес коммутатора — 192.168.1.2, а адрес ПК — 192.168.1.66, выбрано обновление по протоколу TFTP. Тогда на экране появится следующая информация конфигурирования:

```
[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]
```

4. Включите на ПК сервер FTP/TFTP. При TFTP запустите программу сервера TFTP, при FTP — программу сервера FTP. Перед началом загрузки файла обновления проверьте соединение между сервером и коммутатором, для этого выдайте с сервера команду ping. Если команда ping проходит, в режиме BootROM коммутатора введите команду “**load**”. Если эта команда не проходит, выполните процедуру поиска неполадок для выявления причин сбоя. Ниже приведена информация, появляющаяся на экране при обновлении системы с помощью файла образа.

```
[Boot]: load nos.img Loading...

Loading file ok!
```

5. В режиме BootROM введите команду “**write nos**.**img**”. На экране появится информация о сохранении файла образа.

```
[Boot]: write nos.imgWriting nos.img...Write nos.img OK.

[Boot]:
```

6. Выполните обновление файла boot.rom, используя такую же процедуру, что и в пункте 4.

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

7. В режиме BootROM введите команду “**write boot**.**rom**”. На экране появится информация о сохранении системой обновленного файла.

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

8. После успешно выполненного обновления, в режиме BootROM введите команду “**run**” для возврата в командный интерфейс конфигурирования CLI.

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

2.5.3 Обновление по протоколам FTP/TFTP

2.5.3.1 Начальные сведения о протоколах FTP/TFTP

Протоколы FTP (File Transfer Protocol) и TFTP (Trivial File Transfer Protocol) представляют собой протоколы передачи файлов, принадлежащие четвертому уровню стека протоколов TCP/IP (транспортный уровень). Они используются для передачи файлов между хостами, а также между хостами и коммутатором. При передаче файлов по обоим этим протоколам используется модель клиент-сервер. Различия между протоколами описаны ниже.

Протокол FTP использует TCP для обеспечения надежной, ориентированной на соединение, потоковой передачи данных. Однако он не обеспечивает авторизации доступа к файлу, использует простой механизм аутентификации (при аутентификации имя пользователя и пароль передаются в виде простого текста). При использовании FTP для передачи файлов, между клиентом и сервером необходимо установить два соединения: Соединение управления и соединение передачи данных. Для установления соединения управления, FTP-клиентом на порт 21 сервера должен быть передан запрос на передачу; по соединению управления будут проведены переговоры о соединении передачи данных.

Существует два типа соединений передачи данных: активное соединение и пассивное соединение.

При активном соединении, клиент передает свой адрес и номер порта для передачи данных на сервер, соединение управления поддерживается до тех пор, пока передача данных не будет завершена. Затем сервер, используя адрес и номер порта, предоставленные клиентом, устанавливает соединение передачи данных для порта 20 (если он ничем не занят) для передачи данных; если порт 20 занят, сервер автоматически генерирует другой номер порта для установления соединения передачи данных.

При пассивном соединении клиент по соединению управления уведомляет сервер об установлении пассивного соединения. После этого сервер создает свой собственный порт приема данных и информирует клиента об этом порте. Клиент устанавливает соединение передачи данных с указанным портом.

После того, как соединение передачи данных с указанным адресом и портом установлено, начинает действовать третья сторона, обеспечивающая работу службы передачи данных.

Протокол TFTP основан на протоколе UDP, при котором используется ненадежная потоковая передача данных без аутентификации пользователя и без авторизации для контроля прав доступа к файлу. Передача правильных данных гарантируется за счет механизма отправки данных и получения подтверждений с последующей повторной передачей пакетов, для которых

истекло определенное время таймера. Преимущество TFTP по сравнению с FTP состоит в простоте передачи файла и в небольшом объеме передаваемой служебной информации.

Коммутатор может функционировать и как FTP/TFTP-клиент, и как FTP/TFTP-сервер. Когда коммутатор работает, как FTP/TFTP-клиент, файлы конфигурирования или системные файлы могут быть загружены с удаленных FTP/TFTP-серверов (которыми могут быть хосты или другие коммутаторы) без какого-либо влияния на нормальное функционирование коммутатора. Кроме того в режиме FTP-клиента, список файлов может быть восстановлен с сервера. Конечно, коммутатор может загружать и файлы текущей конфигурации, а также системные файлы на удаленные FTP/TFTP-серверы (которые могут быть хостами или другими коммутаторами). Когда коммутатор работает как FTP/TFTP-сервер, он может осуществлять загрузку и выгрузку файлов для авторизованных FTP/TFTP-клиентов в соответствии со списком файлов, то есть использоваться в качестве FTP-сервера.

Ниже перечислено несколько терминов, часто используемых при FTP/TFTP. ROM: Сокращенное обозначение EPROM, перезаписываемого ПЗУ. Функции EPROM выполняет флэш-память коммутатора. SDRAM: Оперативная память коммутатора, используется программным обеспечением системы, в ней также хранятся последовательности команд конфигурирования. FLASH: Флэш-память, используемая для хранения системного файла и файла конфигурации. Системный файл: Содержит файл образа системы и загрузочный файл. Файл образа системы: Сжатый файл для драйвера аппаратных средств коммутатора и программы поддержки программного обеспечения, обычно обозначается как файл обновления IMAGE. В коммутаторе файл образа системы может быть сохранен только во флэш-памяти. В штатном режиме работы коммутатора имя файла образа системы, загружаемого по FTP в глобальном режиме, должно быть nos.img, файлы образа системы с другими именами будут отвергаться. Файл загрузки: Файл, который инициализирует коммутатор, также называемый файлом обновления ROM (большой по размеру файл, который при сжатии дает файл образа системы). В коммутаторе файл загрузки может быть сохранен только в ROM. В штатном режиме файл загрузки коммутатора имеет имя boot.rom.

Файл конфигурирования: Содержит файл конфигурирования, загружаемый при начальной загрузке и файл с текущей рабочей конфигурацией. Различие между файлом конфигурирования, загружаемым при начальной загрузке, и файлом с текущей рабочей конфигурацией может использоваться для упрощения резервного копирования и обновления конфигураций. Файл начальной загрузки коммутатора: Содержит последовательность команд конфигурирования, используемую при начальной загрузке коммутатора. Файлы конфигурирования начальной загрузки сохраняются в коммутаторах только во флэш-памяти и это соответствует сохранению конфигурирования. Для предотвращения несанкционированной загрузки файла и упрощения конфигурирования, в штатном режиме работы коммутатора имя файла конфигурирования начальной загрузки должно быть startup-config. Файл текущей рабочей конфигурации: Обозначает последовательность команд текущего рабочего конфигурирования коммутатора. В коммутаторах файл рабочей конфигурации хранится в оперативной памяти (RAM). В текущей версии коммутатора, текущая рабочая последовательность команд конфигурации running-config может быть сохранена из оперативной памяти во флэш-память с помощью команды write, либо с помощью команды copy running-config startup-config. В этом случае текущая рабочая последовательность команд конфигурирования станет содержимым файла конфигурирования начальной загрузки, эта операция называется сохранением конфигурации. Для предотвращения несанкционированной загрузки файла и упрощения конфигурирования, в штатном режиме работы коммутатора имя файла текущей рабочей конфигурации должно быть running-config. Файл заводской конфигурации: Файл конфигурации, поставляемый в комплекте с коммутатором, имеет имя factory-config. После ввода команд set default и write и последующей перезагрузки коммутатора, будет загружена заводская конфигурация, при этом текущий файл конфигурации начальной загрузуки будет переписан.

2.5.3.2 Настройка протоколов FTP/TFTP

Конфигурирование как FTP-, так и TFTP-клиента почти не различаются, поэтому процедуры настройки протоколов FTP и TFTP в этом руководстве будут рассмотрены совместно.

Последовательность настройки протоколов FTP/TFTP:

1. Настройка FTP/TFTP-клиента
   - Загрузить или выгрузить файл конфигурации или системный файл
   - Для FTP-клиента может быть проверен список файлов на сервере
2. Настройка FTP-сервера
   - Запуск FTP-сервера
   - Настройка имени пользователя и пароля для регистрации по FTP

- Изменение времени простоя соединения с FTP-сервером
- Выключение (Shut down) FTP-сервера

3. Настройка сервера TFTP
   - Запуск TFTP-сервера
   - Настройка времени простоя соединения с TFTP-сервером
   - Настройка времени повторной передачи для соединения с TFTP-сервером.
   - Выключение (Shut down) TFTP-сервера

1. Настройка FTP/TFTP-клиента
   - Загрузить или выгрузить файл конфигурации или системный файл.

Команда	Описание
Привилегированный режим	
copy <source-url> <destination-url> [**ascii** | **binary**]	Загрузка/выгрузка файла FTP/TFTP-клиента
Глобальный режим конфигурирования	
dir <ftpServerUrl>	Формат FtpServerUrl выглядит следующим образом ftp: //user: password@IP Address

2. Настройка FTP-сервера

Команда	Описание
Глобальный режим конфигурирования	
ftp-server enable **no ftp-server enable**	Запускает FTP-сервер. Отмена команды: “no ftp-server enable” выключает FTP-сервер и прекращает регистрацию пользователей по FTP
ip ftp username <username> {nopassword | password {0 | 7} <password>} **no ip ftp username** <username>	Устанавливает имя пользователя и пароль на FTP-сервере. Отмена команды (с no) удаляет имя пользователя и пароль
ftp-server timeout <seconds>	Устанавливает время простоя соединения
tftp-server enable **no tftp-server enable**	Запускает TFTP-сервер. Команда “**no ftp-server enable**” выключает TFTP-сервер и прекращает регистрацию пользователей по TFTP
tftp-server retransmission-timeout <seconds>	Задает максимальное время повторной передачи в течение интервала времени таймера

3. Настройка сервера TFTP

Команда	Описание
Глобальный режим конфигурирования	
tftp-server enable **no tftp-server enable**	Запускает TFTP-сервер. Команда “**no ftp-server enable**” выключает TFTP-сервер и прекращает регистрацию пользователей по TFTP
tftp-server retransmission-timeout <seconds>	Задает максимальное время повторной передачи в течение интервала времени таймера
tftp-server retransmission-number <number>	Задает максимальное время повторной передачи в течение интервала времени таймера

2.5.3.3 Примеры конфигурирования протоколов FTP/TFTP

На Рис. 12 приведена схема подключения коммутатора для загрузка файла nos.img для использования в качестве FTP/TFTP-клиента

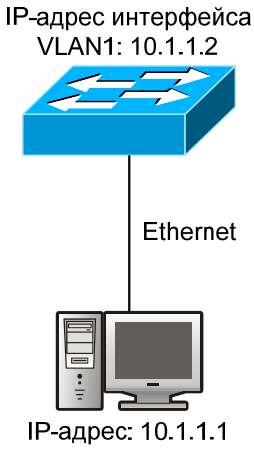

Рис. 12. Загрузка файла nos.img для использования в качестве FTP/TFTP-клиента

Пример 1:

Коммутатор используется, как FTP/TFTP-клиент. Коммутатор подключен к одному из портов компьютера и функционирует, как FTP/TFTP–сервер с IP-адресом 10.1.1.1. Коммутатор функционирует как FTP/TFTP-клиент, IP-адрес интерфейса VLAN1 10.1.1.2. Требуется загрузить в коммутатор файл “nos.img”, находящийся на компьютере.

Конфигурирование протокола FTP на компьютере: Запустите на компьютере программное обеспечение FTP-сервера, задайте имя пользователя “Switch” и пароль “switch”. Поместите файл “12_30_nos.img” в соответствующий каталог FTP-сервера на компьютере.

В коммутатор введите следующие команды:

```
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
```

После ввода этих команд файл “nos.img”, находящийся на компьютере будет загружен во флэш-память коммутатора.

Пример 2:

Коммутатор функционирует, как FTP-сервер. Коммутатор функционирует, как FTP-сервер, один из его портов подключен к компьютеру, являющемуся FTP-клиентом. Требуется передать файл “nos.img” с коммутатора на компьютер и сохранить его с именем 12_25_nos.img.

Процедура конфигурирования 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 switch
```

Конфигурирование на компьютере: С помощью любого программного обеспечения FTP-клиента зарегистрируйтесь на коммутаторе, используя имя “Switch” и пароль “Password”. Введите команду “get nos.img nos.img”, чтобы загрузить файл “nos.img” с коммутатора на компьютер.

Пример 3:

Коммутатор функционирует, как TFTP-сервер. Коммутатор функционирует, как TFTP-сервер, один из его портов подключен к компьютеру, являющимся TFTP-клиентом. Требуется загрузить файл “nos.img” с коммутатора в компьютер. Процедура конфигурирования 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
```

Конфигурирование на компьютере: Зарегистрируйтесь на коммутаторе с помощью любого TFTP-клиента, затем используйте команду “**tftp**” для загрузки файла “nos.img” коммутатора в компьютер.

Пример 4:

Коммутатор функционирует, как FTP-клиент и выполняет просмотр списка файлов на FTP-сервере. Условия синхронизации: Коммутатор подключен к компьютеру через порт Ethernet, компьютер функционирует, как FTP-сервер с IP-адресом 10.1.1.1. Коммутатор функционирует, как FTP-клиент, IP-адрес интерфейса управляющей VLAN1 равен 10.1.1.2. Конфигурирование протокола FTP на компьютере: Запустите на PC программное обеспечение FTP-сервера, задайте имя пользователя “Switch” и пароль “switch”. Введите в коммутатор проследовательность команд:

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 неполадок при использовании протоколов FTP/TFTP

До запуска программы FTP используйте команду “**ping**” для проверки возможности установления соединения между FTP-клиентом и сервером. Если команда **ping** дает сбой, необходимо изучить соответствующую информацию по устранению неполадок, чтобы восстановить соединение по линии. После того, как файлы будут успешно переданы, на дисплей будут выведены сообщения, приведенные ниже.

Если они отсутствуют, проверьте линию, затем снова введите команду “**copy**”.

```
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. ..
```

После того, как файлы будут успешно приняты, на дисплей будут выведены сообщения, приведенные ниже.

Если они отсутствуют, проверьте линию, затем снова введите команду “**copy**”.

```
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 по FTP выполнено обновление системного файла или файла начальной загрузки системы коммутатора, коммутатор не должен быть перезагружен до тех пор, пока на дисплей не будут выведены сообщения “close ftp client” (закрываю ftp-клиент) или “226 Transfer complete.” (передача завершена). Эти сообщения показывают, что обновление выполнено успешно, в противном случае, коммутатор может не загрузиться. Если обновление системного файла или файла начальной загрузки системы коммутатора по FTP дало сбой, пожалуйста, попытайтесь выполнить обновление снова, либо используйте для обновления режим BootROM.

2.5.3.5 Устранение неполадок при использовании протокола TFTP

При загрузке/выгрузке системного файла по протоколу TFTP, должна быть гарантирована возможность установления соединения и линии связи. До запуска программы TFTP используйте команду “**ping**” для проверки возможности установления соединения между TFTP-клиентом и сервером. Если команда ping дает сбой, необходимо изучить соответствующую информацию по устранению неполадок, чтобы восстановить соединение по линии. После того, как файлы будут успешно переданы, на дисплей будут выведены сообщения, приведенные ниже.

Если они отсутствуют, проверьте линию, затем снова введите команду “**copy**”.

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

После того, как файлы будут успешно приняты, на дисплей будут выведены сообщения, приведенные ниже.

Если они отсутствуют, проверьте линию, затем снова введите команду “**copy**”.

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

Если по TFTP выполнено обновление системного файла или файла начальной загрузки системы коммутатора, коммутатор не должен быть перезагружен до тех пор, пока на дисплей не будет выведено сообщение “close tftp client” (закрываю tftp-клиент). Это сообщение показывает, что обновление выполнено успешно, в противном случае, коммутатор может не загрузиться. Если обновление системного файла или файла начальной загрузки системы коммутатора по TFTP дало сбой, пожалуйста, попытайтесь выполнить обновление снова, либо используйте для обновления режим BootROM.

3 Настройка стекирования

3.1 Начальные сведения об управлении сетью со стеками

Управление сетью со стеками является внутриполосным. В отличие от настройки с использованием интерфейсов CLI, SNMP и Web, в которых реализовано прямое управление соответствующими коммутаторами с рабочей станции управления, при управлении сетью со стеками реализуется прямое управление соответствующими коммутаторами (коммутаторами-членами) посредством промежуточного коммутатора (управляющего коммутатора). Управляющий коммутатор может управлять многими коммутаторами-членами. После того, как будет настроен общедоступный IP-адрес управляющего коммутатора, всеми коммутаторами-членами, имеющими частные IP-адреса можно будет управлять удаленно. Это позволяет экономить общедоступные IP-адреса, запас которых ограничен. Управление сетью со стеками может динамически обнаруживать коммутаторы, являющиеся кандидатами для работы в стеке (коммутаторы-кандидаты). Администраторы сети могут статически или динамически добавлять коммутаторы-кандидаты в уже существующий стек. Кроме того, используя управляющий коммутатор, они могут настраивать коммутаторы-кандидаты и управлять ими. Когда коммутаторы-члены распределены физически (находятся на разных этажах здания), управление сетью со стеками дает значительные преимущества. Более того, управление сетью со стеками является внутриполосным. Управляющий коммутатор может связываться с коммутаторами-членами, используя существующую сеть. Поэтому нет необходимости строить специальную сеть для управления.

Управление сетью со стеками имеет следующие особенности:

Экономятся IP-адреса

Упрощается настройка сети

Отсутствует зависимость от топологии сети и расстояний

Автоматическое обнаружение, автоматическая настройка

Используя заводские настройки для управления сетью со стеками, можно осуществлять управление многими коммутаторами.

С управляющего коммутатора можно осуществлять управление любыми коммутаторами-членами стекастека.

3.2 Настройка управления сетью со стеками

Последовательность настройка управления стекированием:

1. Включить или выключить функцию работы со стеками
2. Создать стек
   - Настроить частный IP-адрес пула коммутаторов-членов стека
   - Создать или удалить стек
   - Добавить или удалить коммутатор-член
3. Настроить атрибуты стека на управляющем коммутаторе
   - Включить или выключить автоматическое включение в стек
   - Установить автоматическое добавление коммутаторов-членов к коммутаторам-членам, заданным вручную
   - Задать или изменить время поддержки сообщений на коммутаторах стека.
   - Задать максимальное число сообщений, потерявших актуальность, но которые могут быть разрешены
   - Стереть список коммутаторов-кандидатов, обнаруженных управляющим коммутатором
4. Настроить атрибуты стека на коммутаторе-кандидате
   - Задать время поддержки сообщений стека
   - Задать максимальное число сообщений, потерявших актуальность, но которые могут быть разрешены в стеке
5. Удаленное управление сетью со стеком
   - Удаленное управление настройкой
   - Удаленное обновление коммутатора-члена
   - Перезагрузка коммутатора-члена
6. Управление сетью со стеками по web-интерфейсу
   - Включить протокол http
7. Управление сетью со стеками по протоколу snmp

- Включить snmp-сервер

1. Включить или выключить функцию работы со стеками

Команда	Описание
Глобальный режим конфигурирования	
cluster run [key <WORD>] [vid <VID>] **no cluster run**	Включает функцию стекирования на коммутаторе или выключает

2. Создать стек

Команда	Описание
Глобальный режим конфигурирования	
cluster ip-pool <commander-ip> **no cluster ip-pool**	Позволяет настроить частный IP-адрес пула коммутаторов-членов стека
cluster commander [<cluster-name>] **no cluster commander**	Позволяет создать или удалить стек
cluster member {candidate-sn <candidate-sn> | mac-address <mac-addr> [id <member-id>]} **no cluster member** {id <member-id> | mac-address <mac-addr>}	Позволяет добавить или удалить коммутатор-член

3. Настроить атрибуты стека на управляющем коммутаторе

Команда	Описание
Глобальный режим конфигурирования	
cluster auto-add **no cluster auto-add**	Позволяет включить или выключить добавление в стек нового обнаруженного коммутатора-кандидата, либо запретить такое добавление
cluster member auto-to-user	Позволяет заменить автоматическое добавление коммутаторов-членов на добавление их вручную
cluster keepalive interval <second> **no cluster keepalive interval**	Позволяет задать время поддержки сообщений в стеке
cluster keepalive loss-count <int> **no cluster keepalive loss-count**	Позволяет задать максимальное число сообщений, потерявших актуальность, но которые могут быть разрешены в стеке
Привилегированный режим	
clear cluster nodes [nodes-sn <candidate-sn-list> | mac-address <mac-addr>]	Позволяет стереть список коммутаторов-кандидатов, обнаруженных управляющим коммутатором

4. Настроить атрибуты стека на коммутаторе-кандидате

Команда	Описание
Глобальный режим конфигурирования	
cluster keepalive interval <second> **no cluster keepalive interval**	Позволяет задать время поддержки сообщений в стеке
cluster keepalive loss-count <int> **no cluster keepalive loss-count**	Позволяет задать максимальное число сообщений, потерявших актуальность, но которые могут быть разрешены в стеке

5. Удаленное управление сетью со стеком

Команда	Описание
Глобальный режим конфигурирования	
rcommand member <member-id>	Введенная для управляющего коммутатора, эта команда позволяет настроить коммутаторы-члены и управлять ими
rcommand commander	Введенная для коммутатора-члена, эта команда позволяет настроить коммутатор-член
cluster reset member [id <member-id> | mac-address <mac-addr>]	Введенная для управляющего коммутатора, эта команда позволяет перезагрузить коммутатор-член
cluster update member <member-id> <src-url> <dst-filename> [ascii | binary]	Введенная для управляющего коммутатора, эта команда позволяет удаленно обновить коммутатор-член. Можно обновить только файл nos.img

6. Управление сетью со стеками по Web-интерфейсу

Команда	Описание
Глобальный режим конфигурирования	
ip http server	Включает функцию http на управляющем коммутаторе и коммутаторе-члене. Примечание: Когда управляющий коммутатор связывается с коммутатором-членом по web-интерфейсу, на коммутаторе-члене должна быть включена функция http. Управляющий коммутатор связывается с коммутатором-членом через узел синхронизации (beat member node), имеющийся в топологии стека

7. Управление сетью со стеками по протоколу snmp

Команда	Описание
Глобальный режим конфигурирования	
snmp-server enable	Включает функцию snmp-сервера на управляющем коммутаторе и коммутаторе-члене. Примечание: Когда управляющий коммутатор связывается с коммутатором-членом по протоколу snmp, на коммутаторе-члене должна быть включена функция snmp-сервера. Управляющий коммутатор связывается с коммутатором-членом, если задана символьная строка <commander-community>@sw<m ember id>

3.3 Примеры настройки стека

Имеется четыре коммутатора Switch 1 — Switch 4 (Рис. 13), при этом Switch 1 является управляющим коммутатором, а остальные коммутаторы — это коммутаторы-члены. Switch 2 и Switch 4 соединены с управляющим коммутатором напрямую, а Switch 3 подключен к нему через Switch 2.

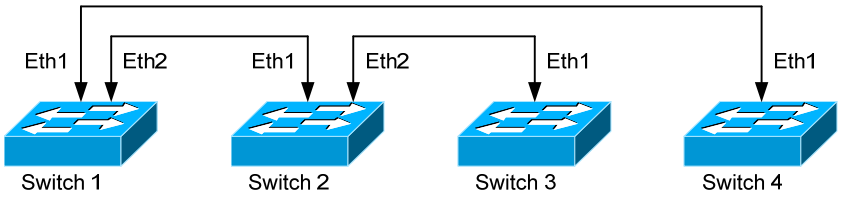

Рис. 13. Примеры настройки стекирования

Настройка для управляющего коммутатора (Switch 1):

```
Switch1(config)#cluster run
Switch1(config)#cluster ip-pool 10.2.3.4
Switch1(config)#cluster commander 5526
Switch1(config)#cluster auto-add
```

Настройка для коммутаторов членов (Switch 2 — Switch 4):

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

3.4 Устранение неполадок при администрировании стекирования

Если при администрировании стека возникли проблемы, пожалуйста, проверьте следующие причины их возникновения:

Проверьте правильность конфигурирования управляющего коммутатора, включена ли функция автоматического добавления в стек. Проверьте, принадлежит ли VLAN стека порты, подключенные к управляющему коммутатору и коммутаторам-членам.

После того как управление стеком включено на интерфейсе VLAN1 управляющего коммутатора, пожалуйста, не включайте протокол маршрутизации (RIP, OSPF, BGP) на этот VLAN, чтобы предотвратить вещание через протокол маршрутизации частных адресов стека этот VLAN на другие коммутаторы, приводящее к зацикливанию маршрутов.

Проверьте правильность соединения управляющего коммутатора с коммутаторами-членами. Для этого можно использовать пакеты отладки стекирования, позволяющие проверить

правильность обработки пакетов администрирования стекирования управляющим коммутатором и коммутаторами-членами.

4 Настройка портов

4.1 Начальные сведения по настройке портов

Коммутатор содержит 24 электрических порта Fast Ethernet 100 Мбит/с и 2 комбо-порта Gigabit Ethernet 1000 Мбит/с.

4.2 Процедура настройки сетевых параметров порта

1. Войдите в режим настройки сетевых параметров порта
2. Настройте сетевые параметры портов
   - Включите или выключите порты
   - Задайте имена портов
   - Задайте для портов типы кабелей
   - Установите для портов скорость и режим дуплекса
   - Настройте управление скоростью
   - Настройте управление трафиком
   - Включите или выключите функцию петли для порта
3. Настройте функцию управления датами подавления пакетов
4. Протестируйте виртуальные кабели

1. Войдите в режим настройки сетевых параметров порта

Команда	Описание
Режим настройки интерфейсов	
interface ethernet <interface-list>	Включает режим настройки сетевых параметров порта

2. Настройка сетевых параметров Ethernet-портов

Команда	Описание
Режим настройки интерфейсов	
shutdown **no shutdown**	Включает или выключает заданные порты
name <string> **no name**	Присваивает имя или удаляет его для заданных портов
mdi { auto | across | normal } **no mdi**	Задает тип кабеля для указанного порта
speed-duplex {**auto** | **force10-half** | **force10-full** | **force100-half** | **force100-full** | **force100-fx** | {{**force1g-half** | **force1g-full**} [**nonegotiate** [**master** | **slave**]]}}	Задает скорость и режим дуплекса для оптических портов 1000 Мбит/с
bandwidth control <bandwidth> {**both** | **receive** | **transmit**} **no bandwidth control**	Задает для указанных портов скорости приема и передачи данных
flow control **no flow control**	Включает или выключает функции управления трафиком для указанных портов

3. Настройте функцию управления датами подавления пакетов

Команда	Описание
Режим настройки интерфейсов	
rate-suppression {**broadcast** | **brmc** | **brmcdlf** | **all**} <Kbits> **no rate-suppression**	Включает функцию подавления пакетов на коммутаторе, позволяет установить максимальное количество пропускаемых данных. Отмена команды: “no rate-suppression” используется для выключения функции подавления пакетов

4. Протестируйте виртуальные кабели

Команда	Описание
Режим настройки интерфейсов	
Virtual-cable-test	Тестирует виртуальные кабели порта

4.3 Пример настройки порта

Схема применения коммутаторов приведена на Рис. 14.

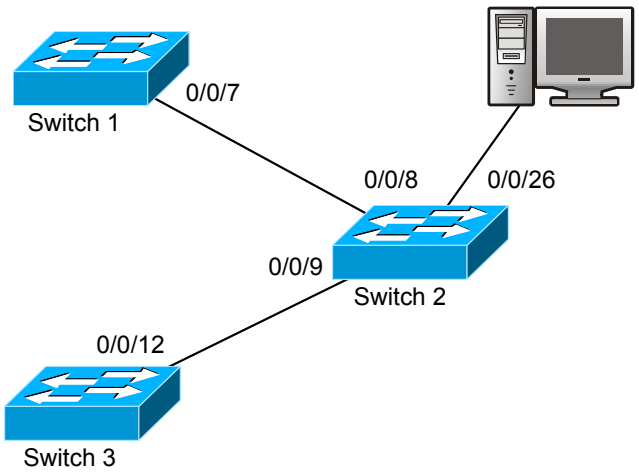

Рис. 14. Схема применения

По умолчанию используется VLAN1, так как на всех коммутаторах интерфейсы VLAN не настроены.

Коммутатор	Порт	Атрибуты
Switch1	0/0/7	Ограничение входной скорости: 150 M
Switch2	0/0/8	Порт-источник для зеркального порта
	0/0/9	Скорость 100 Мбит/с, полный дуплекс, порт-источник для зеркального порта
	0/0/26	Скорость 1000 Мбит/с, полный дуплекс, зеркальный порт (порт назначения)
Switch3	0/0/12	100 Мбит/с, полный дуплекс

Пример настройки:

Switch1:

```
Switch1(config)#interface ethernet 0/0/7
Switch1(config-If-ethernet0/0/7)#bandwidth control both 150
```

Switch2:

```
Switch2(config)#interface ethernet 0/0/9
Switch2(config-If-ethernet0/0/9)#speed-duplex force100-full
Switch2(config-If-ethernet0/0/9)#exit
Switch2(config)#interface ethernet 0/0/26
Switch2(config-If-ethernet0/0/26)# speed-duplex force1000-full
Switch2(config-If-ethernet0/0/26)#exit
Switch2(config)#monitor session 1 source interface ethernet0/0/8;0/0/9
Switch2(config)#monitor session 1 destination interface ethernet 0/0/26
```

Switch3:

```
Switch3(config)#interface ethernet 0/0/12
Switch3(config-If-ethernet0/0/12)#speed-duplex force100-full
Switch3(config-If-ethernet0/0/12)#exit
```

4.4 Устранение неполадок с портами

Ниже перечислены некоторые ситуации, часто возникающие в процессе настройки порта и рекомендуемые способы устранения проблем. Два соединенных друг с другом оптических интерфейса не будут связываться по линии, если на одном из них задано автоматическое определение параметров, а на другом принудительно установлена скорость и режим дуплекса. Это соответствует стандарту IEEE 802.3.

Не рекомендуется использовать следующие комбинации: на одном и том же порту включено управление трафиком и задано ограничение группового трафика; на одном и том же порту задано ограничение скорости и настройки для группового трафика, широковещательного трафика, используется управление для одноадресного трафика с неизвестным назначением, Если заданы такие комбинации, пропускная способность порта может оказаться меньше требуемой.

5 Настройка функции изоляции портов

5.1 Начальные сведения об изоляции портов

Функция изоляции портов — это независимая функция, действующая между портами и позволяющая изолировать потоки различных портов. Используя изоляцию портов, пользователи могут изолировать порты в VLAN, чтобы сохранить ресурсы VLAN и улучшить надежность работы сети. Когда эта функция включена, порты в группе изолированных портов будут изолированы один от другого (в отличие от портов, принадлежащих разным группам изолированных портов). Может случиться и ситуация, когда не окажется группы, способной передавать данные другой группе обычным способом, Коммутатор поддерживает не более 16 групп изолированных портов.

100 Мбитные порты обычно используются для подключения устройств (downlink), как uplink-порты они используются только в специальных случаях. Имейте в виду, что 8 из них функционируют, как полная группа. Это означает, что если порт ethernet 0/0/1 сконфигурирован, как uplink-порт, то все порты от ethernet 0/0/1 до ethernet 0/0/8 также будут uplink-портами и будут способны связываться с другими портами. Если порт ethernet 0/0/1 сконфигурирован, как downlink-порт, то порты ethernet 0/0/1 — ethernet 0/0/8 также будут downlink-портами. Остальные порты также подчиняются этому правилу.

5.2 Последовательность настройки изоляции портов

1. Создание группы изолированных портов
2. Добавление Ethernet-портов в группу
3. Вывод на дисплей информации о конфигурации изолированных портов

1. Создание группы изолированных портов

Команда	Описание
Глобальный режим конфигурирования	
isolate-port group <WORD> **no isolate-port group** <WORD>	Задает группу изолированных портов. Отмена команды (с no) удаляет группу изолированных портов

2. Добавление Ethernet-портов в группу

Команда	Описание
Глобальный режим конфигурирования	
isolate-port group <WORD> **switchport interface** [<ethernet>] <IFNAME> \ **no isolate-port group** <WORD> **switchport interface** [<ethernet>] <IFNAME>	Добавляет один или несколько портов для их изоляции в группу изолированных портов. Каждый порт группы изолирован от остальных. Отмена команды (с no) удаляет один или несколько портов из группы

3. Вывод на дисплей информации о конфигурации изолированных портов

Команда	Описание
Привилегированный режим, глобальный режим конфигурирования	
show isolate-port group [<WORD>]	Выводит на дисплей информацию об изолированных портах, в том числе информацию по всем сконфигурированным группам изолированных портов, а также по всем Ethernet-портам в каждой группе

5.3 Примеры применения функции изоляции портов

Пример использования функции изоляции портов приведен на Рис. 15.

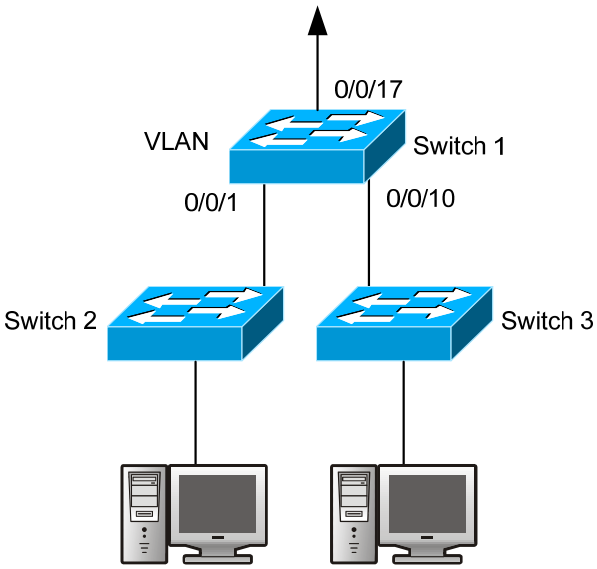

Рис. 15. Пример применения функции изоляции портов

Топология и конфигурация коммутаторов показана на рисунке выше. Порты e0/0/1, e0/0/10 и e0/0/17 принадлежат VLAN 100. Требуется, чтобы после включения изоляции портов на коммутаторе Switch 1, порты e0/0/1 и e0/0/10 этого коммутатора не могли связываться между собой, в то время как каждый из них может связываться с uplink-портом e0/0/17. Таким образом, связь между любой парой downlink-портов блокирована, а заданный uplink-порт работает в нормальном режиме. Uplink-порт должен связываться с любым портом как обычно. Последовательность команд для настройки коммутатора Switch 1:

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

6 Настройка обнаружения петель в портах

6.1 Начальные сведения об обнаружении петель в портах

По мере совершенствования Ethernet-коммутаторов, доступ к сети через них получает все большее количество пользователей. В сети предприятия, пользователи получают доступ к ней через коммутаторы уровня 2, что предъявляет жесткие требования и к работе в Интернет и к межсетевому обмену на уровне 2. Когда необходим межсетевой обмен уровня 2, сообщения будут передаваться с помощью MAC-адресации, которая обеспечивает точность, необходимую для корректного межсетевого обмена сообщениями между пользователями. При коммутации уровня 2 сообщения будут передаваться с помощью MAC-адресации. Устройства уровня 2 обучаются MAC-адресам, используя MAC-адрес источника. Следовательно, когда порт принимает сообщение от источника с неизвестным MAC-адресом, он добавляет этот MAC-адрес для порта, на котором было принято сообщение, поэтому передача последующих сообщений назначенных на этот MAC-адрес может осуществляться напрямую — обучение MAC-адресу проводится один раз, для всех передаваемых сообщений.

Когда устройство уровня 2 уже обучено MAC-адресу нового источника и изменяется только порт источника, то исходный порт источника будет заменен новым портом. В результате исходный MAC-адрес будет соответствовать новому порту. Поэтому, если в линии существует петля, все MAC-адреса всей сети уровня 2 будут соответствовать порту, на котором имеется петля (при этом MAC-адреса будут часто переключаться с одного порта на другой) — это приведет к неработоспособности сети уровня 2. В связи с этим крайне важно проверять сетевые порты на наличие петель. При обнаружении петли, устройство-обнаружитель должно послать сообщения сигнализации в систему управления сетью, дающее системному администратору информацию, достаточную для обнаружения, локализации и решения проблем сети, при этом длительные простои сети должны быть исключены.

Так как обнаружение петель может происходить динамически, на основании решений о наличии петли в линии, устройства, поддерживающие управление портами (например, изоляцию портов, управление обучением порта MAC-адресам) могут автоматически отслеживать эту ситуацию, что не только снижает нагрузку на системных администраторов, но также уменьшает время отклика, сводя к минимуму эффекты от наличия петель в сети.

6.2 Последовательность настройки функции обнаружения петель в портах

1. Настройка временного интервала для обнаружения петли
2. Включение функции обнаружения петли на порту
3. Настройка метода управления обнаружением петли в порту
4. Вывод на дисплей информации об обнаружении петли в порту и отладочной информации
5. Настройка режима управления обнаружением петли в порту (включено или нет автоматическое восстановление)

1. Настройка временного интервала для обнаружения петли

Команда	Описание
Глобальный режим конфигурирования	
loopback-detection interval-time <**loopback**> <**no-loopback**> **no loopback-detection interval-time**	Настройка временного интервала для обнаружения петли

2. Включение функции обнаружения петли на порту

Команда	Описание
Режим настройки интерфейсов	
loopback-detection specified-VLAN <vlan-list> **no loopback-detection specified-vlan** <vlan-list>	Включает или выключает функцию обнаружения петли на порту

3. Настройка метода управления обнаружением петли в порту

Команда	Описание
Режим настройки интерфейсов	
loopback-detection control {**shutdown** | **block**	Включает или выключает функцию

learning} **no loopback-detection control**	управления обнаружением петли на порту

4. Вывод на дисплей информации об обнаружении петли в порту и отладочной информации

Команда	Описание
Привилегированный режим	
debug loopback-detection **no debug loopback-detection**	Включает вывод отладочной информации модуля обнаружения петли на порту. Отмена команды: no debug loopback-detection прекращает вывод отладочной информации
show loopback-detection [interface <interface-list>]	Выводит на дисплей состояние и результаты обнаружения петель для всех портов (если параметры команды не заданы). Если в команде заданы параметры будет отображена информация только для указанных портов

5. Настройка режима управления обнаружением петли в порту (включено или нет автоматическое восстановление)

Команда	Описание
Глобальный режим конфигурирования	
loopback-detection control-recovery timeout <0-3600>	Позволяет настроить режим управления обнаружением петли в порту (включено или нет автоматическое восстановление), либо задать время восстановления

6.3 Пример настройки функции обнаружения петель в портах

Пример использования функции обнаружения петель приведен на Рис. 16

Рис. 16. Пример применения функции обнаружения петель в портах.

Коммутатор определяет наличие петель в топологии сети. Настройка функции:

Когда функция обнаружения петли будет включена на порту, которым коммутатор подключен к внешней сети, коммутатор будет уведомлять подключенную сеть о существовании петли и управлять портом на коммутаторе, чтобы гарантировать нормальную работу всей сети. Последовательность команд для настройки коммутатора:

```
Switch(config)#loopback-detection interval-time 35 15
Switch(config)#interface ethernet 0/0/1
Switch(config-If-ethernet0/0/1)#loopback-detection special-vlan 1-3
Switch(config-If-ethernet0/0/1)#loopback-detection control block
```

6.4 Устранение неполадок обнаружения петель в портах

По умолчанию функция обнаружения петель в портах выключена, ее следует включать только, когда это требуется.

7 Настройка функции ULDP

7.1 Начальные сведения о функции ULDP

Однонаправленная линия — это основное состояние линии при ошибках, особенно в оптических линиях. Однонаправленность линии означает, что только один порт линии может принимать сообщения от связанного с ним порта, в то время как другой порт не может принимать сообщения от связанного с ним порта. Так как на физическом уровне линии соединены и работают нормально, то проверка линий на физическом уровне не выявляет каких-либо проблем связи между устройствами. Как показано наРис. 17, Рис. 18, проблему с оптическим соединением невозможно выявить, используя такие механизмы физического уровня, как автоматическое определение параметров.

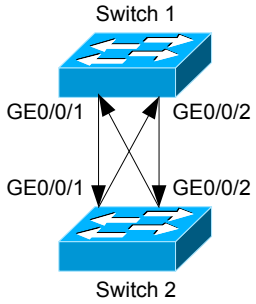

Рис. 17. Кроссовое оптическое соединение.

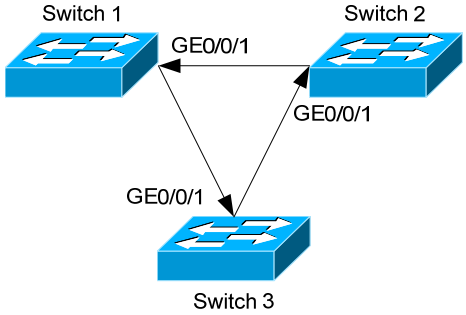

Рис. 18. Один конец каждого оптического кабеля не присоединен.

Такого рода проблемы часто случаются в следующих ситуациях: при неполадках с конвертером гигабитного интерфейса GBIC (Giga Bitrate Interface Converter), либо с интерфейсами, при ошибках ПО — в этих случаях аппаратные средства становятся недоступны, либо работают неправильно, Однонаправленная линия приводит к серьезным проблемам, например к зацикливанию связующего дерева, broadcast — шторму (broadcast black hole).

Протокол обнаружения однонаправленной связи ULDP (Unidirectional Link Detection Protocol) помогает выявить причины сбоев, возникающих по вышеперечисленным причинам. Если коммутатор подключен оптическими или медными Ethernet-линиями (например, витой парой категории 5 ultra), протокол ULDP позволяет контролировать состояние связи на физических линиях. При обнаружении однонаправленной связи протокол будет посылать пользователю предупреждения, кроме того, пользователь может настроить протокол на автоматическое или ручное отключение порта.

Протокол ULDP коммутаторов распознает удаленные устройства и проверяет корректность соединений линий с помощью интерактивных сообщений ULDP. Когда ULDP включен на порту, функционирует процедура обработки состояний протокола. Для различных состояний протокола создаются сообщения, которые посылаются для проверки состояния соединения, при этом по линии выполняется обмен информацией с удаленными устройствами. Протокол ULDP может динамически обучаться интервалу времени, через который удаленные устройства посылают сообщения уведомления. В соответствии с этим интервалом ULDP устанавливает TTL (time to live) — время поддержки сообщений. Кроме того, ULDP обеспечивает перезагрузку, необходимую после отключения порта протоколом ULDP. При перезагрузке производится еще одна проверка.

Временные интервалы сообщений уведомления и перезагрузки ULDP могут быть заданы пользователем. Это ускоряет обнаружение ошибок в конкретных условиях работы сети.

Если ULDP работает нормально, это говорит о том, что линия работает в режиме полного дуплекса, ULDP включен на обоих концах линии, используется один и тот же метод аутентификации и пароль.

7.2 Последовательность настройки протокола ULDP

1. Включение функции ULDP в глобальном режиме конфигурирования
2. Включение функцию ULDP на порту
3. Настройка агрессивного режима в глобальном режиме конфигурирования
4. Настройка агрессивного режима на порту
5. Установка метода выключения однонаправленной линии
6. Установка интервала времени для сообщений Hello
7. Установка интервала времени восстановления
8. Перезагрузка порта, выключенного протоколом ULDP
9. Вывод на дисплей информацию отладки и ULDP

1. Включение функции ULDP в глобальном режиме конфигурирования

Команда	Описание
Глобальный режим конфигурирования	
udlp enable **udlp disable**	Включает или выключает функцию ULDP в глобальном режиме конфигурирования

2. Включение функцию ULDP на порту

Команда	Описание
Режим настройки интерфейсов	
uldp enable **uldp disable**	Включает или выключает функцию ULDP на порту

3. Настройка агрессивного режима в глобальном режиме конфигурирования

Команда	Описание
Режим настройки интерфейсов	
uldp aggressive-mode **no uldp aggressive-mode**	Позволяет установить режим работы на порту

4. Настройка агрессивного режима на порту

Команда	Описание
Режим настройки интерфейсов	
uldp aggressive-mode **no uldp aggressive-mode**	Позволяет установить режим работы на порту

5. Установка метода выключения однонаправленной линии

Команда	Описание
Глобальный режим конфигурирования	
uldp manual-shutdown **no uldp manual-shutdown**	Позволяет установить метод выключения однонаправленной линии

6. Установка интервала времени для сообщений Hello

Команда	Описание
Глобальный режим конфигурирования	
uldp hello-interval <integer> **no uldp hello-interval**	Позволяет задать интервал отправки сообщений Hello — в пределах от 5 до 100 секунд. По умолчанию 10 секунд

7. Установка интервала времени восстановления

Команда	Описание
Глобальный режим конфигурирования	
uldp recovery-time <integer> **no uldp recovery-time** <integer>	Позволяет задать интервал восстановления путем перезагрузки — в пределах от 30 до 86400 секунд. По умолчанию 0 секунд

8. Перезагрузка порта, выключенного протоколом ULDP

Команда	Описание
Глобальный режим конфигурирования или режим настройки порта	
uldp reset	В глобальном режиме конфигурирования — перезагрузка всех портов. В режиме настройки интерфейсов — перезагрузка указанного порта

9. Вывод на дисплей информацию отладки и ULDP

Команда	Описание
Привилегированный режим	
show uldp [interface ethernet IFNAME]	Выводит на дисплей информацию ULDP. При вводе команды без параметров на дисплее отображается общая информация ULDP. Если в команде в виде параметра задан порт, на дисплей будет выведена общая информация и информация для порта
debug uldp fsm interface ethernet <IFname> **no debug uldp fsm interface ethernet** <IFname>	Включает или выключает вывод отладочных сообщений об изменении состояния для указанного порта
debug uldp error **no debug uldp error**	Позволяет включить или выключить вывод сообщений об ошибках. Позволяет включить или выключить вывод сообщений о событиях. Включает или выключает тип сообщений, которые могут отправляться и приниматься на всех портах. Включает или выключает вывод детального содержания сообщений определенного типа, которые могут отправляться и приниматься на указанном порту
debug uldp event **no debug uldp event** **debug uldp packet {receive | send}** **no debug uldp packet {receive | send}**	
debug uldp {**hello** | **probe** | **echo** | **unidir** | **all**} [**receive** | **send**] **interface ethernet** <IFname> **no debug uldp** {**hello** | **probe** | **echo** | **unidir** | all} [**receive** | **send**] **interface ethernet** <IFname>	

7.3 Примеры настройки функции ULDP

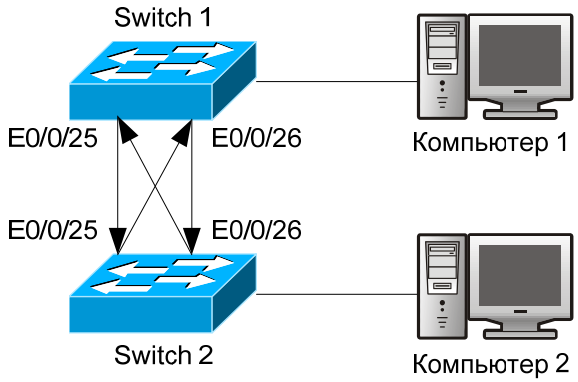

Рис. 19. Кроссовое оптическое соединение.

В топологии сети, показанной на Рис. 19, порты E0/0/25 E0/0/26 коммутатора Switch 1, а также порты E0/0/25 E0/0/26 коммутатора Switch 2 являются оптическими портами. Соединение является кроссовым. Соединения на физическом уровне выполнены без ошибок и функционируют нормально, однако уровень линии передачи данных функционирует неправильно. ULDP может обнаружить и исключить такие ошибочные состояния линии. В результате порты E0/0/25, E0/0/26 коммутатора Swiotch 1 и порты E0/0/25, E0/0/26 коммутатора Switch 2 будут выключены ULDP. Порты могут работать правильно только в том случае, если нет ошибок в соединениях.

Команды настройки коммутатора Switch 1:

```
Switch1(config)#uldp enable
Switch1(config)#interface ethernet 0/0/1
Switch1(config-If-ethernet0/0/1)#uldp enable
```

```
Switch1(config-If-ethernet0/0/1)#exit
Switch1(config)#interface ethernet0/0/2
Switch1(config-If-ethernet0/0/2)#uldp enable
```

Команды настройки коммутатора Switch 2:

```
Switch2(config)#uldp enable
Switch2(config)#interface ethernet0/0/3
Switch2(config-If-ethernet0/0/3)#uldp enable
Switch2(config-If-ethernet0/0/3)#exit
Switch2(config)#interface ethernet0/0/4
Switch2(config-If-ethernet0/0/4)#uldp enable
```

В результате порты E0/0/25, E0/0/26 2 коммутатора Switch 1 выключены ULDP, уведомления об этом выведены на дисплей компьютера 1 (см. ниже).

```
   %Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet0/0/25 need
to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet0/0/25 shut down!
%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet0/0/26 need to
be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet0/0/26 shutted down! Port e0/0/25,
and port e0/0/26 of SWITCH 2 are all shut down by ULDP, and there is notification
information on the CRT terminal of PC2.
%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet0/0/25 need to
be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet0/0/25 shutted down!
%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet0/0/26 need to
be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet0/0/26 shutted down!
```

7.4 Устранение неполадок ULDP

Замечания, касающиеся настройки:

- Для того чтобы ULDP смог обнаружить, что один или нескольких оптических портов не подключены, либо неправильно подключены в кроссе, порты должны работать в дуплексном режиме и на одной и той же скорости.
- Если механизм автоматического определения параметров оптических портов для какого-либо некорректно подключенного порта установит рабочий режим и скорость портов, ULDP не сможет помешать этому, при этом не важно включен ULDP или нет. В такой ситуации порт считается выключенным (“Down”).
- Для уверенности в том, что порты окружения (neighbors) могут быть созданы правильно и корректно будут обнаруживаться однонаправленные линии, необходимо, чтобы ULDP был включен на обоих концах линии, использовался один и тот же метод аутентификации и пароль. В настоящее время ввод пароля на обоих концах не требуется.
- Интервал отправки сообщений hello можно изменить так, чтобы ULDP мог быстрее реагировать на ошибки соединений в линиях при различных условиях работы сети. По умолчанию интервал отправки сообщений hello установлен 10 секунд и может быть задан в пределах от 5 до 100 секунд. Однако этот интервал должен быть менее 1/3 от времени сходимости STP. Если интервал слишком большой, цикл STP будет сгенерирован до того, как ULDP обнаружит и выключит порт с однонаправленным соединением. Если интервал слишком короткий, увеличится нагрузка на сеть и ее пропускная способность снизится.
- ULDP не обрабатывает никакие события LACP. Он обращается с каждой линией группы TRUNK (например, Port-channel, портами TRUNK), как с независимой линией и соответствующим образом обрабатывает каждую из них.
- ULDP несовместим с подобными протоколами других производителей; это означает, что пользователи не могут использовать ULDP на одном конце линии, а на другом ее конце — подобный протокол другого производителя.
- Функция ULDP по умолчанию выключена. Одновременно с включением функции ULDP в глобальном режиме конфигурирования может быть включен и вывод отладочных сообщений. Имеется несколько команд отладки (DEBUG), выводящих отладочную информацию, например, информацию о событиях, состояниях,

ошибках и сообщениях. В зависимости от значений параметров, выводятся сообщения различных типов.

- Таймер восстановления по умолчанию выключен, он будет включен только в том случае, когда пользователем задан интервал времени восстановления (30-86400 секунд).
- Команда и механизм перезагрузки могут перезагружать только порты, автоматически выключенные ULDP. Порты, выключенные пользователями вручную или другими модулями не будут перезагружаться по ULDP.

8 Настройка функции LLDP

8.1 Начальные сведения о функции LLDP

LLDP (Link Layer Discovery Protocol) — это новый протокол, определенный стандартом 802.1ab. Протокол включает на соседних устройствах отправку сообщений об их состоянии на другие устройства, кроме того на всех портах каждого устройства выполняется сохранение информации об устройствах. Если необходимо, порты могут посылать обновленную информацию на соседние устройства, непосредственно подключенные к ним. Соседние устройства будут сохранять эту информацию в стандартных MIB SNMP. Используя MIB, система управления сетью может проверять состояние соединения уровня 2. LLDP не конфигурирует элементы сети и потоки, и не управляет ими. Протокол LLDP лишь сообщает информацию о конфигурировании уровня 2. Другие средства, определенные в стандарте 802.1ab используют информацию LLDP для обнаружения конфликтов уровня 2. Сейчас IEEE использует существующую физическую топологию, интерфейсы и объекты MIB IETF.

Таким образом, упрощенно LLDP можно считать протоколом обнаружения соседних устройств. Он определяет для Ethernet-устройств (коммутаторов, маршрутизаторов, точек доступа WLAN и т. д.) стандартный метод, которым они уведомляют соседние сетевые устройства о своем существовании и сохраняют информацию обо всех обнаруженных соседних устройствах. Детальная информация о конфигурации устройства и обнаруженных устройствах, полученная протоколом может, например, использоваться для оповещения.

Более точно, LLDP определяет состав основной информации оповещения, протокол транспортировки оповещений и метод хранения принятой информации оповещений. При формировании своей собственной информации оповещения, устройство может помещать для транспортировки множество фрагментов информации оповещения в один пакет данных локальной сети. Тип транспортировки определяется значением в поле TLV (Type Length Value — значение длины типа). Все устройства, поддерживающие LLDP, должны поддерживать оповещения об ID устройства и ID порта, однако при этом подразумевается, что большая часть устройств должны также поддерживать оповещения об имени системы, ее описании и производительности. Оповещения с описанием системы и о производительности системы могут также содержать полезную информацию, необходимую для сбора информации о потоках в сети. Оповещение с описанием системы может содержать такие данные, как полное имя устройства, отправившего оповещение, тип аппаратных средств системы, информацию о версии программного обеспечения операционной системы и так далее.

Протокол LLDP (802.1AB Link Layer Discovery Protocol) будет использоваться для поиска причин возникновения проблем в сети предприятия, он ускоряет процесс поиска неисправностей, увеличивает возможности ПО управления сетью, так как работает с точной топологией сети.

В ПО управления сетью для отслеживания изменений и состояния топологии часто используется функция автоматического обнаружения (“Automated Discovery”), однако только в самом лучшем ПО такого рода можно достигать уровня 3 и классифицировать устройства во всех IP-подсетях. Этот тип данных очень примитивен, фиксируются только основные события, например, добавление и удаление соответствующих устройств, но не детальная информация о том, как эти устройства взаимодействуют с сетью.

Информация об уровне 2 включает информацию об устройствах и их портах, о том, какие коммутаторы подключены к остальным устройствам и т. п.. Можно вывести на дисплей информацию о маршрутах между клиентами, коммутаторами, маршрутизаторами, серверами приложений, сетевыми серверами. Эти подробности крайне необходимы для планирования и исследования причин сбоев сети.

LLDP будет очень полезным инструментом управления, обеспечивающим сбор точной информации о зеркалировании сети, потоках в сети и исследовании проблем, возникающих в сети.

8.2 Последовательность настройки функции LLDP

1. Включение функции LLDP в глобальном режиме конфигурирования
2. Включение или выключение на коммутаторе функции LLDP на основе портов
3. Настройка рабочего состояния порта LLDP
4. Настройка интервалов обновления сообщений LLDP
5. Настройка множителя времени поддержки сообщений LLDP
6. Настройка задержки отправки обновляющих сообщений
7. Настройка интервалов отправки сообщений Trap

8. Настройка включения функции Trap порта
9. Настройка свойств отправки дополнительной информации порта
10. Настройка размера памяти, используемой для хранения таблицы удаленного доступа для порта
11. Настройка типа операции, выполняемой, когда таблица удаленного доступа полностью заполнена
12. Вывод на дисплей информации отладки LLDP

1. Включение функции LLDP в глобальном режиме конфигурирования

Команда	**Описание**
Глобальный режим конфигурирования	
lldp enable lldp disable	Глобально включает или выключает функцию LLDP

2. Включение или выключение на коммутаторе функции LLDP на основе портов

Команда	**Описание**
Режим настройки интерфейсов	
lldp enable lldp disable	Включает или выключает на коммутаторе функцию LLDP на основе портов

3. Настройка рабочего состояния порта LLDP

Команда	**Описание**
Режим настройки интерфейсов	
lldp mode (**send** | **receive** | **both** | **disable**)	Выполняет настройку рабочего состояния порта LLDP

4. Настройка интервалов обновления сообщений LLDP

Команда	**Описание**
Глобальный режим конфигурирования	
lldp tx-interval <integer> **no lldp tx-interval**	Позволяет задать интервалы обновления сообщений LLDP (можно ввести значение, либо использовать значение, заданное по умолчанию)

5. Настройка множителя времени поддержки сообщений LLDP

Команда	**Описание**
Глобальный режим конфигурирования	
lldp msgTxHold <value> **no lldp msgTxHold**	Позволяет задать множитель времени поддержки обновления сообщений LLDP (можно ввести значение, либо использовать значение, заданное по умолчанию)

6. Настройка задержки отправки обновляющих сообщений

Команда	**Описание**
Глобальный режим конфигурирования	
lldp transmit delay <seconds> **no lldp transmit delay**	Позволяет задать интервалы отправки обновляющих сообщений LLDP (можно ввести значение, либо использовать значение, заданное по умолчанию)

7. Настройка интервалов отправки сообщений Trap

Команда	**Описание**
Глобальный режим конфигурирования	
lldp notification interval <seconds> **no lldp notification interval**	Позволяет задать интервалы отправки сообщений Trap (можно ввести значение, либо использовать значение, заданное по умолчанию)

8. Настройка включения функции Trap порта

Команда	**Описание**
Режим настройки интерфейсов	
lldp trap <**enable**|**disable**>	Включает или выключает функцию Trap порта

9. Настройка свойств отправки дополнительной информации порта

Команда	**Описание**
Режим настройки интерфейсов	

lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap] **no lldp transmit optional tlv**	Позволяет настроить свойства отправки дополнительной информации порта (можно выбрать значение, либо использовать значение, заданное по умолчанию)

10. Настройка размера памяти, используемой для хранения таблицы удаленного доступа для порта

Команда	Описание
Режим настройки интерфейсов	
lldp neighbors max-num < value > **no lldp neighbors max-num**	Позволяет задать размер памяти для хранения таблицы удаленного доступа для порта (можно задать значение, либо выбрать значение, заданное по умолчанию)

11. Настройка типа операции, выполняемой, когда таблица удаленного доступа полностью заполнена

Команда	Описание
Режим настройки интерфейсов	
lldp tooManyNeighbors {**discard** | **delete**}	Позволяет задать тип операции, выполняемой, когда таблица удаленного доступа заполнена

12. Вывод на дисплей информации отладки LLDP

Команда	Описание
Привилегированный режим, глобальный режим конфигурирования	
show lldp	Выводит на дисплей текущую информацию LLDP
show lldp interface ethernet <IFNAME>	Выводит на дисплей информацию настройки LLDP на текущем порту
show lldp traffic	Выводит на дисплей информацию по всем счетчикам.
show lldp neighbors interface ethernet < IFNAME >	Выводит на дисплей LLDP-информацию об устройствах окружения для текущего порта
show debugging lldp	Выводит информацию для всех портов, на которых включена отладка LLDP
Привилегированный режим	
debug lldp no debug lldp	Включает или выключает режим отладки
debug lldp packets interface ethernet <IFNAME> **no debug lldp packets interface ethernet** <IFNAME>	В глобальном режиме конфигурирования или в режиме настройки интерфейсов включает или выключает прием и отправку отладочных пакетов
Режим настройки интерфейсов	
clear lldp remote-table	Очищает таблицу удаленного доступа на порту

8.3 Пример настройки функции LLDP

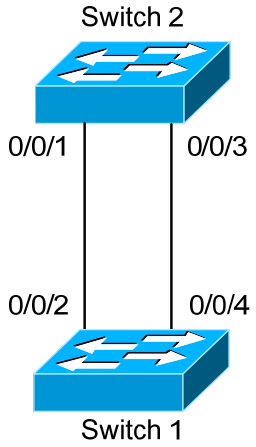

Рис. 20. Пример типичной конфигурации при использовании функции LLDP

В сети, топология которой показана на Рис. 20, порты 1,3 коммутатора Switch 2 подключены к портам 2,4 коммутатора Switch 1.

Порт 1 коммутатора Switch 2 работает в режиме только приема сообщений, для опции TLV порта 4 коммутатора Switch 1 выбрано значение portDes и SysCap.

Команды настройки коммутатора Switch 1:

```
Switch 1(config)# lldp enable
Switch 1(config)#interface ethernet 0/0/4
Switch 1(config-lf-ethernet0/0/4)# lldp transmit optional tlv portDesc sysCap
Switch 1(config-lf-ethernet0/0/4)exit
```

Команды настройки коммутатора Switch 2:

```
Switch 2(config)#lldp enable
Switch 2(config)#interface ethernet0/0/1
Switch 2(config-lf-ethernet0/0/1)# lldp mode receive
Switch 2(config-lf-ethernet0/0/1)#exit
```

8.4 Устранение неполадок работы функции LLDP

Функция LLDP по умолчанию выключена. После того, как функция LLDP включена в глобальном режиме конфигурирования коммутатора, можно включить режим отладки командой debug lldp” для контроля отладочной информации.

Используя команду “show” функции LLDP можно вывести на печать информацию о конфигурировании в глобальном режиме конфигурирования, либо в режиме настройки интерфейсов.

9 Настройка Port Channel

9.1 Начальные сведения о Port Channel

Чтобы понять, что такое Port Channel, необходимо ввести понятие группы портов. Группа портов — это группа физических портов на уровне конфигурирования; только физические порты, входящие в группу портов могут участвовать в агрегации линии и становиться портами-членами Port Channel. На логическом уровне, группа портов является не портом, а последовательностью портов. При некоторых условиях физические порты группы портов реализуют агрегацию порта и формируют Port Channel, который имеет все свойства физического порта и, поэтому, становится независимым логическим портом. Агрегация порта — это абстрактное понятие; имеется в виду множество портов (последовательность портов) с одинаковыми свойствами, представляющее собой один логический порт. Port Channel представляет собой набор физических портов, на логическом уровне он используется как один физический порт. Port Channel может использоваться пользователем, как обычный порт. С помощью Port Channel возможно увеличение пропускной способности сети и резервирование линии. Агрегация портов обычно используется, когда коммутатор подключен к маршрутизатору, PC или другим коммутаторам.

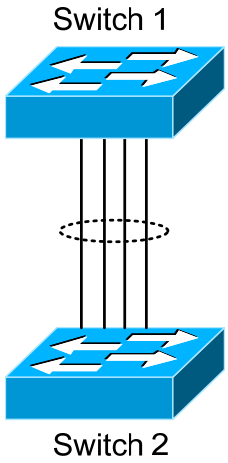

Рис. 21. Агрегация портов

Как показано на Рис. 21, коммутатор Switch 1 агрегирован в Port Channel, пропускная способность этого Port Channel равна сумме пропускных способностей всех четырех портов. Если необходимо передать трафик с Switch 1 на Switch 2 через Port Channel, расчет закрепляемого трафика будет выполнен на основе MAC-адреса источника и значения младшего разряда MAC-адреса назначения. По результатам вычислений будет принято решение — какой порт должен передавать этот трафик. При отказе порта в Port Channel, другие его порты примут на себя трафик, предназначавшийся отказавшему порту, при этом будет использован алгоритм закрепления трафика. Этот алгоритм реализован на аппаратном уровне. Коммутатор обеспечивает два метода настройки агрегации порта: создание Port Channel вручную и динамическое создание Port Channel на основе протокола LACP (Link Aggregation Control Protocol — протокол управления агрегацией линии). Агрегация портов может быть выполнена только на портах, работающих в режиме полного дуплекса.

Чтобы Port Channel работал правильно, физические порты-члены Port Channel должны иметь одинаковые свойства, перечисленные ниже:

- Все порты должны работать в режиме полного дуплекса.
- Все порты должны работать на одной и той же скорости.
- Все порты должны быть портами доступа, они должны принадлежать одному и тому же VLAN, либо все должны быть магистральными портами.
- Если порты являются магистральными, их свойства “Allowed VLAN” (разрешенная VLAN) и “Native VLAN” (исходная VLAN) должны быть одинаковыми.

Если настройка Port Channel на коммутаторе выполнена вручную или динамически, система автоматически установит в Port Channel на порту с наименьшим номером режим Master Port (режим управляющего порта). Если на коммутаторе активирован протокол spanning tree, этот

протокол будет считать Port Channel логическим портом и посылать кадры BPDU через управляющий порт.

Агрегация порта тесно связана с аппаратными средствами коммутатора. Коммутатор допускает агрегацию физических портов любых двух коммутаторов, максимально поддерживается 8 групп портов по 8 портов в каждой группе.

После того, как порты агрегированы, их можно использовать, как обычный порт. Коммутатор имеет встроенный режим настройки интерфейса агрегации, в этом режиме пользователь может ввести соответствующие настройки, подобно тому, как это делается в режиме настройки VLAN или физического порта.

9.2 Настройка Port Channel

1. Создание группы портов в глобальном режиме конфигурирования
2. Добавление портов в определенную группу в режиме настройки интерфейсов
3. Вход в режим настройки port-channel

1. Создание группы портов в глобальном режиме конфигурирования

Команда	Описание
Глобальный режим конфигурирования	
port-group [**load-balance** {dst-no port-group [load-balance] <port-group-number> src-mac | dst-src-ip}] <port-group-number>	Создает группу портов и задает метод балансировки нагрузки для этой группы

2. Добавление портов в определенную группу в режиме настройки интерфейсов

Команда	Описание
Режим настройки интерфейсов	
port-group <port-group-number>{**active**|**passive**|**on**} **no port-group** <port-group-number>	Позволяет добавить порты в группу портов и задать их режим. Отмена команды: “**no port-group**” удаляет группу портов

3. Вход в режим настройки port-channel

Команда	Описание
Глобальный режим конфигурирования	
interface port-channel <port-channel-number>	Осуществляет вход в режим настройки port-channel

9.3 Примеры использования Port Channel

Пример 1: Настройка Port Channel для протокола

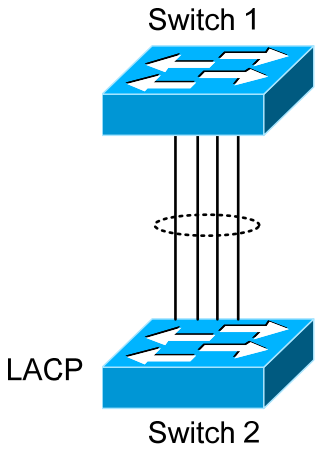

Рис. 22. Настройка Port Channel для протокола LACP

Имеется два коммутатора серии ZES-2000 (Рис. 22), при этом порты 1, 2, 3,4 коммутатора Switch 1 являются портами доступа и принадлежат VLAN1. Добавим эти три порта в группу 1 в активном режиме. Порты 6, 8, 9, 10 коммутатора Switch 2 являются портами доступа, которые

также принадлежат VLAN1. Добавим эти четыре порта в группу 2 в пассивном режиме. Все порты должны быть соединены кабелями.

Процедураинастройки:

```
Switch1#config
Switch1(config)#interface eth 0/0/1-4
Switch1(config-if-port-range)#port-group 1 mode active
Switch1(config-if-port-range)#exit
Switch1(config)#interface port-channel 1
Switch1(config-if-port-channel1)#
Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface eth 0/0/6
Switch2(config-if-ethernet0/0/6)#port-group 2 mode passive
Switch2(config-if-ethernet0/0/6)#exit
Switch2(config)#interface eth 0/0/8-10
Switch2(config-if-port-range)#port-group 2 mode passive
Switch2(config-if-port-range)#exit
Switch2(config)#interface port-channel 2
Switch2(config-if-port-channel2)#
```

Результат настройки:

ПО успешно выполнило агрегацию портов, теперь порты 1, 2, 3, 4 коммутатора Switch 1 образуют агрегированный порт с именем “Port-Channel1”, порты 6, 8 — 10 коммутатора Switch 2 образуют агрегированный порт с именем “Port-Channel2”; настройки могут быть сделаны в режиме настройки соответствующего агрегированного порта.

Пример 2: Настройка Port Channel в режиме ON.

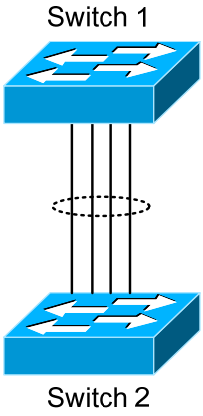

Рис. 23. Настройка Port Channel в режиме ON

Пример: Как показано на Рис. 23, порты 1, 2, 3, 4 коммутатора Switch 1 являются портами доступа и принадлежат VLAN1. Добавим эти четыре порта в группу 1 в режиме “on”. Порты 6, 8 — 10 коммутатора Switch 2 являются портами доступа, которые также принадлежат VLAN1. Добавим эти четыре порта в группу group2 в режиме “on”.

Процедура настройки:

```
Switch1#config
Switch1(config)#port-group 1
Switch1(config)#interface ethernet 0/0/1
Switch1(config-if-ethernet0/0/1)#port-group 1 mode on
Switch1(config-if-ethernet0/0/1)#exit
Switch1(config)#interface ethernet 0/0/2
Switch1(config-if-ethernet0/0/2)#port-group 1 mode on
Switch1(config-if-ethernet0/0/2)#exit
Switch1(config)#interface ethernet 0/0/3
Switch1(config-if-ethernet0/0/3)#port-group 1 mode on
Switch1(config-if-ethernet0/0/3)#exit
Switch1(config)#interface ethernet 0/0/4
Switch1(config-if-ethernet0/0/4)#port-group 1 mode on
```

```
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 0/0/6
Switch2(config-if-ethernet0/0/6)#port-group 2 mode on
Switch2(config-if-ethernet0/0/6)#exit
Switch2(config)#interface ethernet 0/0/8-10
Switch2(config-if-port-range)#port-group 2 mode on
Switch2(config-if-port-range)#exit
```

Результат настройки:

Порты 1, 2, 3, 4 коммутатора Switch 1 добавлены по порядку в группу портов 1, в этой группе принудительно установлен режим “on”. Коммутатору на другом конце не требуется обмена сообщениями LACP BPDU для завершения агрегирования. Агрегирование будет завершено, как только будет введена команда добавления порта 2 в группу 1, при этом порт 1 и порт 2 будут агрегированы в port-channel 1. Когда в группу 1 будет введен порт 3, порт 1 и порт 2 будут разгруппированы и повторно сгруппированы с портом 3 для формирования port-channel 1. Когда в группу 1 будет введен порт 4, port-channel 1 портов 1, 2 и 3 будет разгруппирован, а затем сгруппирован снова с портом 4 для формирования port-channel 1. (Когда новый порт вводится в агрегированную группу портов, группа будет разгруппирована, а затем на ее основе будет создана новая группа.) Теперь все четыре порта на обоих коммутаторах (Switch 1 и Switch 2) агрегированы в режиме “on” и принадлежат соответствующему агрегированному порту.

9.4 Устранение неполадок Port Channel

Если при настройке агрегированных портов возникли проблемы, в первую очередь проверьте следующее:

Удостоверьтесь в том, что все порты в группе портов имеют одинаковые свойства, например, все они работают в режиме полного дуплекса, принудительно установлена одна и та же скорость, порты имеют одни и те же свойства VLAN и т. д. Если обнаружены несоответствия, исправьте их.

Некоторые команды нельзя использовать для порта, входящего в port-channel, например, arp, bandwidth, ip, ip-forward и т. д.

После того, как создан port-channel, все настройки порта могут быть сделаны только на порту port-channel.

LACP несовместим с безопасными портами и портами 802.1x. Если на порту уже включены эти два протокола, LACP использовать невозможно.

Если при создании port-channel конфигурирование выполнено неправильно, на экране появятся сообщения, приведенные ниже. NOTICE: Please check ACL/Qos/DCSCM config. No ACL/Qos/DCSCM operation is allowed if the port is in a PortGroup.

Шаги по удалению или настройке ACL/Qos/DCSCM на порту, входящему в группу портов PortGroup.

1. Удалить все порты-члены из группы PortGroup
2. Настроить одни и те же параметры ACL/Qos/DCSCM на всех портах-членах.
3. Добавить порты обратно в группу PortGroup.

Методы разделения потока всеми портами группы должны быть одинаковыми. Если новые сконфигурированные группы портов отличаются от прежних, на экран будет выведено сообщение об этом.

100M-порты не поддерживают режим разделения потока dst-src-ip.

10 Настройка Jumbo-кадров

10.1 Начальные сведения о Jumbo-кадрах

До настоящего времени кадры Jumbo не были стандартизированы (в частности, не были стандартизированы их формат и длина). Обычно кадры с размером от 1519 до 9000 относят к jumbo-кадрам. Если в сети необходимо передавать jumbo-кадры, то ее пропускную способность следует увеличить на 2% — 5%. В техническом плане Jumbo — это просто длинный кадр, принятый или посланный коммутатором. Однако из-за своей длины Jumbo-кадры не могут быть посланы в CPU. Мы исключили передачу Jumbo-кадров в CPU в процессе приема пакетов.

10.2 Последовательность настройки работы с кадрами Jumbo

1. Включение функции Jumbo

1. Включение функции Jumbo

Команда	Описание
Глобальный режим конфигурирования	
jumbo enable [<mtu-value>] **no jumbo enable**	Позволяет задать размер MTU для JUMBO-кадра и включить функцию приема/передачи JUMBO-кадров. Отмена команды (с no) выключает функцию приема/передачи JUMBO-кадров

11 Настройка виртуальных сетей (VLAN)

11.1 Настройка VLAN

11.1.1 Начальные сведения о VLAN

VLAN (Virtual Local Area Network — виртуальная локальная сеть) — это технология, при которой логические адреса устройств в сети делятся на сегменты в зависимости от функций, выполняемых устройствами, приложений и требований управления. Действуя таким образом, можно сформировать виртуальные локальные группы, не зависящие от физического расположения устройств, в них входящих. Анонсированный IEEE протокол IEEE 802.1Q стандартизует реализацию VLAN, функции VLAN коммутатора поддерживают стандарт IEEE 802.1Q.

Основная идея технологии VLAN состоит в динамическом разделении всей локальной сети на множество отдельных областей вещания (Рис. 24) в соответствии с требованиями, предъявляемыми к сети.

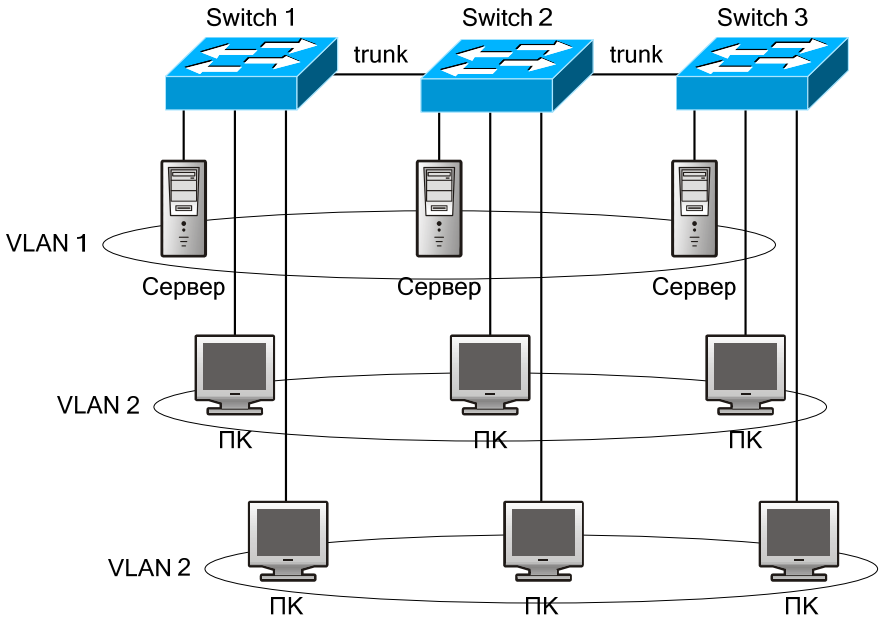

Рис. 24. Сеть VLAN, определенная логически

Каждая область вещания представляет собой VLAN. Сети VLAN обладают теми же свойствами, что и физические локальные сети, за исключением того, что VLAN являются логическими, а не физическими сетями. Поэтому конфигурирование сетей VLAN может выполняться безотносительно к физическому расположению устройств; вещательный, многоадресный и одноадресный трафики отдельно взятой VLAN отделены от трафика других VLAN.

Благодаря вышеперечисленным особенностям, технология VLAN обеспечивает следующие преимущества:

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

В коммутаторах VLAN и протокол GVRP (GARP VLAN Registration Protocol — протокол GARP-регистрации VLAN) реализованы в соответствии со стандартом 802.1Q. В этой главе подробно рассматривается настройка и применение VLAN и GVRP.

11.1.2 Настройка VLAN

1. Создание и удаление VLAN

2. Присвоение и удаление имени VLAN
3. Закрепление портов коммутатора для VLAN
4. Настройка типа порта коммутатора
5. Настройка магистрального порта
6. Настройка порта доступа
7. Включение/выключение правил обработки входных пакетов VLAN на портах
8. Настройка частной VLAN
9. Настройка ассоциации частной VLAN

1. Создание и удаление VLAN

Команда	Описание
Глобальный режим конфигурирования	
vlan WORD **no vlan** WORD	Позволяет создать или удалить VLAN, включить режим VLAN

2. Присвоение и удаление имени VLAN

Команда	Описание
Глобальный режим конфигурирования	
name <vlan-name> **no name**	Позволяет присвоить или удалить имя VLAN

3. Закрепление портов коммутатора для VLAN

Команда	Описание
Режим VLAN	
switchport interface <interface-list> **no switchport interface** <interface-list>	Позволяет закрепить порты коммутатора для VLAN

4. Настройка типа порта коммутатора

Команда	Описание
Режим настройки интерфейсов	
switchport mode {**trunk** | **access**}	Позволяет задать текущий порт, как магистральный или порт доступа

5. Настройка магистрального порта

Команда	Описание
Режим настройки интерфейсов	
switchport trunk allowed vlan {WORD | **all** | **add** WORD | **except** WORD | **remove** WORD} **no switchport trunk allowed vlan**	Позволяет разрешить прохождение магистрали через VLAN, либо запретить это. Отмена команды: no switchport trunk allowed vlan восстанавливает настройки, используемые по умолчанию
switchport trunk native vlan <vlan-id> **no switchport trunk native vlan**	Позволяет установить PVID для магистрального порта, либо удалить PVID

6. Настройка порта доступа

Команда	Описание
Режим настройки интерфейсов	
switchport access vlan <vlan-id> **no switchport access vlan**	Позволяет добавить текущий порт к VLAN с указанным числовым идентификатором VLAN. Отмена команды: no switchport access vlan восстанавливает настройки, используемые по умолчанию

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

Команда	Описание
Глобальный режим конфигурирования	
vlan ingress enable **no vlan ingress enable**	Позволяет включить или выключить правила обработки входящих пакетов VLAN

8. Настройка частной VLAN

Команда	Описание
Режим VLAN	
private-vlan {**primary** | **isolated** |	Позволяет настроить текущую VLAN как частную

community} **no private-vlan**	VLAN. Отмена команды: no private-vlan удаляет частную VLAN

9. Настройка ассоциации частной VLAN

Команда	Описание
Режим VLAN	
private-vlan association <secondary-vlan-list> **no private-vlan association**	Позволяет задать или удалить ассоциацию частной VLAN

11.1.3 Типичное применение VLAN

Типовая схема использования VLAN приведена на Рис. 25.

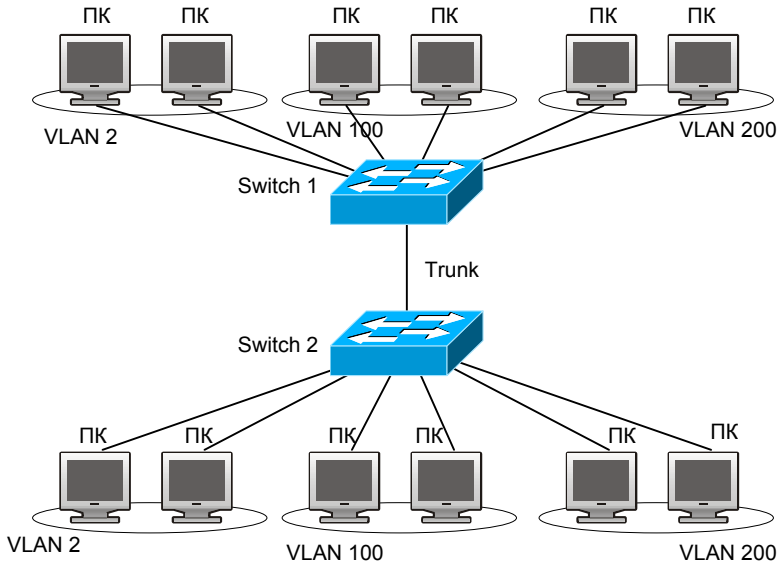

Рис. 25. Типичная топология VLAN

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

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

Объект настройки	Описание объекта настройки
VLAN2	Порты коммутаторов 2-4 на площадках 1 и 2
VLAN100	Порты коммутаторов 5-7 на площадках 1 и 2
VLAN200	Порты коммутаторов 8-10 на площадках 1 и 2
Магистральные порты	Порты коммутаторов 11 на площадках 1 и 2

Обмен трафиком VLAN между коммутаторами происходит по магистральной линии, соединяющей магистральные порты обоих коммутаторов. Все остальные сетевые устройства подключены к портам соответствующих VLAN.

В этом примере порты 1 и 12 не используются и могут использоваться для управления, либо для других целей. Процедура настройки:

Настройка коммутатор 1:

```
Switch1(config)#vlan 2
Switch1(config-vlan2)#switchport interface ethernet 0/0/2-4
Switch1(config-vlan2)#exit
Switch1(config)#vlan 100
Switch1(config-vlan100)#switchport interface ethernet 0/0/5-7
Switch1(config-vlan100)#exit
Switch1(config)#vlan 200
Switch1(config-vlan200)#switchport interface ethernet 0/0/8-10
```

```
Switch1(config-vlan200)#exit
Switch1(config)#interface ethernet 0/0/11
Switch1(config-if-ethernet0/0/11)#switchport mode trunk
Switch1(config-if-ethernet0/0/11)#exit
Switch1(config)#
```

Настройка коммутатор 2:

```
Switch2(config)#vlan 2
Switch2(config-vlan2)#switchport interface ethernet 0/0/2-4
Switch2(config-vlan2)#exit
Switch2(config)#vlan 100
Switch2(config-vlan100)#switchport interface ethernet 0/0/5-7
Switch2(config-vlan100)#exit
Switch2(config)#vlan 200
Switch2(config-vlan200)#switchport interface ethernet 0/0/8-10
Switch2(config-vlan200)#exit
Switch2(config)#interface ethernet 0/0/11
Switch2(config-if-ethernet0/0/11)#switchport mode trunk
Switch2(config-if-ethernet0/0/11)#exit
```

11.2 Настройка GVRP

11.2.1 Начальные сведения о GVRP

Протокол GARP (Generic Attribute Registration Protocol) может использоваться для динамического распределения, распространения и регистрации атрибутов информации между коммутаторами-членами в сети коммутации. Атрибутом может быть информация VLAN, групповой MAC-адрес другой информации. Очевидно, что протокол GARP может транспортировать множество функций атрибутов на коммутатор, на который их необходимо передать (populate). На основе GARP определены различные приложения (называемые приложениями-объектами GARP), одним из них является GVRP.

Протокол GVRP (GARP VLAN Registration Protocol) — это приложение, использующее для работы механизм GARP. Оно отвечает за обслуживание информации динамической регистрации VLAN и передачу регистрационной информации на другие коммутаторы. Коммутаторы, поддерживающие GVRP могут принимать информацию динамической регистрации VLAN от других коммутаторов и обновлять локальную информацию регистрации VLAN в соответствии с принятой. Коммутатор, на котором включен протокол GVRP может передавать свою собственную информацию регистрации VLAN на другие коммутаторы. Принятая информация регистрации VLAN содержит локальную статическую информацию, заданную вручную и динамическую информацию, полученную обучением от других коммутаторов. Поэтому, за счет передачи информации регистрации VLAN, состоятельная информация VLAN может быть распространена на все коммутаторы с включенным GVRP.

11.2.2 Настройка GVRP

1. Настройка параметров таймера GARP
2. Включение функции GVRP

1. Настройка параметров таймера GARP

Команда	Описание
Режим настройки интерфейсов	
garp timer join <timer-value> **no garp timer join garp timer leave** <timer-value> **no garp timer leave garp timer hold** <timer-value> **no garp timer hold**	Настройка таймеров удержания, слияния и выхода для GARP
Глобальный режим конфигурирования	
garp timer leaveall <timer-value> **no garp timer leaveall**	Позволяет настроить таймер общего выхода для GARP

2. Включение функции GVRP

Команда	Описание
Режим настройки интерфейсов	
gvrp	Включает или выключает функцию GVRP на текущем

no gvrp	порту
Глобальный режим конфигурирования	
gvrp **no gvrp**	Включает или выключает функцию GVRP на коммутаторе

11.2.3 Пример применения GVRP

Пример использования GVRP приведён на Рис. 26

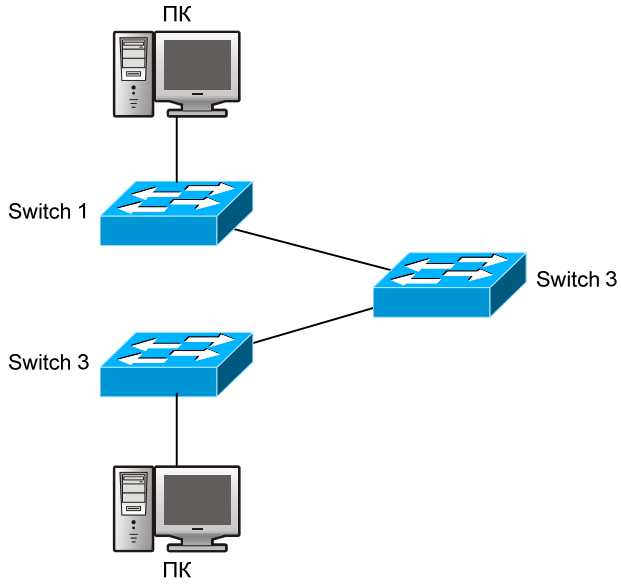

Рис. 26. Типичная топология при использовании GVRP

Для получения информации динамической регистрации VLAN и ее обновления на коммутаторах, на коммутаторе включен протокол GVRP. Требуется настроить GVRP на коммутаторах Switch 1, 2 и 3, включить на коммутаторе Switch 2 динамическое обучение VLAN100 таким образом, чтобы две рабочие станции, присоединенные к VLAN100 на коммутаторах Switch 1 и 3 могли связываться друг с другом через коммутатор Switch 2 без использования статических адресов VLAN100.

Объект настройки	Описание объекта настройки
VLAN100	Порты 2 — 6 коммутаторов Switch 1 и 3
Магистральные порты	Порты 11 коммутаторов Switch 1 и 3, порты 10, 11 коммутатора Switch 2
GVRP в глобальном режиме конфигурирования	Коммутаторы Switch 1, 2, 3
GVRP в режиме настройки интерфейсов	Порты 11 коммутаторов Switch 1 и 3, порты 10, 11 коммутатора Switch 2

Подключим две рабочие станции к портам VLAN100 на коммутаторах Switch 1 и 2, подключим порт 11 коммутатора Switch 1 к порту 10 коммутатора Switch 2; порт 11 коммутатора Switch 2 к порту 11 коммутатора Switch 3.

Процедура настройки коммутатора 1:

```
Switch1(config)# gvrp
Switch1(config)#vlan 100
Switch1(config-vlan100)#switchport interface ethernet 0/0/2-6
Switch1(config-vlan100)#exit
Switch1(config)#interface Ethernet 0/0/11
Switch1(config-if-ethernet0/0/11)#switchport mode trunk
Switch1(config-if-ethernet0/0/11)# gvrp
Switch1(config-if-ethernet0/0/11)#exit
```

Процедура настройки коммутатора 2:

```
Switch2(config)# bridge-ext gvrp
```

```
Switch2(config)#interface ethernet 0/0/10
Switch2(config-if-ethernet0/0/10)#switchport mode trunk
Switch2(config-if-ethernet0/0/10)# gvrp
Switch2(config-if-ethernet0/0/10)#exit
Switch2(config)#interface ethernet 0/0/11
Switch2(config-if-ethernet0/0/11)#switchport mode trunk
Switch2(config-if-ethernet0/0/11)# gvrp
Switch2(config-if-ethernet0/0/11)#exit
```

Процедура настройки коммутатора 3:

```
Switch3(config)# gvrp
Switch3(config)#vlan 100
Switch3(config-vlan100)#switchport interface ethernet 0/0/2-6
Switch3(config-vlan100)#exit
Switch3(config)#interface ethernet 0/0/11
Switch3(config-if-ethernet0/0/11)#switchport mode trunk
Switch3(config-if-ethernet0/0/11)# gvrp
Switch3(config-if-ethernet0/0/11)#exit
```

11.2.4 Устранение неполадок при GVRP

Настройки счетчика GARP для магистральных портов на обоих концах магистральной линии должны быть одинаковыми, в противном случае GVRP будет работать неправильно

11.3 Настройка туннеля Dot1q

11.3.1 Начальные сведения о туннеле Dot1q

Туннель Dot1q (также называемый QinQ (802.1Q-in-802.1Q)) является расширением стандарта 802.1Q. Его основной идеей является инкапсуляция пользовательского тега VLAN (тега CVLAN) в теге VLAN поставщика услуг (тег SPVLAN). Пакет, содержащий два тега VLAN, передается по магистральной сети составной сети поставщика услуг Интернета, при этом для пользователей обеспечивается простой туннель уровня 2. Им просто и легко управлять, применяя статическую настройку, что особенно хорошо подходит для маленьких офисных сетей или малых районных городских сетей, использующих в качестве магистрального оборудования коммутатор уровня 3.

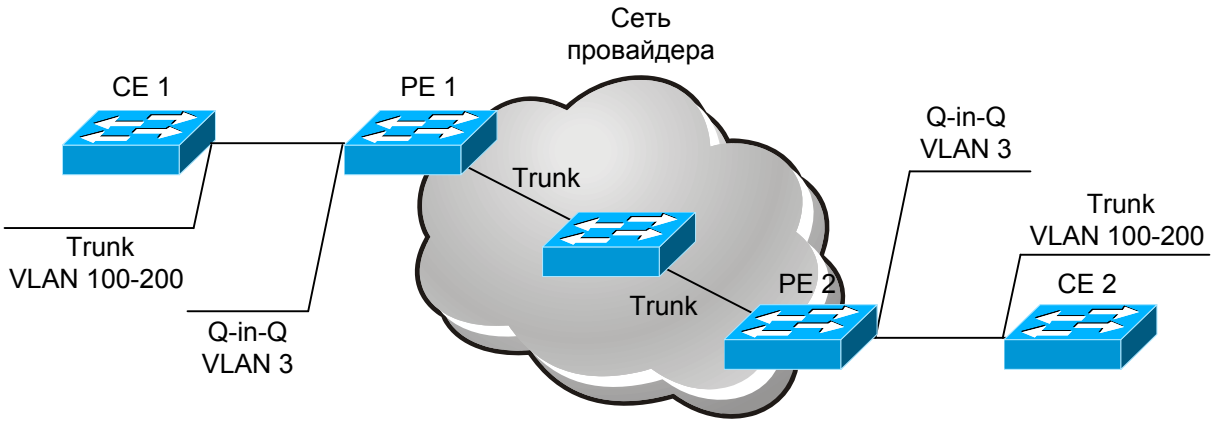

Рис. 27. Туннель Dot1q в режиме работы через Интернет

Как показано на Рис. 27, после включения на порту пользователя, dot1q-туннель закрепляет за каждым пользователем идентификатор SPVLAN (SPVID). На рисунке показан идентификатор пользователя 3. Одному и тому же пользователю сети должен быть присвоен один и тот же SPVID на различных PE. Когда пакет, отправленный с CE1, достигает PE1, он содержит тег VLAN 200-300 внутренней сети пользователя. Как только функция туннеля будет включена, в тег пакета другой VLAN будет добавлен порт пользователя на коммутаторе провайдера, ID которого является SPVID, закрепленный за пользователем. После этого пакет будет передаваться в VLAN3 только в том случае, когда он поступает в сеть поставщика услуг Интернета, уже неся в себе два тега VLAN (внутренний тег добавляется при вхождении на коммутатор провайдера, а внешний является идентификатором SPVID), при этом информация VLAN сети пользователя является открытой для сети поставщика услуг. Когда пакет достигает удаленного коммутатора

провайдера, перед его передачей на удаленный коммутатор клиента с порта на удаленном коммутаторе провайдера, внешний тег VLAN удаляется; после этого, пакет принятый удаленным коммутатором клиента становится абсолютно идентичным тому, который был послан локальным коммутатором клиента. Для пользователя роль сети оператора (между PE1 и PE2) состоит в обеспечении надежной линии уровня 2.

Технология Dot1q-туннеля позволяет поставщику услуг Интернет поддерживать множество клиентских VLAN с помощью только одной собственной VLAN. И поставщик услуг Интернет, и клиенты могут конфигурировать свои VLAN независимо друг от друга.

Dot1q-туннель обеспечивает следующие характеристики:

- Можно применять простое статическое конфигурирование, не требуется сложного конфигурирования и обслуживания.
- Операторы должны будут присвоить каждому пользователю только один SPVID, при этом число конкурирующих поддерживаемых пользователей увеличивается. Одновременно с этим пользователи получают полную свободу в выборе и управлении идентификаторами ID VLAN (могут выбираться пользователями произвольно в пределах от 1 до 4096).
- Пользовательская сеть рассматривается как независимая. Когда поставщик услуг Интернет модифицирует свою сеть, оригинальные конфигурации пользовательских сетей изменяться не должны.

Детальное описание применения и конфигурирования dot1q-туннеля при использовании коммутаторов серии будет представлено в этом разделе.

11.3.2 Последовательность настройки туннеля Dot1q

Последовательность настройки туннеля Dot1q-Tunnel:

1. Включение функции туннеля dot1q на коммутаторе.
2. Настройка типа протокола (TPID) на коммутаторе.
3. Настройка порта, как порта туннеля dot1q.

1. Включение функции туннеля dot1q на коммутаторе.

Команда	Описание
Глобальный режим конфигурирования	
dot1q-tunnel enable **no dot1q-tunnel enable**	Позволяет войти в режим туннеля dot1q в портах или выйти из этого режима

2. Настройка типа протокола (TPID) на коммутаторе.

Команда	Описание
Глобальный режим конфигурирования	
dot1q-tunnel tpid {**8100** | **9100** | **9200**}	Позволяет настроить тип протокола на коммутаторе

3. Настройка порта, как порта туннеля dot1q

Команда	Описание
Режим настройки интерфейсов	
switchport dot1q-tunnel mode {**customer** | **uplink**} **no switchport dot1q-tunnel**	Устанавливает порт, как порт туннеля dot1q

11.3.3 Типичные применения туннеля Dot1q

Пример:

Граничные коммутаторы PE1 и PE2 поставщика услуг Интернет ISP осуществляют передачу данных VLAN200-300 между CE1 и CE2 клиентской сети с VLAN3. Порт port1 на PE1 подключен к CE1, порт port10 подключен к сети общего пользования, TPID подключенного оборудования 9100; порт port1 на PE2 подключен к CE2, порт port10 подключен к сети общего пользования.

Объект настройки	Пояснения по настройке
VLAN3	Порт Port1 на PE1 и PE2
Туннель dot1q	Порт Port1 на PE1 и PE2
tpid	9100
Магистральный порт	Порт Port10 на PE1 и PE2

Процедура настройки коммутатора PE1:

```
Switch(config)#vlan 3
Switch(config-vlan3)#switchport interface ethernet 0/0/1
Switch(config-vlan3)#exit
Switch(config)#dot1q-tunnel enable
Switch(config)#dot1q-tunnel tpid 9100
Switch(config)#interface ethernet 0/0/1
Switch(config-if-ethernet0/0/1)#switchport dot1q-tunnel mode customer
Switch(config-if-ethernet0/0/1)#exit
Switch(config)#interface ethernet 0/0/10
Switch(config-if-ethernet0/0/10)#switchport mode trunk
Switch(config-if-ethernet0/0/10)#switchport dot1q-tunnel mode uplink
Switch(config-if-ethernet0/0/10)#exit
Switch(config)#
```

Процедура настройки коммутатора PE2:

```
Switch(config)#vlan 3
Switch(config-vlan3)#switchport interface ethernet 0/0/1
Switch(config-vlan3)#exit
Switch(config)#dot1q-tunnel enable
Switch(config)#interface ethernet0/0/1
Switch(config-if-ethernet0/0/1)#switchport dot1q-tunnel mode customer
Switch(config-if-ethernet0/0/1)#exit
Switch(config)#interface ethernet 0/0/10
Switch(config-if-ethernet0/0/10)#switchport mode trunk
Switch(config-if-ethernet0/0/10)#switchport dot1q-tunnel mode uplink
Switch(config-ethernet0/0/10)#exit
Switch(config)#
```

11.3.4 странение неполадок с туннелями Dot1q

- Пользовательский режим порта может быть установлен только на порту доступа, а режим uplink-порта — только на магистральном порту.
- Для достижения ожидаемой скорости передачи и гарантированно высокой производительности сети, на 1000M-порту рекомендуется использовать режим uplink-порта.
- Эта функция несовместима с частными vlan.

11.4 Настройка трансляции VLAN

11.4.1 Начальные сведения о трансляции VLAN

Трансляция VLAN, как следует из названия, — это способ обмена данными между разными VLAN, при котором исходный VLAN ID транслируется в новый VLAN ID в соответствии с требованиями, заданными пользователем. На данном изделии поддерживается трансляция входящих пакетов, а также трансляция VLAN ID на входе.

Настройка и применение трансляции VLAN будут подробно рассмотрены ниже в этом разделе.

11.4.2 Настройка трансляции VLAN

Последовательность настройки трансляции VLAN:

1. Настройка функции трансляции VLAN на порту
2. Настройка связей трансляции VLAN на порту
3. Настройка трансляции VLAN на порту, проверка наличия сбоев или отброшенных пакетов

1. Настройка функции трансляции VLAN на порту

Команда	Описание
Режим настройки портов	
vlan-translation enable **no vlan-translation enable**	Включает или выключает режим трансляции VLAN

2. Настройка связей трансляции VLAN на порту

Команда	Описание
Режим настройки портов	
vlan-translation <old-vlan-id> **to** <new-vlan-id> **in** **no vlan-translation old-vlan-id in**	Добавляет или удаляет связи для трансляции VLAN

3. Настройка трансляции VLAN на порту, проверка наличия сбоев или отброшенных пакетов

Команда	Описание
Режим настройки портов	
vlan-translation miss drop in **no vlan-translation miss drop in**	Настройка трансляции VLAN на порту, проверка наличия сбоев, отброшенных пакетов

11.4.3 Типичное применение трансляции VLAN

Пример топологии для работы в режиме трансляции VLAN приведён на Рис. 28. Граничные коммутаторы PE1 и PE2 поставщика услуг Интернет ISP осуществляют передачу данных VLAN20 между CE1 и CE2 клиентской сети с VLAN3. Порт port1 на PE1 подключен к CE1, порт port10 подключен к сети общего пользования, порт port1 на PE2 подключен к CE2, порт port10 подключен к сети общего пользования.

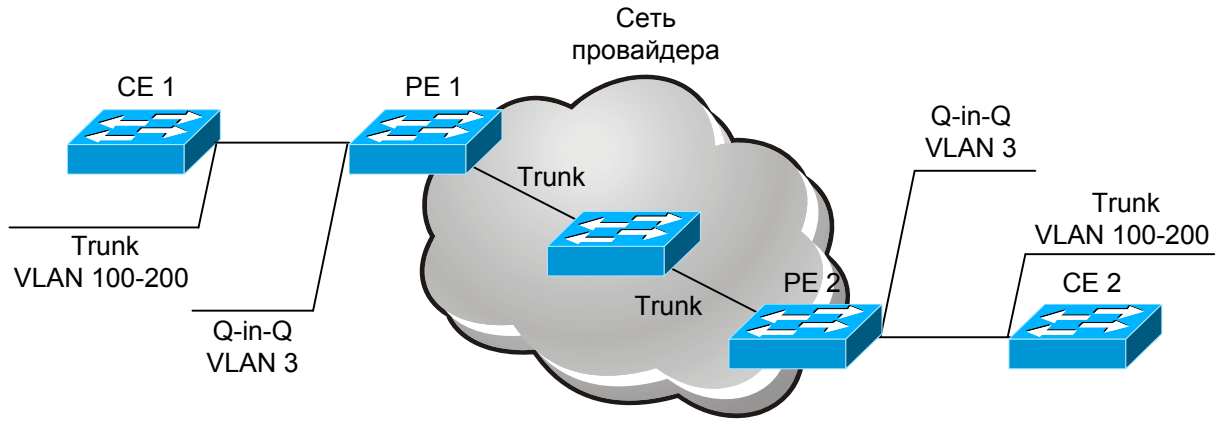

Рис. 28. Топология для работы в режиме трансляции VLAN

Объект настройки	Пояснения по настройке
Трансляция VLAN	Порт Port1 на PE1 и PE2
Магистральные порты	Порт Port1 и Port10 на PE1 и PE2

Процедура настройки коммтаторов PE1, PE2:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-if-ethernet 0/0/1)#switchport mode trunk
Switch(config-if-ethernet 0/0/1)# vlan-translation enable
Switch(config-if-ethernet 0/0/1)# vlan-translation 20 to 3 in
Switch(config-if-ethernet 0/0/1)# exit
Switch(config)#interface ethernet 0/0/10
Switch(config-if-ethernet 0/0/10)#switchport mode trunk
Switch(config-if-ethernet 0/0/10)# vlan-translation enable
Switch(config-if-ethernet 0/0/10)# vlan-translation 3 to 20 in
Switch(config-if-ethernet 0/0/10)#exit
Switch(config)#
```

11.4.4 Устранение неполадок трансляции VLAN

Обычно трансляция VLAN применяется на магистральных портах.

11.5 Настройка динамических VLAN

11.5.1 Начальные сведения о динамических VLAN

В динамических VLAN используется концепция относительности (relative concept), в отличие от статических VLAN (VLAN на основе портов).

Protocol VLAN будет передавать пакеты без тегов в VLAN в соответствии с типом их протокола, вместо того, чтобы определять VLAN, которой они должны быть переданы на основе физических подключений портов коммутатора. После настройки Protocol VLAN, коммутатор будет проверять пакеты, принятые от порта и идентифицировать VLAN на основе типов протоколов пакетов и типов инкапсуляции. Например, если VLAN сконфигурирована по протоколу IPv4 и используется инкапсуляция Ethernet II, все пакеты этого типа без тегов какой-либо VLAN будут считаться принадлежащими VLAN, на которую указывает тип IP-протокола.

Фильтр Protocol VLAN применим только к пакетам без тегов какой-либо VLAN, при этом пакеты с тегами VLAN, принятые от того же порта, не будут обрабатываться Protocol VLAN и сохранят свой оригинальный статус.

Protocol VLAN не создает новых VLAN, он совместно использует уже существующие VLAN, основанные на портах. Как только пакеты поступают в такие VLAN, они начинают передаваться в соответствии с теми же правилами, что и в VLAN, основанных на портах.

В соответствии с классификацией протоколов сетевого уровня, разным VLAN могут принадлежать разные протоколы. Это очень перспективно для сетей, в которых предоставление услуг ориентировано на приложения и специфические услуги, требуемые конкретным пользователям. Кроме того, пользователи могут перемещаться по сети, не меняя свою принадлежность к определенной VLAN. Преимущество этого подхода в том, что при изменении физического местонахождения пользователей не потребуется перенастраивать VLAN, к которой они принадлежат. То, что VLAN может быть классифицирована по типу протокола, является существенным и для администраторов сети Более того, при этом методе не требуются дополнительные теги кадров, идентифицирующие VLAN и это помогает снизить трафик в сети.

В коммутаторах сетевые порты 1000Mbps могут поддерживать протокол VLAN без каких-либо дополнительных условий; в Ethernet-портах 100Mbps для возможности использования этой функции должен быть установлен магистральный режим.

11.5.2 Последовательность настройки динамических VLAN

Последовательность настройки Protocol VLAN:

1. Настройка протокола

Команда	Описание
Глобальный режим конфигурирования	
protocol-vlan mode {**ethernetii** ety**p**e <etype-id> | **llc** {**dsap** <dsap-id> **ssap** <ssap-id>} | **snap etype** <etype-id>} **vlan** <vlan-id> **no protocol-vlan** {**mode** {**ethernetii etype** <etype-id> | **llc** {**dsap** <dsap-id> **ssap** <ssap-id>} | **snap etype** <etype-id>} | **all**}	Добавляет или удаляет соответствующие связи между VLAN и протоколами, то есть для конкретного протокола добавляет конкретную VLAN, либо удаляет ее для этого протокола

11.5.3 Устранение неполадок Protocol VLAN

- Хотя это и не является необходимым, каждая IP protocol VLAN должна содержать протоколы ARP во избежание проблем со связью, обусловленных сбоями ARP.
- Пожалуйста, удостоверьтесь в том, что на каком-либо порту нет VLAN для входящих пакетов, в противном случае передача данных может быть некорректна.

12 Настройка таблицы MAC-адресов

12.1 Начальные сведения о таблице MAC-адресов

Таблица MAC-адресов — это таблица соответствий MAC-адресов устройств назначения портам коммутатора. MAC-адреса делятся на статические и динамические. Статические MAC-адреса настраиваются пользователем вручную; они имеют наивысший приоритет и работают всегда (они не замещаются динамическими адресами); динамические MAC-адреса — это адреса, полученные коммутатором в процессе обучения при передаче кадров данных, они имеют ограниченное время действия. Когда коммутатор принимает кадр данных для передачи, он сохраняет MAC-адрес источника кадра данных и соответствующий ему порт назначения. Затем для получения MAC-адреса назначения к таблице MAC-адресов производятся обращения. В том случае, если соответствие найдено, кадр данных передается в соответствующий порт. В противном случае, коммутатор продвигает кадр данных в Broadcast-домен. Если обучение динамическим MAC-адресам по кадрам данных долгое время не выполняется, соответствующая информация удаляется из ячейки таблицы MAC-адресов. Для таблицы MAC-адресов определены две операции:

1. Получить MAC-адрес;
2. Передать или отфильтровать кадр данных в соответствии с таблицей MAC-адресов.

12.1.1 Получение таблицы MAC-адресов

Таблица MAC-адресов может быть построена статически или динамически. Статическая настройка представляет собой задание соответствий между MAC-адресами и портами; динамическое обучение — это процесс, при котором коммутатор обучается соответствиям между MAC-адресами и портами и регулярно обновляет таблицу MAC-адресов. В этом разделе будет рассматриваться, в основном, процесс динамического обучения MAC-адресам для построения таблицы MAC-адресов.

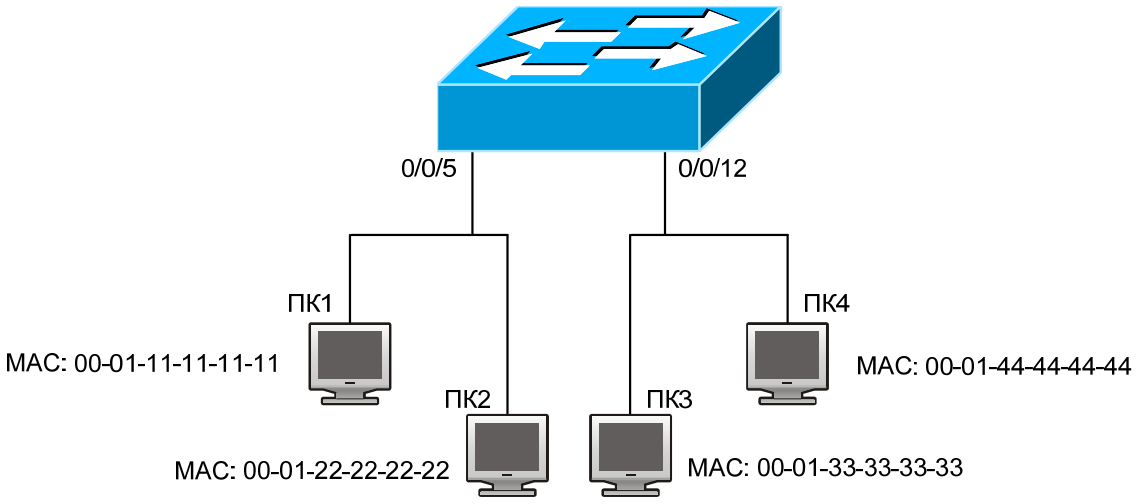

Рис. 29. Схема, поясняющая процесс обучения коммутатора MAC-адресам

На Рис. 29 представлена следующая схема: К коммутатору подключены четыре компьютера. Компьютеры ПК1 и ПК2 принадлежат одному и тому же физическому сегменту (домену коллизий), физический сегмент подключен к порту 0/0/5 коммутатора; ПК 3 и ПК 4 принадлежат одному и тому же сегменту, который подключен к порту 0/0/12 коммутатора.

Вначале таблица MAC-адресов не содержит соответствий адресов. Рассмотрим для примера связь между компьютерами ПК1 и ПК3, процесс обучения MAC-адресам следующий:

1. Когда ПК1 посылает сообщения на ПК3, коммутатор принимает MAC-адрес источника 00-01-11-11-11-11 из этого сообщения, при этом в таблицу MAC-адресов коммутатора добавляется соответствие между 00-01-11-11-11-11 и портом 0/0/5.
2. Одновременно с этим, коммутатор продолжает обучение по сообщению, адрес назначения которого равен 00-01-33-33-33-33. Так как таблица MAC-адресов в данный момент содержит только одно соответствие между MAC-адресом 00-01-11-

11-11-11 и портом 0/0/5 (для порта 00-01-33-33-33-33 соответствие отсутствует), коммутатор передает сообщение во все порты коммутатора (при допущении, что все порты по умолчанию принадлежат VLAN1).

3. ПК3 и ПК4, подключенные к порту 0/0/12 принимают сообщение, посланное ПК1, однако компьютер ПК4 не будет отвечать, так как MAC-адрес назначения равен 00-01-33-33-33-33. Ответ последует только от компьютера ПК3. Когда порт 12 принимает сообщение, посланное ПК3, возникает соответствие между MAC-адресом 00-01-33-33-33-33 и портом 0/0/12, которое добавляется в таблицу MAC-адресов.
4. Теперь в таблице MAC-адресов имеется два динамических члена — соответствие MAC-адреса 00-01-11-11-11-11 — порту 0/0/5 и 00-01-33-33-33-33 — порту 0/0/12.
5. После сеанса связи между ПК 1 и ПК 3 коммутатор не принимает каких-либо сообщений от ПК1 и ПК3. Соответствия MAC-адресов в таблице по прошествии 300 секунд удаляются. 300 секунд, фигурирующие в этом примере, являются временем жизни MAC-адреса, которое выбирается коммутатором по умолчанию. Время жизни MAC-адреса, используемое коммутатором, можно изменить.

12.1.2 Передача или фильтрация кадров

Коммутатор будет передавать или фильтровать принятые кадры данных на основе соответствий, имеющихся в таблице MAC-адресов. Используем пример, приведенный выше (Рис. 2-1). Предположим, что коммутатор обучился адресам компьютеров ПК1 и ПК3, а пользователь вручную настроил соответствие MAC-адресов портам для компьютеров ПК2 и ПК4. Таблица MAC-адресов коммутатора будет такой:

MAC-адрес	Номер порта	Соответствие добавлено при:
00-01-11-11-11-11	0/0/5	динамическом обучении
00-01-22-22-22-22	0/0/5	статической настройке
00-01-33-33-33-33	0/0/12	динамическом обучении
00-01-44-44-44-44	0/0/12	статической настройке

Передача данных в соответствии с таблицей MAC-адресов

Если ПК1 пошлет сообщение на ПК3, коммутатор передаст принятые данные из порта 12 в порт 5.

Фильтрация данных выполняется в соответствии с таблицей MAC-адресов

Если ПК1 пошлет сообщение на ПК2, коммутатор, проверив таблицу MAC-адресов, обнаружит, что ПК2 и ПК1 находятся в одном и том же физическом сегменте и отфильтрует сообщение (то есть отбросит его).

Коммутатор может продвигать кадры трех типов:

Если ПК1 пошлет сообщение на ПК2, коммутатор, проверив таблицу MAC-адресов, обнаружит, что ПК2 и ПК1 находятся в одном и том же физическом сегменте и отфильтрует сообщение (то есть отбросит его).

Коммутатор может продвигать кадры трех типов:

- Broadcast-кадры
- Multicast-кадры
- Unicast-кадры

Ниже рассмотрено, как коммутатор обращается с кадрами этих типов.

1. Broadcast-кадры. Коммутатор может разделять коллизионные домены, если только это не Broadcast-домены. Если VLAN не задана, все устройства, подключенные к коммутатору, будут принадлежать одному и тому же Broadcast-домену. Когда коммутатор принимает Broadcast-кадр, он передает его во все порты. Когда на коммутаторе сконфигурированы VLAN, таблица MAC-адресов будет изменена в соответствии с добавленной информацией VLAN. В этом случае коммутатор не будет передавать принятые Broadcast-кадры во все порты, он будет передавать их во все порты одной и той же VLAN.
2. Multicast-кадры. Когда функция IGMP Snooping не включена, Multicast-кадры будут обрабатываться так же, как Broadcast-кадры. Когда функция IGMP Snooping включена, коммутатор будет передавать Broadcast-кадры только в порты, принадлежащие единственной группе.
3. Unicast-кадры. Когда VLAN не сконфигурирована: если MAC-адрес назначения присутствует в таблице MAC-адресов коммутатора, коммутатор будет непосредственно передавать кадры в соответствующие порты; если MAC-адрес

назначения Unicast-кадра не найден в таблице MAC-адресов, коммутатор будет осуществлять вещание Unicast-кадра. Когда виртуальные сети VLAN сконфигурированы: коммутатор будет передавать Unicast-кадр в пределах одной и той же VLAN. Если MAC-адрес назначения найден в таблице MAC-адресов, но принадлежит разным VLAN, коммутатор может только вещать Unicast-кадр в VLAN, которой он принадлежит.

12.2 Последовательность настройки таблицы Mac-адресов

1. Настройка времени жизни MAC-адресов
2. Настройка передачи статических MAC-адресов или фильтрация кадров

1. Настройка времени жизни MAC-адресов

Команда	Описание
Глобальный режим конфигурирования	
mac-address-table aging-time <**0** | **aging-time**> **no mac-address-table aging-time**	Настройка времени жизни MAC-адресов

2. Настройка передачи статических MAC-адресов или фильтрация кадров

Команда	Описание
Глобальный режим конфигурирования	
mac-address-table {**static** | **blackhole**} **address** <mac-addr> vlan <vlan-id > [**interface** [**ethernet** | **portchannel**] <interface-name>] | [**source**|**destination**|**both**] **no mac-addbress-table** {**static** | **blackhole** | **dynamic**} [**address** <mac-addr>] [**vlan** <vlan-id>] [**interface** [**ethernet** | **portchannel**] <interface-name>]	Позволяет настроить передачу статических MAC-адресов или фильтрацию кадров

12.3 Примеры типичной настройки

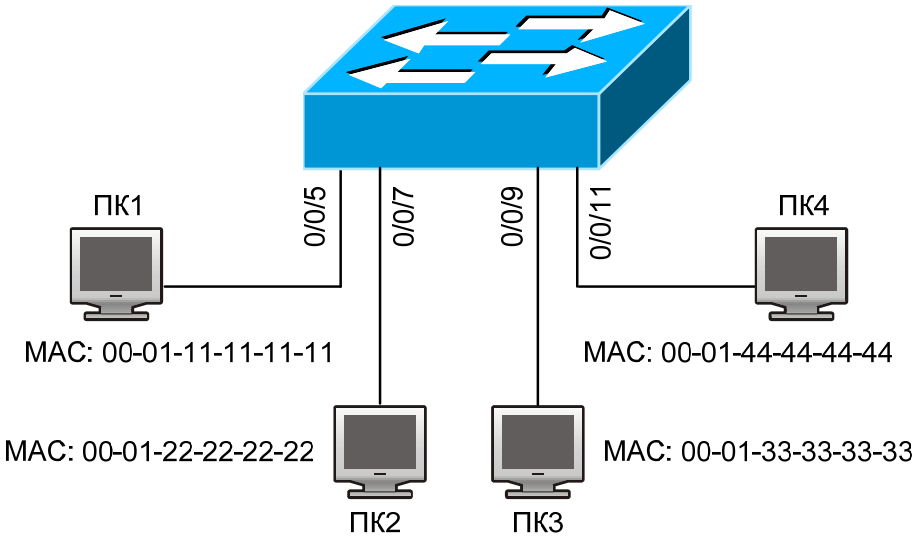

Рис. 30. Пример типичной настройки таблицы MAC-адресов

Пример:

Четыре компьютера, показанные Рис. 30, присоединены к портам 0/0/5, 0/0/7, 0/0/9, 0/0/11 коммутатора; по умолчанию все ПК принадлежат VLAN1. В соответствии с требованиями к сети, включено обучение динамическим адресам. На ПК1 хранятся данные и к нему нет доступа с остальных ПК, принадлежащих другому физическому сегменту; для ПК2 и ПК3 используются статические адреса, привязывающие их соответственно к портам 7 и 9.

Процедура настройки:

Установим на ПК1 MAC-адрес 00-01-11-11-11-11, как фильтрующий.
Switch(config)#mac-address-table static 00-01-11-11-11-11 discard vlan 1.
Зададим статическую связь ПК2 и ПК3 с портами 7 и 9 соответственно.
Switch(config)#mac-address-table static 00-01-22-22-22-22 interface ethernet 0/0/7 vlan 1

Switch(config)#mac-address-table static 00-01-33-33-33-33 interface ethernet 0/0/9 vlan 1

12.4 Устранение неполадок с таблицей MAC-адресов

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

- Поврежден соединительный кабель.
- Включен протокол Spanning Tree и порт имеет состояние «блокирован», либо устройство подключено к порту, но в это время производятся вычисления протокола Spanning Tree — после окончания вычислений порт обучится MAC-адресу.
- Если вышеперечисленные проблемы отсутствуют, проверьте порт коммутатора и обратитесь для поиска решения в службу технической поддержки.

12.5 Более сложные функции работы с MAC-адресами

12.5.1 Привязка MAC-адресов

12.5.1.1 Начальные сведения о привязке MAC-адресов

Большинство коммутаторов поддерживают обучение MAC-адресам, каждый порт может динамически обучаться некоторым MAC-адресам, поэтому потоки данных продвигаются между известными MAC-адресами, для которых порты являются достижимыми. Если MAC-адрес устарел, пакет, ему предназначавшийся, будет направляться во все порты. Другими словами, MAC-адрес, которому обучился порт, будет использоваться для передачи пакетов к этому порту. Если соединение переключено на другой порт, коммутатор снова выполнит обучение MAC-адресу и будет передавать данные новому порту.

Однако в некоторых случаях, правила безопасности или управления могут требовать ограничения MAC-адресов, при этом в порты могут передаваться данные только от привязанных к ним MAC-адресов. После того, как MAC-адрес привязан к порту, от этого порта могут поступать только потоки данных, предназначенные для этого MAC-адреса; потоки данных, предназначенные для других MAC-адресов, не привязанных к порту, не будут проходить через порт.

12.5.1.2 Последовательность настройки привязки MAC-адресов

1. Включить функцию привязки MAC-адресов к портам
2. Закрепить MAC-адреса за портом
3. Настроить свойства привязок MAC-адресов

1. Включить функцию привязки MAC-адресов к портам

Команда	Описание
Режим настройки интерфейсов	
switchport port-security **no switchport port-security**	Включает функцию привязки MAC-адресов и блокирует порт. Когда порт блокирован, функция обучения MAC-адресам не работает. Отмена команды: no switchport port-security выключает функцию привязки MAC-адресов и восстанавливает обучение MAC-адресам на порту

2. Закрепить MAC-адреса за портом

Команда	Описание
Режим настройки интерфейсов	
switchport port-security lock **no switchport port-security lock**	Блокирует порт. После того как порт блокирован, обучение MAC-адресам невозможно. Отмена команды: “no switchport port-security lock” восстанавливает обучение MAC-адресам
switchport port-security convert	Преобразует безопасные динамические MAC-адреса, которым обучился порт, в безопасные статические MAC-адреса
switchport port-security timeout <value> **no switchport port-security timeout**	Включает функцию таймера блокирования порта; команда “no switchport port-security timeout”восстанавливает настройки, используемые по умолчанию

switchport port-security mac-address <mac-address> **no switchport port-security mac-address** <mac-address>	Добавляет безопасный статический MAC-адрес; команда “no switchport port-security mac-address” удаляет безопасный статический MAC-адрес
Привилегированный режим	
clear port-security dynamic [**address** <mac-addr> | **interface** <interface-id>]	Для указанного порта очищает динамические MAC-адреса, полученные обучением

3. Настроить свойства привязок MAC-адресов

Команда	Описание
Режим настройки интерфейсов	
switchport port-security maximum <value> **no switchport port-security maximum** <value>	Задает максимальное число безопасных MAC-адресов для порта; Отмена команды: “no switchport port-security maximum” восстанавливает значение, используемое по умолчанию
switchport port-security violation {**protect** | **shutdown**} **no switchport port-security violation**	Устанавливает для порта режим запрета; команда “no switchport port-security violation” восстанавливает настройки, используемые по умолчанию

12.5.1.3 Устранение неполадок привязки MAC-адресов

Включение привязки MAC-адресов к портам может закончиться неудачей по многим причинам: Ниже перечислены некоторые возможные причины и способу разрешения проблем:

- Если привязку MAC-адресов для порта включить не удается, удостоверьтесь в том, что: порт не участвует в работе протокола Spanning tree; не используется агрегация порта; порт не используется, как магистральный. Привязка MAC-адресов исключает такие настройки. Если привязка MAC-адресов включена, вышеперечисленные функции должны быть до этого выключены.
- Если безопасный адрес задан как статический и затем удален, этот безопасный адрес не удастся использовать, хотя он и будет существовать. По этой причине рекомендуется избегать назначения статических адресов портам, для которых включена привязка MAC-адресов.

13 Настройка протокола MSTP

13.1 Начальные сведения о протоколе MSTP

Протокол MSTP (Multiple STP) — это новый протокол spanning-tree, основанный на протоколах STP и RSTP. Он работает на любых коммутаторах локальных сетей. При работе этого протокола в локальной сети с коммутаторами, использующими протоколы MSTP, RSTP, STP вычисляется общее внутреннее связующее дерево (CIST — common and internal spanning tree). Кроме того, вычисляются независимые экземпляры множества связующих деревьев (MSTI — multiple spanning-tree instances) для каждой области MST (области MSTP). В MSTP используется адаптированная версия протокола RSTP, обеспечивающего быструю сходимость при построении связующего дерева, при этом одному и тому же экземпляру связующего дерева может быть сопоставлено множество сетей VLAN. Этот экземпляр связующего дерева является полностью независимым от других экземпляров связующего дерева. Протокол MSTP обеспечивает множество маршрутов трафика данных и балансировку нагрузки. Благодаря тому, что множество VLAN совместно используют один и тот же экземпляр связующего дерева, при работе MSTP можно снизить число экземпляров связующих деревьев. В результате потребляется меньше вычислительных ресурсов, снижаются требования к пропускной способности.

13.1.1 Регион MSTP

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

Регион MSTP содержит один или несколько коммутаторов с одним и тем же идентификатором MCID (MST Configuration Identification) и локальную сеть с коммутаторами (конкретный коммутатор в регионе MSTP является коммутатором назначения локальной сети, на коммутаторах, закрепленных за локальной сетью, протокол STP не работает). Все коммутаторы одного и того же региона MSTP имеют одинаковые идентификаторы MCID.

MCID имеет три атрибута:

- Имя конфигурации: Содержит буквы и цифры
- Номер версии
- Краткое описание конфигурирования: Сети VLAN, соответствующие экземплярам связующего дерева

Коммутаторы, у которых эти атрибуты одинаковы, считаются принадлежащими одному и тому же региону MST.

Когда протокол MSTP вычисляет CIST в локальной сети с коммутаторами, регион MSTP рассматривается, как коммутатор (Рис. 31):

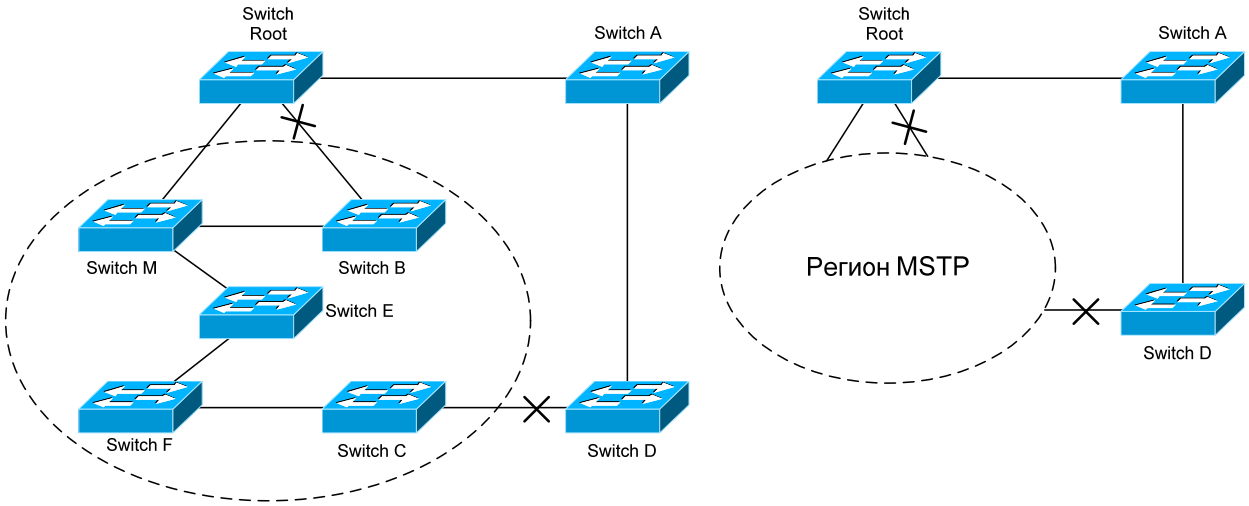

Рис. 31. CIST и регион MST

В сети, приведенной на Рис. 31, если в одном коммутаторе используется STP, а в другом RSTP, то порт между коммутатором M и коммутатором B должен быть блокирован. Однако, если в коммутаторах области, выделенной пунктиром, используется MSTP и сконфигурирован один и тот

же регион MST, то протокол MSTP будет считать этот регион коммутатором. Поэтому блокирован один порт между коммутатором B и корневым узлом; кроме того, блокирован один порт коммутатора D.

13.1.1.1 Операции внутри одного и того же региона MSTP

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

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

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

Все экземпляры MST одного и того же региона совместно используют одни и те же таймеры протокола, однако каждый экземпляр MST имеет свои собственные параметры топологии, например ID корневого коммутатора, метрику маршрута к корневому узлу и т. д.

13.1.1.2 Операции между регионами MST

Если в сети имеется множество регионов, либо в ней уже существуют коммутаторы 802.1D, MSTP создает и обслуживает дерево CST, которое содержит все регионы MST и все существующие коммутаторы с STP в сети. Для преобразования в дерево CST экземпляры MST комбинируются с IST на границе региона.

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

13.1.2 Роли портов

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

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

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

13.1.3 Балансировка нагрузки MSTP

В регионе MSTP сети VLAN могут быть привязаны к различным экземплярам. Благодаря этому, можно создавать различные топологии. Все экземпляры независимы, таким образом, каждый из них может иметь присущие только ему атрибуты, например, приоритет коммутатора, метрику порта и т. п.

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

13.2 Последовательность настройки MSTP

Последовательность настройки MSTP:

1. Включение протокола MSTP, установка режима работы
2. Настройка параметров экземпляров связующего дерева
3. Настройка параметров регионов MSTP

4. Настройка временных параметров MSTP
5. Настройка функции быстрой миграции MSTP
6. Настройка формата пакетов порта
7. Настройка атрибутов связующего дерева порта
8. Настройка атрибутов snooping-ключа аутентификации
9. Настройка режима FLUSH для изменений топологии

1. Включение протокола MSTP, установка режима работы

Команда	Описание
Глобальный режим конфигурирования, режим настройки интерфейсов	
spanning-tree **no spanning-tree**	Включает протокол MSTP или выключает его
Глобальный режим конфигурирования	
spanning-tree mode {**mstp**|**stp**|**rstp**} **no spanning-tree mode**	Позволяет установить режим работы MSTP
Режим настройки интерфейсов	
spanning-tree mcheck	Принудительно устанавливает для порта режим работы по протоколу MSTP

2. Настройка параметров экземпляров связующего дерева

Команда	Описание
Глобальный режим конфигурирования	
spanning-tree mst <instance-id> **priority** <bridge-priority> **no spanning-tree mst** <instance-id> **priority**	Позволяет задать приоритет коммутатора для указанного экземпляра связующего дерева
spanning-tree priority <bridge-priority> **no spanning-tree priority**	Позволяет настроить приоритет связующего дерева на коммутаторе
Режим настройки интерфейсов	
spanning-tree mst <instance-id> **cost** <cost> **no spanning-tree mst** <instance-id> **cost**	Для указанного экземпляра связующего дерева позволяет установить метрику маршрута к порту
spanning-tree mst <instance-id> **port-priority** <port-priority> **no spanning-tree mst** <instance-id> **port-priority**	Позволяет задать приоритет порта для указанного экземпляра связующего дерева
spanning-tree mst <instance-id> **rootguard** **no spanning-tree mst** <instance-id> **rootguard**	Для указанного экземпляра связующего дерева позволяет задать защищенный корневой узел. Порты, для которых установлена защита, не могут быть преобразованы в корневые порты других типов
spanning-tree rootguard **no spanning-tree rootguard**	Для текущего порта задает режим защищенного корневого порта в экземпляре связующего дерева 0. Сконфигурированный защищенный порт не может быть преобразован в корневой порт других типов

3. Настройка параметров регионов MSTP

Команда	Описание
Глобальный режим конфигурирования	
spanning-tree mst configuration **no spanning-tree mst configuration**	Позволяет войти в режим настройки регионов MSTP. Отмена команды: “ no spanning-tree mst configuration” восстанавливает настройки, используемые по умолчанию
Режим настройки регионов MSTP	
show	Выводит на дисплей информацию о работающей в данный момент системе
instance <instance-id> **vlan** <vlan-list> **no instance** <instance-id> [**vlan** <vlan-list>]	Позволяет создать экземпляр связующего дерева и установить соответствие между VLAN и этим экземпляром
name <name> **no name**	Позволяет задать имя региона MSTP

revision-level <level> **no revision-level**	Позволяет задать номер ревизии конфигурирования региона MSTP
abort	Позволяет выйти из режима настройки регионов MSTP и вернуться в глобальный режим конфигурирования без сохранения сделанных настроек региона MSTP
exit	Позволяет сохранить сделанные настройкм региона MSTP, выйти из режима настройки регионов MSTP и вернуться в глобальный режим конфигурирования
no	Отменяет команду или устанавливает начальное значение

4. Настройка временных параметров MSTP

Команда	Описание
Глобальный режим конфигурирования	
spanning-tree forward-time <time> **no spanning-tree forward-time**	Позволяет задать время задержки передачи на коммутаторе
spanning-tree hello-time <time> **no spanning-tree hello-time**	Позволяет задать время Hello при отправке сообщений BPDU
spanning-tree maxage <time> **no spanning-tree maxage**	Позволяет установить срок жизни сообщений BPDU
spanning-tree max-hop <hop-count> **no spanning-tree max-hop**	Позволяет задать максимальное число хопов для сообщений BPDU в регионе MSTP

5. Настройка функции быстрой миграции MSTP

Команда	Описание
Режим настройки интерфейсов	
spanning-tree link-type p2p {**auto** | **force-true** | **force-false**} **no spanning-tree link-type**	Позволяет задать тип линии порта
spanning-tree portfast [**bpdufilter** | **bpduguard**] **no spanning-tree portfast**	Позволяет задать порт, как граничный. Опция Bpdufilter служит для отбрасывания принятых сообщений BPDU. Опция bpduguard при приеме сообщения BPDU закрывает порт. Отмена команды: “ no spanning-tree portfast “ выключает режим пограничного порта, происходит преобразование в порт, который не находится на границе

6. Настройка формата пакетов порта

Команда	Описание
Режим настройки интерфейсов	
spanning-tree format standard **spanning-tree format privacyspanning-tree format auto** **no spanning-tree format**	Позволяет настроить формат пакета связующего дерева порта. При выборе опции standard пакет соответствует стандартам IEEE, при опции privacy пакет совместим с CISCO, auto означает, что формат определяется по принятому пакету

7. Настройка атрибутов связующего дерева порта

Команда	Описание
Режим настройки интерфейсов	
spanning-tree cost	Позволяет задать метрику маршрута к порту
spanning-tree port-priority	Позволяет задать приоритет порта
spanning-tree rootguard	Позволяет установить порт, как не корневой

8. Настройка атрибутов snooping-ключа аутентификации

Команда	Описание
Режим настройки интерфейсов	
spanning-tree digest-snooping **no spanning-tree digest-snooping**	Позволяет порту использовать строку аутентификации партнерского порта. Отмена команды: “no spanning-tree digest-snooping” восстанавливает использование генерированной строки

9. Настройка режима FLUSH для изменений топологии

Команда	Описание
Глобальный режим конфигурирования	
spanning-tree tcflush enable **spanning-tree tcflush disable** **spanning-tree tcflush protect** **no spanning-tree tcflush**	Enable: Связующее дерево строится сразу, как только изменяется топология. Disable: При изменении топологии связующее дерево не строится. Protect: связующее дерево строится через каждые 10 секунд. Отмена команды: “no spanning-tree tcflush” восстанавливает настройку enable, используемую по умолчанию
Режим настройки интерфейсов	
spanning-tree tcflush enable **spanning-tree tcflush disable** **spanning-tree tcflush protect** **no spanning-tree tcflush**	Позволяет настроить режим flush для порта. Отмена команды: “no spanning-tree tcflush” восстанавливает настройки режима flush, заданные в режиме глобального конфигурирования

13.3 Пример применения MSTP

На Рис. 32 приведен типичный сценарий применения протокола MSTP.

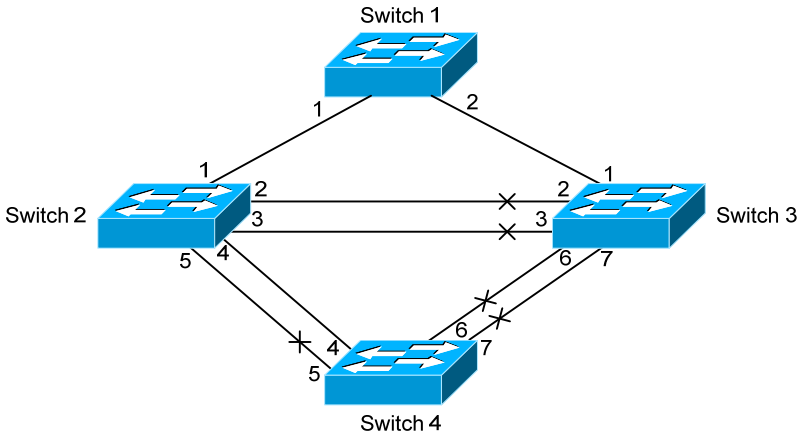

Рис. 32. Типичный сценарий применения протокола MSTP

Соединения между коммутаторами показаны на рисунке выше. Все коммутаторы по умолчанию работают в режиме MSTP, установлены приоритет порта и метрика маршрута к порту, используемые по умолчанию. Параметры коммутаторов, используемые по умолчанию, приведены в таблице:

Имя коммутатора		Switch1	Switch2	Switch3	Switch4
MAC-адрес коммутатора		…00-00-01	…00-00-02	…00-00-03	…00-00-04
Приоритет коммутатора		32768	32768	32768	32768
Приоритет порта	Порт 1	128	128	128	
	Порт 2	128	128	128	
	Порт 3		128	128	
	Порт 4		128		128
	Порт 5		128		128
	Порт 6			128	128
	Порт 7			128	128
Метрика маршрута	Порт 1	200000	200000	200000	
	Порт 2	200000	200000	200000	
	Порт 3		200000	200000	
	Порт 4		200000		200000
	Порт 5		200000		200000
	Порт 6			200000	200000
	Порт 7			200000	200000

По умолчанию протокол MSTP создает топологию дерева с корнем на коммутаторе 1. Порты, обозначенные “x” имеют состояние discarding (блокированы), на остальных портах передача разрешена.

Этапы настройки:

Шаг 1:

Настройка привязки VLAN к порту:

Создать VLAN 20, 30, 40, 50 на Switch 2, Switch 3 и Switch 4.

Установить порты 1-7 как магистральные на Switch 2, Switch 3 и Switch 4.

Шаг 2:

Установка Switch 2, Switch 3 и Switch 4, как принадлежащих одному и тому же дереву MSTP:

Установка для Switch 2, Switch 3 и Switch 4 одного и того же имени региона, совпадающего с именем дерева mstp. Привязка VLAN 20 и VLAN 30 в Switch 2, Switch 3 и Switch 4 к экземпляру связующего дерева 3; привязка VLAN 40 и VLAN 50 в Switch 2, Switch 3 и Switch 4 к экземпляру связующего дерева 4.

Шаг 3:

Установка Switch 3 как корневого коммутатора для экземпляра связующего дерева 3; установка Switch 4 как корневого коммутатора для экземпляра связующего дерева 4.

Установка приоритета коммутатора 0 для экземпляра связующего дерева 3 на Switch 3.

Установка приоритета коммутатора 0 для экземпляра связующего дерева 4 на Switch 4.

Ниже процедура настройки приведена подробно:

На Switch 2:

```
Switch2(config)#vlan 20
Switch2(config-vlan20)#exit
Switch2(config)#vlan 30
Switch2(config-vlan30)#exit
Switch2(config)#vlan 40
Switch2(config-vlan40)#exit
Switch2(config)#vlan 50
Switch2(config-vlan50)#exit
Switch2(config)#spanning-tree mst configuration
Switch2(config-mstp-region)#name mstp
Switch2(config-mstp-region)#instance 3 vlan 20;30
Switch2(config-mstp-region)#instance 4 vlan 40;50
Switch2(config-mstp-region)#exit
Switch2(config)#interface e0/0/1-7
Switch2(config-port-range)#switchport mode trunk
Switch2(config-port-range)#exit
Switch2(config)#spanning-tree
```

На Switch 3:

```
Switch3(config)#vlan 20
Switch3(config-vlan20)#exit
Switch3(config)#vlan 30
Switch3(config-vlan30)#exit
Switch3(config)#vlan 40
Switch3(config-vlan40)#exit
Switch3(config)#vlan 50
Switch3(config-vlan50)#exit
Switch3(config)#spanning-tree mst configuration
Switch3(config-mstp-region)#name mstp
Switch3(config-mstp-region)#instance 3 vlan 20;30
Switch3(config-mstp-region)#instance 4 vlan 40;50
Switch3(config-mstp-region)#exit
Switch3(config)#interface e0/0/1-7
Switch3(config-port-range)#switchport mode trunk
Switch3(config-port-range)#exit
Switch3(config)#spanning-tree
Switch3(config)#spanning-tree mst 3 priority 0
```

На Switch 4:

```
Switch4(config)#vlan 20
Switch4(config-vlan20)#exit
Switch4(config)#vlan 30
```

```
Switch4(config-vlan30)#exit
Switch4(config)#vlan 40
Switch4(config-vlan40)#exit
Switch4(config)#vlan 50
Switch4(config-vlan50)#exit
Switch4(config)#spanning-tree mst configuration
Switch4(config-mstp-region)#name mstp
Switch4(config-mstp-region)#instance 3 vlan 20;30
Switch4(config-mstp-region)#instance 4 vlan 40;50
Switch4(config-mstp-region)#exit
Switch4(config)#interface e0/0/1-7
Switch4(config-port-range)#switchport mode trunk
Switch4(config-port-range)#exit
Switch4(config)#spanning-tree
Switch4(config)#spanning-tree mst 4 priority 0
```

После настройки описанной выше, Switch 1 будет корневым коммутатором экземпляра связующего дерева 0 во всей сети. В регионе MSTP, которому принадлежат Switch 2, Switch 3 и Switch 4: Switch 2 является корневым узлом региона для экземпляра связующего дерева 0, Switch 3 является корневым узлом региона для экземпляра связующего дерева 3, Switch 4 является корневым узлом региона для экземпляра связующего дерева 4.

Трафик VLAN 20 и VLAN 30 посылается через топологию экземпляра связующего дерева 3.

Трафик VLAN 40 и VLAN 50 посылается через топологию экземпляра связующего дерева 4.

Трафик остальных VLAN посылается через топологию экземпляра связующего дерева 0.

Порт 1 на Switch 2 является управляющим портом экземпляров связующих деревьев 3 и 4.

Протокол MSTP путем вычислений генерирует 3 топологии: экземпляров связующих деревьев 0, 3 и 4 (обозначены линиями синего цвета). Порты, обозначенные “x” имеют состояние discarding (блокированы). На остальных портах передача разрешена. Так как экземпляры связующих деревьев 3 и 4 корректны только в регионе MSTP, на Рис. 33 — Рис. 35 показана только топология региона MSTP.

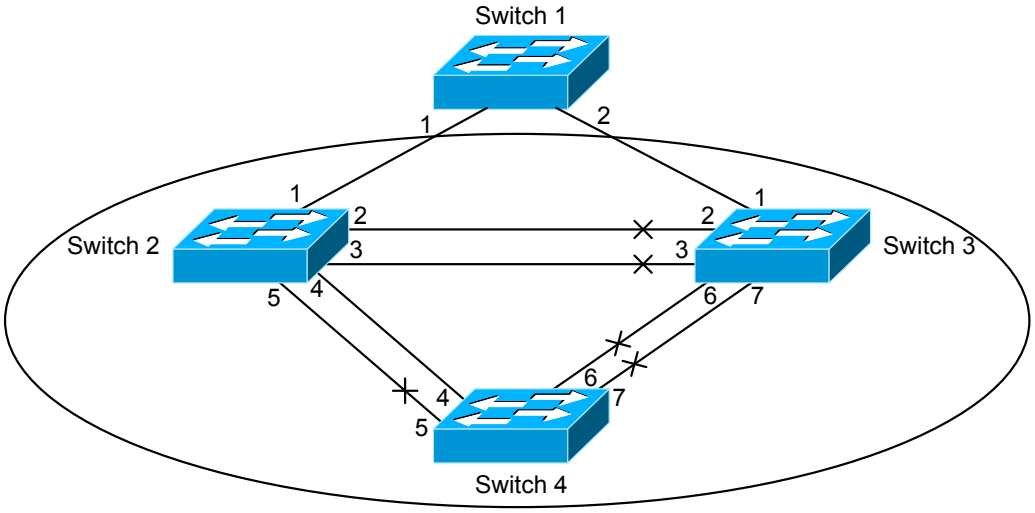

Рис. 33. Топология экземпляра связующего дерева 0, вычисленная протоколом MSTP

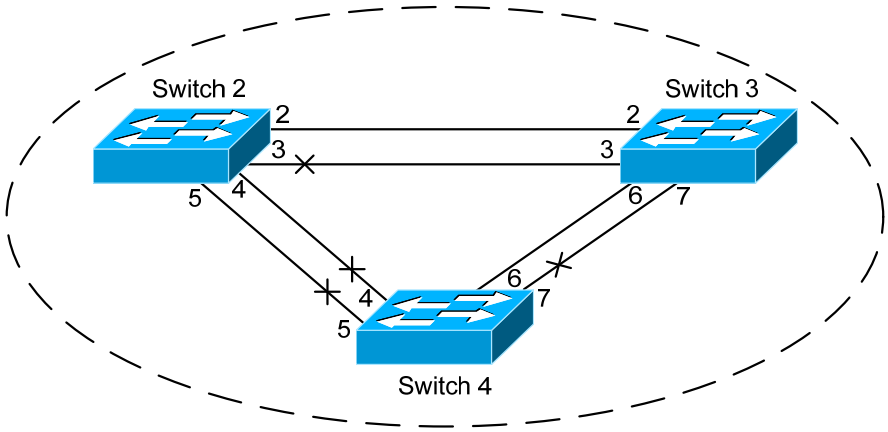

Рис. 34. Топология экземпляра связующего дерева 3, вычисленная протоколом MSTP

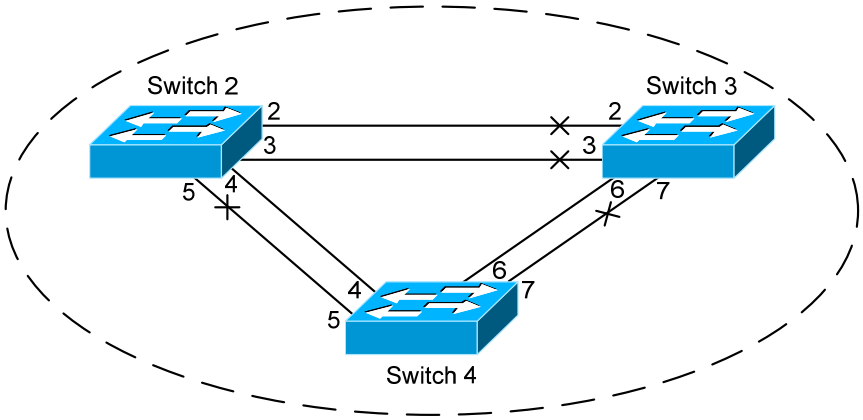

Рис. 35. Топология экземпляра связующего дерева 4, вычисленная протоколом MSTP

13.4 Устранение неполадок протокола MSTP

Для того чтобы протокол MSTP в порте смог работать, MSTP должен быть включен в глобальном режиме конфигурирования. Если MSTP не включен в глобальном режиме конфигурирования, он не будет работать в порту.

Параметры MSTP являются взаимосвязанными, они должны удовлетворять соотношениям, приведенным ниже. В противном случае, протокол MSTP может работать неправильно.2 × (Задержка_передачи_коммутатора – 1,0 секунда) >= Максимальный_срок_жизни_адреса_коммутатора

Максимальный_срок_жизни_адреса_коммутатора >= 2 x (Задержка_Hello_коммутатора + 1,0 секунда)

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

14 Настройка уровня 3

Коммутатор поддерживает функции передачи пакетов только на уровне 2. Однако возможна настройка порта управления уровня 3. В интерфейсе этого порта можно задать IP-адреса, используемые для связи с различными протоколами на основе IP.

14.1 Интерфейс уровня 3

14.1.1 Начальные сведения об интерфейсе уровня 3

В коммутаторах может быть создан интерфейс уровня 3. Он является не физическим, а виртуальным. Интерфейс уровня 3 строится на интерфейсе VLAN. Интерфейс уровня 3 может содержать один или более интерфейсов уровня 2, принадлежащих одному и тому же VLAN, либо не содержать интерфейсов уровня 2. По крайней мере, один из интерфейсов уровня 2, содержащихся в интерфейсе уровня 3, должен быть включен (находиться в состоянии UP) — тогда будет включен и интерфейс уровня 3. В противном случае интерфейс уровня 3 будет выключен (будет находиться в состоянии DOWN). Все интерфейсы уровня 3 коммутатора используют один и тот же MAC-адрес, который выбирается из числа резервированных при создании интерфейса уровня 3 MAC-адресов. Интерфейс уровня 3 является основой для работы протоколов уровня 3. Коммутатор может использовать набор IP-адресов, заданный на уровне 3 для связи с другими устройствами по IP-протоколу. Коммутатор может передавать IP-пакеты между различными интерфейсами уровня 3. Интерфейс петли — это интерфейс уровня 3.

14.1.2 Настройка интерфейса уровня 3

Последовательность настройки интерфейса уровня 3:

1. Создание интерфейса уровня 3
2. Включает или выключает интерфейс VLAN

1. Создание интерфейса уровня 3

Команда	Описание
Глобальный режим конфигурирования	
interface vlan <vlan-id> **no interface vlan** <vlan-id>	Позволяет создать интерфейс VLAN (этот интерфейс является интерфейсом уровня 3). Отмена команды: “no interface vlan <vlan-id>” удаляет интерфейс VLAN (интерфейс уровня 3), созданный в коммутаторе

2. Открытие или закрытие интерфейса VLAN

Команда	Описание
Режим настройки интерфейса VLAN	
shutdown **no shutdown**	Включает или выключает интерфейс VLAN

14.2 Настройка протокола IP

14.2.1 Начальные сведения о протоколах IPv4, IPv6

IPv4 — это текущая версия универсального Интернет-протокола. Практика показала, что протокол IPv4 является простым, гибким, открытым, стабильным, мощным и легким в реализации протоколом. Он обладает хорошей совместимостью с протоколами верхних и нижних уровней. Хотя протокол IPv4 почти не менялся с момента его появления в 80-х годах, он продолжает распространяться по всему миру вместе с распространением Интернет. Однако по мере роста инфраструктуры Интернет и услуг, использующих Интернет-приложения, выявляются и некоторые недостатки протокола IPv4, связанные с масштабом и сложностью сегодняшней Интернет.

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

Наиболее важная проблема, которая решена в IPv6 — это добавление достаточного количества IP-адресов. Запас адресов IPv4 почти исчерпан, в то время как число пользователей Интернет растет в геометрической прогрессии. Объемы предоставляемых Интернет-услуг и число

прикладных устройств продолжают расти опережающими темпами (домашние и малые офисные сети, IP-телефония, терминалы беспроводного информационного обслуживания, использующие Интернет и т. д.). В результате требуется все большее количество IP-адресов, предоставлять которые становится все более затруднительно. Работа по преодолению нехватки IPv4-адресов велась долгое время; были предложены различные технологии, позволяющие продлить срок эксплуатации существующей IPv4-инфраструктуры, в том числе трансляция сетевых адресов NAT (Network Address Translation), технология CIDR (Classless Inter-Domain Routing) и т. д.

Хотя совместное использование технологий CIDR, NAT и частной адресации на какое-то время решает проблему нехватки IPv4-адресов, технология NAT использует плохо подходящую для сквозной работы модель, ведь в самом начале IP-протокол разрабатывался для устройств маршрутизации, обслуживавших промежуточные узлы сети и поддерживавших состояние каждого соединения, что значительно увеличивало задержку в сети и снижало производительность сети. Более того, трансляция адресов пакетов данных в сети сводила на нет работу системы безопасности, использовавшей сквозные проверки сети. Ярким примером этого может служить заголовок аутентификации IPSec.

Для преодоления всех проблем, связанных с современным использованием IPv4, IETF был разработан Интернет-протокол следующего поколения — IPv6, который к настоящему времени стал единственным приемлемым решением.

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 обеспечивает агрегацию маршрутов, значительно снижает число ячеек в таблице маршрутизации, повышает эффективность и расширяемость маршрутизации и обработки пакетных 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 адресов и самонастройка plug-and-play. Большое число хостов сможет легко обнаруживать маршрутизаторы по адресам, автоматически сконфигурированным функцией IPv6, а автоматическое получение глобально-уникальных адресов IPv6 позволит устройствам использовать технологию plug-and-play по протоколу IPv6. Функция автоматической настройки адреса упрощает и переадресацию существующей сети, делает ее удобнее. Для операторов сети функция автоматической настройки адреса делает удобнее переход от одного сервис-провайдера к другому.

Поддержка IPSec. IPSec является опцией для IPv4 и требуется обязательно в протоколе IPv6. IPv6 обеспечивает безопасный расширенный заголовок, который поддерживает сквозные (end-to-end) услуги безопасности, например, управление доступом, конфиденциальность, контроль целостности данных и вследствие этого упрощает реализацию криптозащиты, проверку достоверности и виртуальные частные сети.

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 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 изьежать 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.

Поддерживается широко используемый протокол маршрутизации. IPv6 поддерживает и расширяет поддержку существующих протоколов IGP (Internal Gateway Protocol) и протоколов EGP (Exterior Gateway Protocols). Например, IPv6 поддерживает такие протоколы IPv6-маршрутизации, как RIPng, OSPFv3, IS-ISv6, MBGP4+ и т. д.

Увеличено число групповых адресов, улучшена поддержка групповой рассылки. Что касается broadcast-функций IPv4, таких как Router Discovery и Router Query, то IPv6-функции для группового трафика полностью заменяют их. При групповых рассылках не только экономится пропускная способность сети, улучшается также и производительность ее работы.

14.2.2 Настройка IP-протокола

Интерфейс уровня 3 можно сконфигурировать как интерфейс IPv4, либо как интерфейс IPv6.

14.2.2.1 Настройка адреса IPv4

Последовательность настройки адреса IPv4:

1. Настройка адреса IPv4 интерфейса уровня 3

1. Настройка адреса IPv4 интерфейса уровня 3

Команда	Описание
Режим настройки интерфейсов VLAN	
ip address <ip-address> <mask> [**secondary**] **no ip address** [<ip-address> <mask>]	Позволяет настроить IP-адрес интерфейса VLAN; команда “no ip address [<ip-address> <mask>]” удаляет IP-адрес интерфейса VLAN

14.2.2.2 Настройка адреса IPv6

Последовательность настройки адреса IPv6:

Основная настройка протокола IPv6

- Включение IPv6 в глобальном режиме конфигурирования
- Настройка IPv6-адреса интерфейса

1. Настройка обнаружения соседних устройств IPv6
   - Настройка числа сообщений запросов соседнего устройства DAD
   - Настройка интервалов отправки сообщений запросов соседнего устройства DAD
   - Настройка статических IPv6-адресов соседних устройств
   - Удаление содержимого всех ячеек таблицы соседних устройств IPv6

Основная настройка протокола IPv6

- Включение IPv6 в глобальном режиме конфигурирования

Команда	Описание
Глобальный режим конфигурирования	
ipv6 enable **no ipv6 enable**	Включает такие функции, как передача пакетных данных IPv6, обнаружение соседних устройств, извещения маршрутизаторов, протокол маршрутизации и т. д. Отмена команды: no ipv6 enable выулючает функции IPv6

- Настройка IPv6-адреса интерфейса

Команда	Описание
Режим настройки интерфейсов	
ipv6 address <ipv6-address/prefix-length> [eui-64] **no ipv6 address** <ipv6-address/prefix-length>	Позволяет задать IPv6–адрес, в том числе глобальный адрес агрегации одноадресного трафика, адрес локального сайта и адрес локальной линии. Команда no ipv6 address <ipv6-address/prefix-length> отменяет IPv6-адрес

1. Настройка обнаружения соседних устройств IPv6
   - Настройка числа сообщений запросов соседнего устройства DAD

Команда	Описание

Режим настройки интерфейсов	
ipv6 nd dad attempts <value> **no ipv6 nd dad attempts** <value>	Позволяет задать число сообщений с запросами соседних устройств, посылаемых последовательно, когда интерфейс выполняет дублирование определения адреса. Отмена команды: no ipv6 nd dad attempts <value> восстанавливает значение, заданное по умолчанию (1)

- Настройка интервалов отправки сообщений запросов соседнего устройства DAD

Команда	Описание
Режим настройки интерфейсов	
ipv6 nd ns-interval <seconds> **no ipv6 nd ns-interval** <seconds>	Позволяет задать интервал времени отправки интерфейсом сообщений с запросами соседних устройств. Отмена команды: no ipv6 nd ns-interval <seconds> восстанавливает значение, заданное по умолчанию (1 секунда)

- Настройка статических IPv6-адресов соседних устройств

Команда	Описание
Режим настройки интерфейсов	
ipv6 neighbor <ipv6-address> <hardware-address> **interface** <interface-type interface-number> **no ipv6 neighbor** <ipv6-address>	Позволяет задать статические адреса в таблице соседних устройств, в том числе IPv6-адрес соседнего устройства, MAC-адрес и порт второго уровня. Удаляет содержимое ячеек таблицы соседних устройств

- Удаление содержимого всех ячеек таблицы соседних устройств IPv6

Команда	Описание
Привилегированный режим	
clear ipv6 neighbors	Очищает содержимое всех ячеек таблицы соседних устройств, содержащих статические адреса

14.2.3 Устранение неполадок IPv6

- Перед настройкой IPv6-команд, протокол IPv6 должен быть включен, в противном случае, конфигурирование будет неправильным.
- Время жизни маршрутизатора не должно быть меньше, чем интервал отправки извещений на маршрутизатор.
- Если подключенный компьютер ПК не получил IPv6-адрес, необходимо проверить состояние переключателя извещений RA (по умолчанию он выключен).

14.3 Протокол ARP

14.3.1 Начальные сведения об ARP

Протокол ARP (Address Resolution Protocol — протокол разрешения адресов) в основном используется для преобразования IP-адресов в Ethernet MAC-адреса. Коммутатор поддерживает как статические, так и динамические настройки ARP.

14.3.2 Последовательность настройки протокола ARP

Последовательность настройки протокола ARP:

1. Конфигурирование статических настроек ARP
2. Очистка динамических настроек ARP
3. Очистка статистической информации сообщений ARP

1. Конфигурирование статических настроек ARP

Команда	Описание
Режим настройки интерфейсов VLAN	
arp <ip_address> <mac_address> {[ethernet] <portName>} **no arp** <ip_address>	Позволяет задать статическую запись ARP. Отмена команды: “no arp <ip_address>” удаляет статическую запись ARP

2. Очистка динамических настроек ARP

Команда	Описание
Привилегированный режим	
clear arp-cache	Команда очищает кэш-память ARP, очищает текущее содержимое таблицы ARP, за исключением записей со статическими адресами

3. Очистка статистической информации сообщений ARP

Команда	Описание
Привилегированный режим	
clear arp traffic	Очищает статистическую информации сообщений ARP коммутатора

14.3.3 Устранение неполадок ARP

Если команда ping, выданная для тестирования соединения между коммутатором и напрямую подключенным сетевым устройством показывает отсутствие соединения, для выявления причин этого можно использовать следующие проверки:

- Следует проверить, обучен ли соответствующий протокол ARP коммутатором.
- Если протокол ARP не обучен, включите вывод на дисплей отладочной информации ARP и проконтролируйте условия отправки и приема пакетов ARP.
- Проверьте, исправны ли кабели — их неисправность часто приводит к проблемам с ARP, при этом может не работать и обучение ARP.

15 Защита от ARP-сканирования

15.1 Введение

ARP-сканирование является широко распространенным методом, применяемым при сетевых атаках. Для обнаружения всех активных хостов в сегменте сети, источник атаки осуществляет вещание множества ARP-сообщений, использующих большую часть пропускной способности сети. Кроме того, он может осуществить атаку для перегрузки сети, используя для этого ложные ARP-сообщения, приводящие к неработоспособности сети из-за бесполезной траты ее пропускной способности. Обычно ARP-сканирование предшествует более опасным атакам, например, автоматическому заражению вирусом, сканированию портов, сканированию для кражи информации, отправке искаженных сообщений, DOS-атаке и т. д.

Так как ARP-сканирование угрожает безопасности и стабильности работы сети, часто бывает необходимо предотвратить его. Коммутатор обеспечивает полный комплекс мер для защиты от ARP-сканирования. Если в сегменте сети обнаружен порт или хост с функциями ARP-сканирования, коммутатор отключит источник атаки, чтобы обеспечить безопасность сети.

Существует два метода защиты от ARP-сканирования: на основе портов и на основе IP-адресов. При методе защиты от ARP-сканирования на основе портов, подсчитывается число ARP-сообщений, принятых от порта в течение некоторого времени. Если это число превышает предустановленное пороговое значение, порт выключается. При методе защиты от ARP-сканирования на основе IP-адресов, подсчитывается число ARP-сообщений, принятых с IP-адреса в сегменте в течение некоторого времени. Если это число превышает предустановленное пороговое значение, весь трафик, поступающий с этого IP-адреса, блокируется, хотя порт, связанный с этим IP-адресом, выключен не будет. Эти два метода могут применяться одновременно. После того, как порт или IP-адрес блокированы, пользователи могут восстановить его состояние, используя функцию автоматического восстановления.

Для улучшения работы коммутатора пользователи могут задать безопасные порты и IP-адреса, ARP-сообщения от которых не будут проверяться коммутатором. В результате нагрузка на коммутатор может быть существенно снижена.

15.2 Последовательность настройки защиты от сканирования

Включение функции защиты от ARP-сканирования:

1. Настройка порогового значения при методах защиты от ARP-сканирования на основе портов и на основе IP-адресов.
2. Настройка безопасных портов
3. Настройка безопасных IP-адресов
4. Настройка времени автоматического восстановления
5. Вывод на дисплей отладочной и другой информации, касающейся ARP-сканирования.

Включение функции защиты от ARP-сканирования:

Команда	Описание
Глобальный режим конфигурирования	
anti-arpscan enable **no anti-arpscan enable**	Включает или выключает функцию защиты от ARP-сканирования в глобальном режиме конфигурирования

1. Настройка порогового значения при методах защиты от ARP-сканирования на основе портов и на основе IP-адресов.

Команда	Описание
Глобальный режим конфигурирования	
anti-arpscan port-based threshold <threshold-value> **no anti-arpscan port-based threshold**	Позволяет задать пороговое значение при методе предотвращения ARP-сканирования на основе портов
anti-arpscan ip-based threshold <threshold-value> **no anti-arpscan ip-based threshold**	Позволяет задать пороговое значение при методе предотвращения ARP-сканирования на основе IP-адресов

2. Настройка безопасных портов

Команда	Описание
Режим настройки интерфейсов	
anti-arpscan trust <port supertrust-port> **no anti-arpscan trust** <port supertrust-port>	Позволяет установить атрибуты безопасности портов

3. Настройка безопасных IP-адресов

Команда	Описание
Глобальный режим конфигурирования	
anti-arpscan trust ip <ip-address [<netmask>]> **no anti-arpscan trust ip** <ip-address [<netmask>]>	Позволяет задать атрибуты безопасных IP-адресов

4. Настройка времени автоматического восстановления

Команда	Описание
Глобальный режим конфигурирования	
anti-arpscan recovery enable **no anti-arpscan recovery enable**	Включает или выключает функцию автоматического восстановления
anti-arpscan recovery time <seconds> **no anti-arpscan recovery time**	Позволяет задать время автоматического восстановления

5. Вывод на дисплей отладочной и другой информации, касающейся ARP-сканирования.

Команда	Описание
Глобальный режим конфигурирования	
anti-arpscan log enable **no anti-arpscan log enable**	Позволяет включить или выключить функцию создания сообщений о защите от ARP-сканирования
anti-arpscan trap enable **no anti-arpscan trap enable**	Позволяет включить или выключить функцию SNMP Trap для защиты от ARP-сканирования
show anti-arpscan [**trust** <**ip** | **port** | **supertrust-port**> | **prohibited** <**ip** | **port**>]	Позволяет вывести на дисплей информацию о состоянии и настройках защиты от ARP-сканирования
Привилегированный режим	
debug anti-arpscan <**port** | **ip**> **no debug anti-arpscan** <**port** | **ip**>	Позволяет включить или выключить функцию создания отладочных сообщений о защите от ARP-сканирования

15.3 Примеры настройки защиты от ARP-сканирования

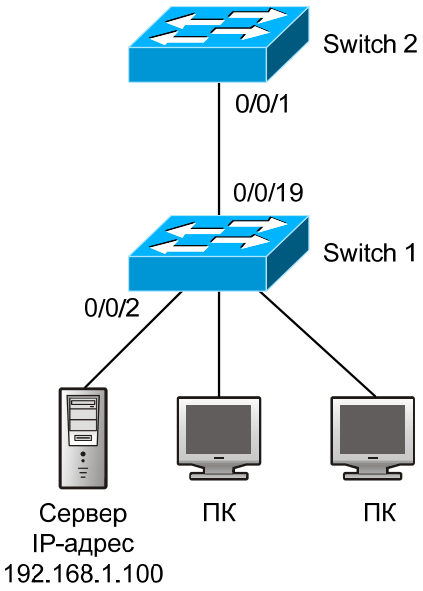

Рис. 36. Пример настройки защиты от ARP-сканирования

В сети, топология которой показана на Рис. 36, порт E0/0/1 коммутатора Switch 2 подключен к порту E0/0/19 коммутатора Switch 1, порт E0/0/2 коммутатора Switch 1 подключен к

файл-серверу (с IP-адресом 192.168.1.100), ко всем остальным портам коммутатора Switch 1 подключены обычные PC. Команды, приведенные ниже, обеспечивают защиту от ARP-сканирования, при этом нормальная работа системы не нарушается. Команды настройки коммутатора Switch 1:

```
Switch1(config)#anti-arpscan enable
Switch1(config)#anti-arpscan recovery time 3600
Switch1(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0
Switch1(config)#interface ethernet0/0/2
Switch1(config-if-ethernet0/0/2)#anti-arpscan trust port
Switch1(config-if-ethernet0/0/2)#exit
Switch1(config)#interface ethernet0/0/19
Switch1(config-if-ethernet0/0/19)#anti-arpscan trust supertrust-port
Switch1(config-if-ethernet0/0/19)#exit
```

Команды настройки коммутатора Switch 2:

```
Switch2(config)# anti-arpscan enable
Switch2(config)#interface ethernet0/0/1
Switch2(config-if-ethernet 0/0/1)#anti-arpscan trust port
Switch2(config-if-ethernet 0/0/1)exit
```

15.4 Устранение неполадок настройки защиты от ARP-сканирования

По умолчанию защита от ARP-сканирования выключена. После включения защиты от ARP-сканирования можно командой “debug anti-arpscan” включить режим отладки для просмотра отладочной информации.

16 Настройка защиты от подмены протоколов ARP, ND

16.1 Основные сведения

Протокол ARP (RFC-826) в основном отвечает за отображение IP-адресов в соответствующие им физические 48-разрядные адреса (MAC-адреса). Например, IP-адрес 192.168.0.1 соответствует Mac-адресу сетевой карты 00-00-11-22-33-44. Процесс отображения состоит в том, что хост вещает пакет данных, содержащий информацию об IP-адресе на хост назначения (запрос ARP). В ответ хост назначения отправляет пакет данных, содержащий его IP- и Mac-адрес. В результате эти два хоста выполняют обмен MAC-адресами.

16.2 Подмена ARP (ARP Spoofing)

В соответствии с структурой протокола ARP, для снижения передачи избыточных данных ARP по сетям делается следующее: несмотря на то, что хост-компьютер принимает ARP-ответ, который он сам не запрашивал, он будет вставлять его в ячейку таблицы ARP. Это создает возможность, называемую “ARP spoofing” (подмена ARP). Если хакер пожелает получить доступ к информации, передаваемой между двумя компьютерами, принадлежащих одной и той же сети (даже если они подключены через коммутатор), он может послать ответный пакет ARP этим двум хостам отдельно, чтобы каждый из них считал MAC-адресом другой стороны MAC-адрес хоста хакера. В результате связь между хостами будет осуществляться не напрямую, а через хост хакера. При этом хакеры не просто получат необходимую им информацию, передаваемую по соединению, они смогут изменять некоторую информацию пакетов данных и передавать их. При использовании хакерами этого метода, на их хосте не потребуется настройки смешанного режима работы сетевой карты, потому что пакетные данные, передаваемые между двумя сторонами попадают в компьютер хакеров на физическом уровне, который работает как реле.

16.3 Организация защиты от подмены ARP в коммутаторе уровня 3

Существует множество способов мониторинга, перехвата информации и атак, использующих сетевой протокол ARP. Большинство из них основаны на подмене ARP, поэтому крайне важно предотвратить ее. Доступ к сети с целью подмены ARP сначала выполняется с фальшивого IP-адреса, при этом фальшивые пакеты ARP поступают на коммутатор. После того, как коммутатор обучится по этим пакетам, они будут переданы на корректный IP-адрес, в результате будет определен его MAC-адрес. После этого, для нескольких корректных IP-адресов будет изменено их отображение в MAC-адреса так, как это требуется для пакетов атакующих. В результате коммутатор выполнит ошибочную передачу пакетов, что повлияет на работу всей сети. Есть и другой вариант — атакующие могут перехватывать (или захватывать) пакеты, передаваемые коммутаторами, либо атаковать другие коммутаторы, хосты, сетевое оборудование.

Действенный способ предотвращения атак и обмана коммутаторов путем подмены ARP в сетях состоит в отключении на коммутаторе функции автоматического обновления. Злоумышленники не смогут изменить корректный MAC-адрес, чтобы передавать фальшивые пакеты, также они не смогут получить и остальную информацию. При этом нет необходимости приостанавливать работу функции автоматического обучения ARP и ND. Это в значительной степени предотвращает атаки и подмену ARP.

ND (neighbor discovering protocol) — это протокол IPv6 для обнаружения соседних устройств. По принципу работы он подобен ARP, поэтому защита от атак и подмены ND осуществляется теми же способами, что и для ARP.

16.4 Настройка защита от подмены протоколов ARP, ND

Последовательность настройки защиты от подмены протоколов ARP, ND:

1. Выключение функции автоматического обновления ARP, ND
2. Выключение функции автоматического обучения ARP, ND
3. Замена динамических настроек ARP, ND статическими настройками

1. Выключение функции автоматического обновления ARP, ND

Команда	Описание
Глобальный режим	

конфигурирования, режим настройки интерфейсов	
ip arp-security updateprotect **no ip arp-security updateprotect** **ipv6 nd-security updateprotect** **no ipv6 nd-security updbateprotect**	Позволяет включить или выключить функцию автоматического обновления протоколов ARP, ND

2. Выключение функции автоматического обучения ARP, ND

Команда	Описание
Глобальный режим конфигурирования, режим настройки интерфейсов	
ipv6 nd-security learnprotect **no ipv6 nd-security learnprotect**	Позволяет включить или выключить функцию автоматического обучения протоколов ARP, ND

3. Замена динамических настроек ARP, ND статическими настройками

Команда	Описание
Глобальный режим конфигурирования, режим настройки интерфейсов	
ip arp-security convert ipv6 nd-security convert	Позволяет заменить динамические настройки ARP, ND статическими настройками

16.5 Пример настройки защиты от подмены протоколов ARP, ND

Пример схемы для настройки защиты от подмены протоколов ARP, приведён на Рис. 37.

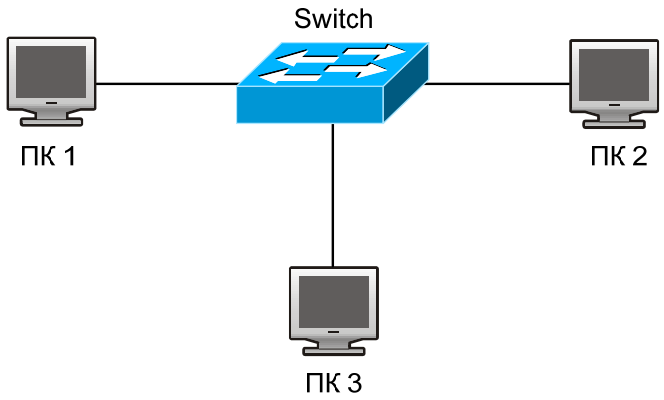

Рис. 37. настройки защиты от подмены протоколов ARP

Оборудование	Настройка	Качество
switch	IP:192.168.2.4; IP:192.168.1.4; MAC: 04-04-04-04-04-04	1
ПК 1	IP:192.168.2.1; MAC: 01-01-01-01-01-01	1
ПК 2	IP:192.168.1.2; MAC: 02-02-02-02-02-02	1
ПК 2	IP:192.168.2.3; MAC: 03-03-03-03-03-03	Какое-то (некоторое)

Между хостами 2 и 3 установлена связь, которая работает нормально. Коммутатор, выбранный хакерами для атаки, передает пакеты, переданные хостом 2 самому себе. Хакерам требуется, чтобы коммутатор передал пакеты хоста 2 на хост 1. Сначала хост хакеров 1 посылает на коммутатор пакет ответа ARP, его формат: 192.168.2.3, 01-01-01-01-01-01, в результате его MAC-адрес отображается в IP-адрес хоста 3, поэтому при обновлении списка ARP коммутатор изменяет IP-адрес. После этого пакетные данные 192.168.2.3 передаются на адрес 01-01-01-01-01-01 (MAC-адрес хоста A).

Затем происходит передача принятых пакетов на 3 путем модификации адресов источника и назначения. В результате данные передаваемые между хостами 2 и 3 принимаются на хосте 1. Так как список ARP регулярно обновляется, еще одна задача для хоста A состоит в постоянной отправке на коммутатор ответного пакета ARP, чтобы его информация все время попадала в обновленный список ARP коммутатора.

Поэтом очень важно защитить список ARP, в стабильных условиях работы настроить команду запрета на обучение ARP, а затем заменить все динамические настройки ARP статическими. Обученный ARP не будет обновляться и пользователи будут защищены.

```
Switch#config
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#arp 192.168.2.1 01-01-01-01-01-01 interface eth 0/0/2
Switch(config-if-vlan1)#interface vlan 2
Switch(config-if-vlan2)#arp 192.168.1.2 02-02-02-02-02-02 interface eth 0/0/2
Switch(config-if-vlan2)#interface vlan 3
Switch(config-if-vlan3)#arp 192.168.2.3 03-03-03-03-03-03 interface eth 0/0/2
Switch(config-if-vlan3)#exit
Switch(config)#ip arp-security learnprotect
Switch(config)#
Switch(config)#ip arp-security convert
```

Если условия работы изменятся, будет включен запрет на обновление ARP и как только выполнится обучение свойствам ARP, обновление не будет производиться по новым ответным пакетам ARP. В результате пользовательские данные будут защищены от злонамеренного доступа.

```
Switch#config
Switch(config)#ip arp-security updateprotect.
```

17 Настройка защиты ARP

17.1 Начальные сведения о защите ARP

В протоколе ARP имеется серьезная уязвимость — она состоит в том, что любое сетевое устройство может посылать ARP-сообщения, уведомляющее о привязке IP-адреса к MAC-адресу. Это дает шанс злоумышленникам, стремящимся подменить ARP. Атакующие могут посылать сообщения ARP request или ARP reply для уведомления о некорректных привязках IP-адресов к MAC-адресам, чтобы вызвать сбои в работе сети. При подмене ARP возникают опасности двух видов (Рис. 38):

1. ПК 4 посылает ARP-сообщение, уведомляющее о привязке IP-адреса ПК 2 к MAC-адресу ПК 4. Это приведет к тому, что все IP-сообщения, направляемые на ПК 2, будут посылаться на ПК 4. Поэтому ПК 4 сможет контролировать и захватывать сообщения, направляемые на ПК 2.
2. ПК 4 посылает ARP-сообщения, уведомляющее о привязке IP-адреса ПК 2 к некорректному MAC-адресу, в результате ПК 2 не будет принимать предназначенные ему сообщения. В частности, если атакующий будет выполнять роль шлюза и подменит ARP, вся сеть станет неработоспособной.

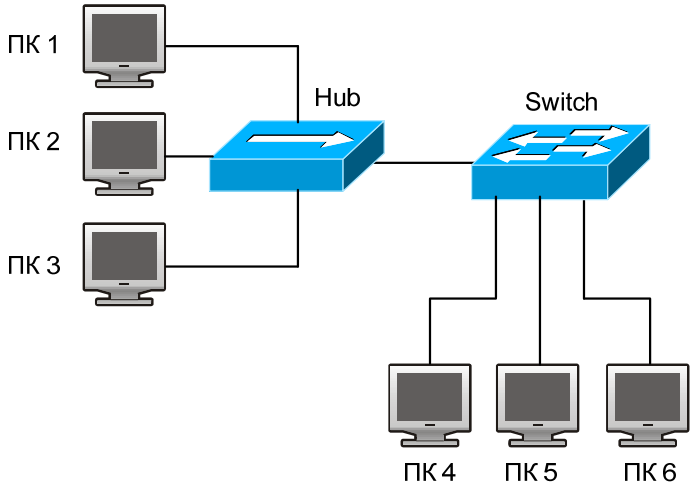

Рис. 38. Защита от ARP-атак

Для защиты записей ARP важных сетевых устройств и недопущения их подмены другими устройствами на коммутаторе используются фильтрующие элементы списка. Основная идея — использовать фильтрующие элементы списка в коммутаторе для проверки всех ARP-сообщений, входящих через порт. Если адрес источника ARP-сообщения защищен, сообщения будут отброшены и дальше передаваться не будут.

Функция ARP GUARD обычно используется для защиты шлюза от атак. Если от подмены ARP требуется защитить все доступные ПК сети, на порту необходимо задать настройки для большого числа адресов ARP GUARD, которые займут большую часть памяти FFP на чипе, — в результате может ухудшиться работа других приложений. Это было бы неправильно. Поэтому рекомендуется использовать схему доступа с общедоступному ресурсу. Подробнее об этом см. в соответствующей документации.

17.2 Настройка функции ARP GUARD

1. Настройка защищенного IP-адреса

Команда	Описание
Режим настройки портов	
arp-guard ip <addr> **no arbp-guard ip** <addr>	Позволяет настроить или удалить адрес ARP Guard

18 Настройка самообращенных запросов (Gratuitous ARP)

18.1 Начальные сведения о запросах Gratuitous ARP

Gratuitous ARP — это вид запроса ARP, посылаемый хостом и содержащий IP-адрес этого хоста в качестве назначения запроса ARP.

Коммутатор может обрабатывать такие запросы ARP следующим образом: интерфейсы уровня 3 коммутатора могут быть настроены на оповещение о gratuitous ARP-пакетах в течение некоторого периода времени, либо в глобальном режиме конфигурирования можно включить отправку gratuitous ARP-пакетов во все интерфейсы.

Цели отправки запросов gratuitous ARP могут быть следующими:

1. Снижение частоты отправки запросов ARP в коммутатор. Хосты сети будут периодически посылать запросы ARP в шлюзы для обновления MAC-адресов шлюзов. Если коммутатор оповещает о запросах gratuitous ARP, хост не будет посылать свои запросы. В результате снижается частота отправки хостами запросов ARP по MAC-адресам шлюзов.
2. Gratuitous ARP — это метод предотвращения подмены ARP. Коммутаторы, оповещающие о запросах gratuitous ARP будут принуждать хосты обновлять свои таблицы ARP. В результате фальшивые ARP шлюзов не будут работать.

18.2 Последовательность настройки функции Gratuitous ARP

1. Включение функции gratuitous ARP, настройка интервалов времени отправки запросов gratuitous ARP
2. Вывод на дисплей информации о настройках запросов gratuitous ARP

1. Включение функции gratuitous ARP, настройка интервалов времени отправки запросов gratuitous ARP

Команда	Описание
Глобальный режим конфигурирования, режим настройки интерфейсов	
ip gratuitous-arp <5-1200> **no ip gratuitous-arp**	Позволяет включить функцию gratuitous ARP, настроить интервал времени отправки запросов gratuitous ARP. Отмена команды no ip gratuitous-arp отменяет запросы gratuitous ARP

2. Вывод на дисплей информации о настройках запросов gratuitous ARP

Команда	Описание
Привилегированный режим, режим конфигурирования	
show ip gratuitous-arp [**interface vlan** <1-4094>]	Позволяет вывести на дисплей информацию о настройках запросов gratuitous ARP

18.3 Пример настройки запросов Gratuitous ARP

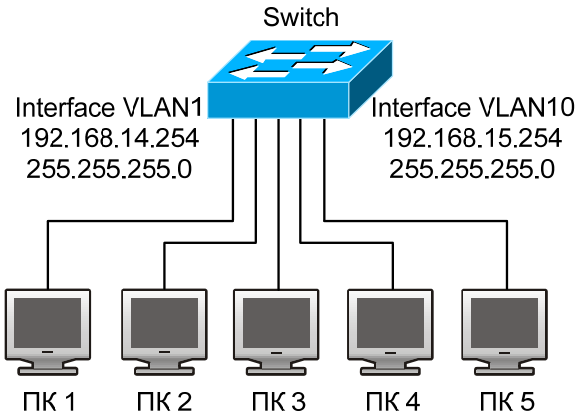

Рис. 39. Пример настройки запросов Gratuitous ARP

В схеме сети, показанной на Рис. 39, интерфейс VLAN 10 с IP-адресом 192.168.15.254 и маской адресов сети 255.255.255.0 принадлежит коммутатору Switch. К интерфейсу подключены три компьютера ПК 3, ПК 4, ПК 5. IP-адрес интерфейса VLAN 1 192.168.14.254, его маска адресов сети 255.255.255.0. К этому интерфейсу подключены два компьютера — ПК 1 и ПК 2. Запросы Gratuitous ARP можно включить, введя следующие команды:

Настроим два интерфейса на одновременное использование запросов gratuitous ARP.

```
Switch(config)#ip gratuitous-arp 300
Switch(config)#exit
```

Настроим использование запросов gratuitous ARP только на одном интерфейсе:

```
Switch(config)#interface vlan 10
Switch(config-if-vlan10)#ip gratuitous-arp 300
Switch(config-if-vlan10)#exit
Switch(config) #exit
```

18.4 Устранение неполадок с запросами Gratuitous ARP

По умолчанию запросы Gratuitous ARP выключены. Когда запросы gratuitous ARP включены, отладочная информация о пакетах ARP может быть получена, если ввести команду debug ARP.

Если запросы gratuitous ARP включены в глобальном режиме конфигурирования, они могут быть выключены также только в глобальном режиме конфигурирования. Если запросы gratuitous ARP включены в режиме настройки интерфейсов, они могут быть выключены также только в режиме настройки интерфейсов.

Если запросы gratuitous ARP включены и в глобальном режиме конфигурирования и в режиме настройки интерфейсов, и в обоих режимах задан интервал обновления, коммутатор выберет значение, заданное в режиме настройки интерфейсов.

19 Настройка Multicast-протокола IPv4

19.1 Технология DCSCM

19.1.1 Начальные сведения о технологии DCSCM

Технология DCSCM (Destination control and source control multicast) — безопасное управление групповым трафиком) имеет три преимущества: управление источником группового трафика, управление пользователями группового трафика, использование приоритетов в политиках группового обслуживания.

Для управления источником группового трафика при технологии DCSCM используются следующие основные методы:

1. В пограничном коммутаторе (если он сконфигурирован для управления источником группового трафика) пропускаются только групповые данные указанной в настройках коммутатора группы, посылаемые указанным в настройках источником.
2. При RP-коммутаторе в состоянии ядра PIM-SM, всем зарегистрированным (REGISTER) адресатам, кроме заданных в настройках коммутатора источника и группы, будут напрямую посылаться сообщения REGISTER_STOP. Запрещается создание элементов списка. (Эта задача выполняется модулем PIM-SM).

Технология DCSCM реализована на основе управления сообщениями отчетов IGMP, поступающими от пользователей, поэтому управляемыми модулями являются модули IGMP snooping и модуль IGMP. При управлении используются три метода: Управление по VLAN+MAC — адресу источника сообщения, управление по IP-адресу источника сообщения, управление в соответствии с портом, от которого приходят сообщения. При IGMP snooping можно использовать все три метода, а при IGMP (из-за того, что этот протокол принадлежит уровню 3) — только управление по IP-адресу источника сообщения.

При обслуживании группового трафика по приоритетам, реализованным в технологии DCSCM, используются следующие методы: для групповых данных, предназначенных для небольшой области, назначаются приоритеты, заданные пользователем в точке доступа — это приводит к большему приоритету при передаче данных по магистрали и гарантирует, что данные будут переданы через всю сеть с приоритетом, указанным пользователем.

19.1.2 Последовательность настройки DCSCM

1. Настройка управления источником
2. Настройка управления назначением
3. Настройка политик обслуживания группового трафика

1. Настройка управления источником

Настройку управления источником можно разделить на три этапа: первый этап — включение управления источником в глобальном режиме конфигурирования, для которого используются следующие команды:

Команда	Описание
Глобальный режим конфигурирования	
[**no**] **ip multicast source-control** (Required)	Включает управление источником в глобальном режиме конфигурирования. Отмена команды: “[no] ip multicast source-control” выключает управление источником. Следует иметь в виду, что после ввода этой команды все групповые сообщения будут по умолчанию выгружены. Управление источником может осуществляться только после его включения в глобальном режиме конфигурирования. Управление источником может быть выключено в глобальном режиме конфигурирования только после того, как будут выключены все сконфигурированные для него правила

Следующий этап — настройка правил управления источником. Используется тот же метод, что и при управлении списками доступа ACL — используются идентификаторы ACL ID с 5000 по 5099. Для каждого ID может быть сконфигурировано не более 10 правил. Следует иметь в виду, что эти правила образуют последовательность — первым проверяется самое раннее правило. Как только будет достигнуто согласование, все последующие правила игнорируются. Команда, которая выполняет это:

Команда	Описание
Глобальный режим конфигурирования	
[**no**] **access**-**list** <5000-5099> {**deny** | **permit**} **ip** {{<source> <source-wildcard>} | {host-source <source-host-ip>} | any-source} {{<destination> <destination-wildcard>} | {host-de stination <destination-host-ip>} | any-destin ation}	Позволяет задать правила, используемые для управления источником. Правила действуют только для указанного порта. Отмена команды: no access-list удаляет соответствующее правило

Следующая команда (см. ниже) позволяет изменить настройку правила для указанного порта. Примечание: Так как сконфигурированные правила содержат списки аппаратных устройств, то при введении слишком большого числа правил конфигурация может оказаться неработоспособной из-за переполнения списков нижнего уровня. Поэтому пользователям рекомендуется использовать как можно более простые правила. Команда, которая выполняет настройку правил:

Команда	Описание
Режим настройки порта	
[**no**] **ip multicast source**-**control access**-**group** <5000-5099>	Позволяет настроить правило, используемое портом при управлении источником. Отмена команды: no ip multicast source-control access-group <5000-5099> удаляет соответствующее правило

2. Настройка управления назначением

Подобно настройке управления источником, выполняется в три этапа:

Первый этап: включение управления назначением в глобальном режиме конфигурирования (так как управление назначением должно предотвращать прием групповых данных несанкционированными пользователями). После включения управления назначением в глобальном режиме конфигурирования коммутатор не будет осуществлять вещание принятого группового трафика. Поэтому следует избегать подключения двух и более коммутаторов 3 уровня к коммутатору, на котором включено управление назначением в одной VLAN. Команды настройки:

Команда	Описание
Глобальный режим конфигурирования	
[**no**] **multicast destination**-**control** (**required**)	Позволяет глобально включить управление IP источником. Отмена команды: “no multicast destination-control” выключает управление источником в глобальном режиме конфигурирования. Все другие настройки возымеют действие только после того, как управление источником будет включено в глобальном режиме конфигурирования. После этого выполняется настройка правил управления

Следующий этап состоит в настройке правил управления назначением, которые подобны правилам управления источником, за исключением того, что используются идентификаторы списков доступа (ACL ID) с 6000 по 7999.

Команда	Описание
Глобальный режим конфигурирования	
[**no**] **access**-**list** <6000-7999> {**deny** | **permit**} **ip** {{<source> <source-wildcard>} | {host-source <source-host-ip>} |any-source} {{<destination> <destination-wildcard>} | {host-destination <destination-host-ip>} | any-destination}	Позволяет настроить правило, используемое для управления назначением. Правило может быть применено только к указанному источнику (с IP-адресом или с VLAN-MAC-адресом) или к порту. Отмена команды: no access-list <6000-7999> удаляет соответствующее правило

Последний этап состоит в настройке правила для указанного IP-источника, VLAN-MAC источника или порта. Следует иметь в виду, что для глобального использования правил необходимо сначала включить IGMP-SNOOPING. Команда настройки:

Команда	Описание
Режим настройки порта	
[**no**] **ip multicast destination**-**control access**-**group** <6000-7999>	Позволяет настроить правило, используемое портом при управлении источником. Отмена команды: no ip multicast destination-control access-group <6000-7999> удаляет соответствующее правило
Глобальный режим конфигурирования.	
[**no**] **ip multicast destination**-**contro** l <1-4094> <macaddr> **access**-**group** <6000-	Позволяет настроить правило, используемое указанной VLAN-MAC при управлении источником.

7999>	Отмена команды: no ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999> удаляет соответствующее правило
[**no**] **ip multicast destination-control** <source> <source-wildcard> **access-group** <6000-7999>	Позволяет настроить правило, используемое при управлении источником, имеющим указанный IP-адрес или маску подсети. Отмена команды: no ip multicast destination-control <source> <source-wildcard> access-group <6000-7999> удаляет соответствующую настройку

3. Настройка политик обслуживания группового трафика

Политики обслуживания группового трафика позволяют удовлетворить требования пользователей к приоритетам групповых данных. Следует с осторожностью использовать команду, приведенную ниже, так как она влияет на приоритет передачи групповых данных по магистрали. Команда настройки приоритета указанного группового трафика:

Команда	Описание
Глобальный режим конфигурирования	
[**no**] **ip multicast policy** <ipaddress/m> <ipaddress/m> **cos** <priority>	Позволяет задать политику обслуживания группового трафика, задать приоритет источников и группп (в некотором диапазоне). Диапазон приоритетов: <0 — 7>

19.1.3 Примеры применения DCSCM

1. Управление источником

Для предотвращения бесконтрольной отправки групповых данных пограничным коммутатором, настроим его так, чтобы только коммутатору, подключенному к порту Ethernet0/0/5, было разрешено посылать групповые данные для группы с IP-адресом 225.1.2.3. При этом коммутатор, присоединенный к порту Ethernet0/0/25 сможет передавать групповые данные без каких-либо ограничений. Процедура настройки:

```
Switch(config)#access-list 5000 permit ip any host 225.1.2.3
Switch(config)#access-list 5001 permit ip any any
Switch(config)#ip multicast source-control
Switch(config)#interface ethernet0/0/5
Switch(config-If-Ethernet0/0/5)#ip multicast source-control access-group 5000
Switch(config)#interface ethernet0/0/10
Switch(config-If-Ethernet0/0/10)#ip multicast source-control access-group 5001
```

2. Управление назначением:

Пусть требуется, чтобы пользователи сегмента 10.0.0.0/8 не могли вступить в группу 238.0.0.0/8.

Во-первых, включим IGMP snooping для VLAN, в которой это происходит (VLAN2).

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

Затем настроим соответствующий список доступа ACL для управления назначением и настроим указанный IP-адрес для использования в списке доступа ACL.

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

Теперь пользователи этого сегмента могут вступать только в группы, отличные от 238.0.0.0/8.

3. Политика обслуживания группового трафика

Сервер 210.1.1.1 посылает важные групповые данные в группу 239.1.2.3. Настройка его коммутатора доступа может быть выполнена командой:

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

Теперь, когда групповой поток проходит через магистраль этого коммутатора в другие коммутаторы, он будет иметь приоритет 4 (обычно это наивысший приоритет, более высокий имеют только данные протокола, однако если мы выберем более высокий приоритет, при

передаче очень больших объемов групповых данных протокол коммутатора может работать неправильно).

19.1.4 Устранение неполадок DCSCM

Модуль DCSCM реализует функции, подобные спискам доступа ACL. Проблемы возникают в основном в связи с неправильными настройками. Пожалуйста, внимательно изучите приведенные выше инструкции. Если Вы самостоятельно не смогли установить причины возникновения проблем, пожалуйста, обратитесь в службу технической поддержки компании Zelax.

19.2 Протокол IGMP Snooping

19.2.1 Начальные сведения о протоколе IGMP Snooping

Протокол IGMP (Internet Group Management Protocol — протокол управления Интернет-группами) используется для управления групповым IP-трафиком. Протокол IGMP используется сетевыми устройствами, поддерживающими групповой трафик (например, маршрутизаторами) для отправки запросов хостам-членам групп, либо хостами-членами групп для информирования маршрутизатора о доступности пакетов с некоторым групповым адресом. Все эти операции выполняются путем обмена сообщениями IGMP. Маршрутизатор использует групповой адрес (224.0.0.1) — он может использоваться для отправки сообщений с запросами о наличии в сети членов групп IGMP. Если хост желает вступить в группу, он отвечает по групповому адресу этой группы уведомлением о наличии в сети члена группы IGMP.

IGMP Snooping еще называют прослушиванием IGMP. С помощью IGMP Snooping коммутатор предотвращает веерную рассылку группового трафика, так как этот трафик продвигается только к портам, ассоциированным с групповыми устройствами. Коммутатор «прослушивает» сообщения IGMP, обмен которыми идет между групповым маршрутизатором и хостами и корректирует групповую таблицу передачи на основе результатов прослушивания. Затем он может принять решение осуществить форвардинг пакетов в соответствии с таблицей передачи.

19.2.2 Последовательность настройки IGMP Snooping

1. Включение протокола IGMP Snooping
2. Настройка протокола IGMP Snooping

1. Включение протокола IGMP Snooping

Команда	Описание
Глобальный режим конфигурирования	
ip igmp snooping **no ip igmp snooping**	Включает функцию IGMP Snooping. Отмена команды: ”No ip igmp snooping” глобально выключает функцию IGMP Snooping
ip igmp snooping vlan <vlan-id> **no ip igmp snooping** vlan <vlan-id>	Включает функцию IGMP Snooping на указанном VLAN. Отмена команды: No ip igmp snooping VLAN <vlan-id> выключает функцию IGMP Snooping на указанном VLAN

2. Настройка протокола IGMP Snooping

Команда	Описание
Глобальный режим конфигурирования	
ip igmp snooping vlan < vlan-id > **limit** {**group** <g_limit> | **source** <s_limit>} **no ip igmp snooping vlan** < vlan-id > **limit**	Позволяет задать максимальное число групп IGMP snooping, в которые может вступить хост, и максимальное число источников, которые может иметь группа. Отмена команды: “no ip igmp snooping vlan <vlan-id> limit ” восстанавливает настройки, используемые по умолчанию
ip igmp snooping vlan <vlan-id> **l2-general-querier** **no ip igmp snooping vlan** <vlan-id> **l2-general-querier**	Устанавливает указанную vlan, как маршрутизатор уровня 2. Рекомендуется, чтобы в каждом сегменте мог быть сконфигурирован маршрутизатор уровня 2. Отмена команды: “no ip igmp snooping vlan <vlan-id> l2-general-querier” отменяет конфигурацию маршрутизатора уровня 2
ip igmp snooping vlan <vlan-id> **l2-general-querier-version**	Позволяет задать номер версии VLAN, выполняющей функции маршрутизатора уровня 2

<version>	
ip igmp snooping vlan <vlan-id> **l2-general-querier-source** <source>	Позволяет задать номер версии VLAN, выполняющей функции маршрутизатора уровня 2
ip igmp snooping vlan <vlan-id> **mrouter-port interface** <interface–name> **no ip igmp snooping vlan** <vlan-id> **mrouter-port interface** <interface–name>	Позволяет задать статический порт mrouter. Команда ”no ip igmp snooping vlan <vlan-id> mrouter-port interface <interface — name>” отменяет конфигурацию порта mrouter
ip igmp snooping vlan <vlan-id> **mrpt** <value > **no ip igmp snooping vlan** <vlan-id> **mrpt**	Позволяет задать срок жизни порта mrouter. Команда “no ip igmp snooping vlan <vlan-id> query-mrsp” восстанавливает настройки, используемые по умолчанию
ip igmp snooping vlan <vlan-id> **query-interval** <value> **no ip igmp snooping vlan** <vlan-id> **query-interval**	Позволяет задать интервал отправки запросов Команда “no ip igmp snooping vlan <vlan-id> query-interval” восстанавливает настройки, используемые по умолчанию
ip igmp snooping vlan <vlan-id> **immediately-leave** **no ip igmp snooping vlan** <vlan-id> **immediately-leave**	Позволяет задать IGMP snooping для указанного VLAN, чтобы включить функцию временного выхода команда ”no ip igmp snooping vlan <vlan-id> immediate-leave” выключает функцию временного выхода
ip igmp snooping vlan <vlan-id> **query-mrsp** <value> **no ip igmp snooping vlan** <vlan-id> **query-mrsp**	Позволяет задать максимальное время ожидания ответа на запрос. Отмена команды: ”no ip igmp snooping vlan <vlan-id> query-mrsp” восстанавливает настройки, используемые по умолчанию
ip igmp snooping vlan <vlan-id> **query-robustness** <value> **no ip igmp snooping vlan** <vlan-id> **query-robustness**	Позволяет задать надежность (robustness). Отмена команды: “no ip igmp snooping vlan <vlan-id> query-robustness” восстанавливает настройки, используемые по умолчанию
ip igmp snooping vlan <vlan-id> **suppression-query-time** <value> **no ip igmp snooping vlan** <vlan-id> **suppression-query-time**	Позволяет задать время подавления запросов. Отмена команды: “no ip igmp snooping vlan <vlan-id> suppression-query-time” восстанавливает настройки, используемые по умолчанию
ip igmp snooping vlan <vlan-id> **static-group** <A.B.C.D> [**source** <A.B.C.D>] **interface** [**ethernet** | **port-channel**] <IFNAME> **no ip igmp snooping vlan** <vlan-id> **static-group** <A.B.C.D> [**source** <A.B.C.D>] **interface** [**ethernet** | **port-channel**] <IFNAME>	Позволяет задать в указанном порту статическую группу. Отмена команды: “no ip igmp snooping vlan <vlan-id> tatic-group <multicast-IPAddress> interface {[ethernet|port-channel] <interfaceName>” отменяет сделанные настройки
ip igmp snooping vlan <vlan-id> **report source-address** <A.B.C.D> **no ip igmp snooping vlan** <vlan-id> **report source-address**	Позволяет настроить передачу адреса источника пакетов IGMP. Отмена команды: “no ip igmp snooping vlan <vlan-id> report source-address” отменяет передачу адреса источника пакетов IGMP

19.2.3 Примеры применения IGMP Snooping

Применение функции IGMP Snooping (Рис. 40)

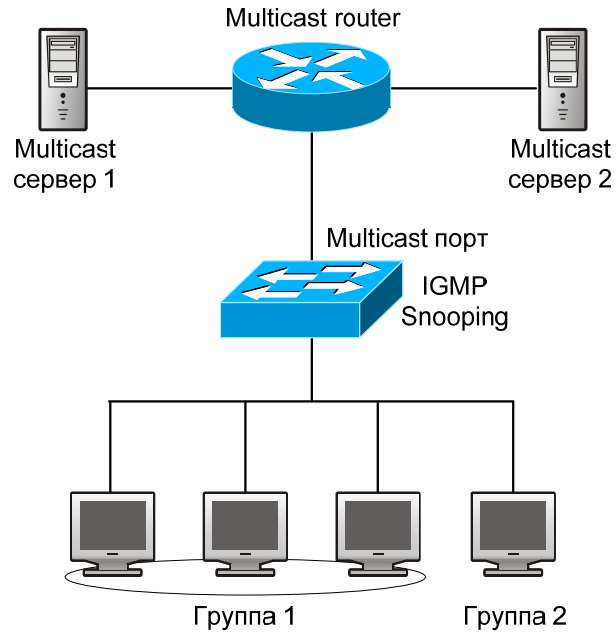

Рис. 40. Включение функции IGMP Snooping

Пример: Как показано на рисунке, на коммутаторе сформирована VLAN 100 с портами 1, 2, 6, 10 и 12.К портам 2, 6, 10, 12 подключны четыре хоста, а к порту 1 — групповой маршрутизатор. Так как IGMP Snooping по умолчанию выключен (либо на коммутаторе, либо в сетях VLAN), то для включения IGMP Snooping на VLAN 100, IGMP Snooping должен быть сначала включен в глобальном режиме конфигурирования коммутатора; после включения IGMP Snooping на VLAN 100, ее порт 1 можно установить как порт M-Router.

Процедура настройки:

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

Конфигурация групповой рассылки сообщений:

Предположим, что имеются два сервера групповой рассылки сообщений: Групповой сервер 1 и Групповой сервер 2. На трех хостах одновременно функционирует групповое ПО, они подключены к портам 2, 6 и 10 и заказали программу 1. Четвертый хост подключен к порту 12 и заказал программу 2.

Прослушивание при IGMP Snooping даст следующий результат:

Протоколом IGMP Snooping на VLAN 100 будет построена таблица групп, в которой порты 1, 2, 6 и 10 будут присвоены группе 1, а порты 1, 12 — группе 2. Все четыре хоста смогут принимать заказанные программы: Порты 2, 6 и 10 не будут принимать трафик программы 2; порт 12 не будет принимать трафик программы 1.

Пример 2: IGMP-маршрутизатор уровня 2 (Рис. 41)

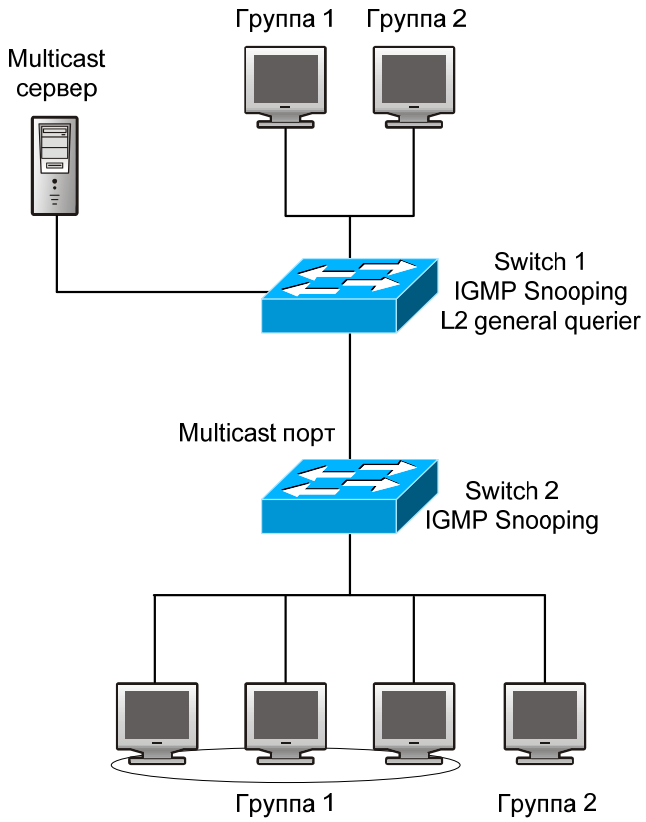

Рис. 41. IGMP-маршрутизатор уровня 2

Конфигурация коммутатора Switch 2 такая же, как и в сценарии 1. Место группового маршрутизатора сценария 1 занимает Switch 1.Предположим, что на Switch 1 сформирован VLAN 60 с портами 1, 2, 6, 10 и 12. Порт 1 подключен к групповому серверу, порт 2 — к коммутатору Switch 2. Для регулярной отправки запросов IGMP-маршрутизатор должен быть включен в глобальном режиме конфигурирования на VLAN60.

Процедура настройки:

```
Switch1#config
Switch1(config)#ip igmp snooping
Switch1(config)#ip igmp snooping vlan 60
Switch1(config)#ip igmp snooping vlan 60 L2-general-querier
Switch2#config
Switch2(config)#ip igmp snooping
Switch2(config)#ip igmp snooping vlan 100
Switch2(config)#ip igmp snooping vlan 100 mrouter interface ethernet 0/0/1
```

Конфигурация групповой рассылки такая же, как в примере 1.

Результат прослушивания IGMP Snooping такой же, как и в примере 1.

Пример 3:

Совместная работа с групповыми протоколами уровня 3. Коммутатор из сценария 1 заменен маршрутизатором с теми же настройками. Настройки групповой рассылки и IGMP snooping те же, что и в сценарии 1. Настроим PIM-SM на маршрутизаторе и включим PIM-SM на vlan 100 (будем использовать тот же режим PIM с подключенным групповым маршрутизатором).

Последовательность команд настройки:

```
switch#config
switch(config)#ip pim multicast-routing
switch(config)#interface vlan 100
switch(config-if-vlan100)#ip pim sparse-mode
```

Когда включен групповой протокол уровня 3, IGMP snooping не распределяет пакеты. Он выполняет только следующие задачи:

- Удаляет групповые пакеты уровня 2

- Выполняет функции маршрутизатора для уровня 3 с vlan, при этом S и G используются, как параметры
- Когда IGMP уровня 3 выключен, снова начинается распределение групповых пакетов уровня 2

Рассматривая пакеты IPMC уровня 3, можно обнаружить, что порты могут быть определены по групповым пакетам уровня 3. Это гарантирует, что IGMP snooping будет работать совместно с групповыми протоколами уровня 3.

19.2.4 Устранение неполадок при IGMP Snooping

В процессе настройки и использования функции IGMP Snooping администраторы могут обнаружить, что IGMP Snooping работает неправильно — вероятно, из-за неправильно выполненных физических соединений или настройки. Администратор должен обеспечить следующее:

- Правильность физических соединений;
- IGMP Snooping должен быть включен в глобальном режиме конфигурирования (командой ip igmp snooping).
- Настройка VLAN (командой ip igmp snooping vlan <vlan-id>) должна выполняться, когда IGMP Snooping уже включен в глобальном режиме конфигурирования.
- Vlan используется в качестве маршрутизатора уровня 2 либо в том же сегменте задан статический mrouter.
- Проверить правильность информации IGMP Snooping с помощью команды ”show ip igmp snooping vlan <vid>”.

20 Настройка Multicast-протокола IPv6

20.1 Технология DCSCM для протокола IPv6

20.1.1 Начальные сведения о технологии IPv6 DCSCM

Технология IPv6 DCSCM (безопасное управление групповым трафиком) имеет три преимущества: управление источником группового трафика, управление пользователями группового трафика, использование приоритетов в политиках группового обслуживания.

Для управления источником группового трафика при технологии IPv6 DCSCM используются следующие основные методы:

1. В пограничном коммутаторе (если он сконфигурирован для управления источником группового трафика) пропускаются только групповые данные указанной в настройках коммутатора группы, посылаемые указанным в настройках источником.
2. При RP-коммутаторе в состоянии ядра PIM-SM, всем зарегистрированным (REGISTER) адресатам, кроме заданных в настройках коммутатора источника и группы, будут напрямую посылаться сообщения REGISTER_STOP. Запрещается создание элементов списка. (Эта задача выполняется модулем PIM-SM).

Технология IPv6 DCSCM реализована на основе управления сообщениями MLD, поступающими от пользователей, поэтому управляемыми модулями являются модули MLD snooping и модуль MLD. При управлении используются три метода: управление по VLAN+MAC — адресу источника сообщения, управление по IP-адресу источника сообщения, управление в соответствии с портом, от которого приходят сообщения. При MLD snooping можно использовать все три метода, а при MLD (из-за того, что этот протокол принадлежит уровню 3) — только управление по IP-адресу источника сообщения.

При обслуживании группового трафика по приоритетам, реализованном в технологии DCSCM, используются следующие методы: для групповых данных, предназначенных для небольшой области, назначаются приоритеты, заданные пользователем в точке доступа — это приводит к большему приоритету при передаче данных по магистрали и гарантирует, что данные будут переданы через всю сеть с приоритетом, указанным пользователем.

20.1.2 Последовательность настройки IPv6 DCSCM

1. Настройка управления источником
2. Настройка управления назначением
3. Настройка политик обслуживания группового трафика

1. Настройка управления источником

Настройку управления источником можно разделить на три этапа: первый этап — включение управления источником в глобальном режиме конфигурирования, для которого используются следующие команды:

Команда	Описание
Глобальный режим конфигурирования	
ipv6 multicast source-control (necessary) **no ipv6 multicast source-control**	Включает управление источником в глобальном режиме конфигурирования. Отмена команды: “no ipv6 multicast source-control” выключает управление источником. Следует иметь в виду, что после ввода этой команды все групповые сообщения будут по умолчанию выгружены. Управление источником может осуществляться только после его включения в глобальном режиме конфигурирования. Управление источником может быть выключено в глобальном режиме конфигурирования только после того, как будут выключены все сконфигурированные для него правила

Следующий этап — настройка правил управления источником. Используется тот же метод, что и при управлении списками доступа ACL — используются идентификаторы ACL ID с 8000 по 8099. Для каждого ID может быть сконфигурировано не более 10 правил. Следует иметь в виду, что эти правила образуют последовательность — первым проверяется самое раннее правило. Как только будет достигнуто согласование, все последующие правила игнорируются. Поэтому последними правилами должны быть правила, разрешенные в глобальном режиме конфигурирования. Команда, которая выполняет это:

Команда	Описание
Глобальный режим конфигурирования	
[**no**] **ipv6 access-list** <8000-8099> {**deny** | **permit**} {{<source/M>} | {host-source <source-host-ip>} | any-source} {{<destination/M> } | {host-destination <destination-host-ip>} | any-destination}	Позволяет задать правила, используемые для управления источником. Правила действуют только для указанного порта. Отмена команды: no ipv6 access-list удаляет соответствующее правило

Следующая команда (см. ниже) позволяет настроить правила для указанного порта.

Так как сконфигурированные правила содержат списки аппаратных устройств, то при введении слишком большого числа правил конфигурация может оказаться неработоспособной из-за переполнения списков нижнего уровня. Поэтому пользователям рекомендуется использовать как можно более простые правила.

Команда, которая выполняет настройку правил:

Команда	Описание
Режим настройки порта	
[**no**] **ipv6 multicast source-control access-group** <8000-8099>	Позволяет настроить правило, используемое портом при управлении источником. Отмена команды: no ipv6 multicast source-control access-group <8000-8099> удаляет соответствующее правило

2. Настройка управления назначением

Подобно настройке управления источником, выполняется в три этапа:

Первый этап: включение управления назначением в глобальном режиме конфигурирования (так как управление назначением должно предотвращать прием групповых данных несанкционированными пользователями). После включения управления назначением в глобальном режиме конфигурирования коммутатор не будет осуществлять вещание принятого группового трафика. Поэтому следует избегать подключения двух и более коммутаторов 3 уровня к коммутатору, на котором включено управление назначением в одной VLAN. Команда настройки:

Команда	Описание
Глобальный режим конфигурирования	
multicast destination-control (necessary)	Включает управление IPV4- и IPv6-источником в глобальном режиме конфигурирования. Отмена команды: “no multicast destination-control (necessary)” выключает управление источником. Все другие настройки возымеют действие только после того, как управление источником будет включено в глобальном режиме конфигурирования

Следующий этап состоит в настройке правил управления назначением, которые подобны правилам управления источником, за исключением того, что используются идентификаторы списков доступа (ACL ID) с 9000 по 10099.

Команда	Описание
Глобальный режим конфигурирования	
[**no**] **ipv6 access-list** <9000-10099> {**deny** | **permit**} {{<source/M>} | {host-source <source-host-ip>} | any-source} {{<destination/M>} | {host-destination <destination-host-ip>} | any-destination}	Позволяет настроить правило, используемое для управления назначением. Правило может быть применено только к указанному источнику (с IP-адресом или с VLAN-MAC-адресом) или к порту. Отмена команды: no ipv6 access-list <9000-10099> удаляет соответствующее правило

Последний этап состоит в настройке правила для указанного IP-источника, VLAN-MAC источника или порта. Следует иметь в виду, что для глобального использования правил необходимо сначала включить MLD-snooping. Если этого не сделать, то можно только использовать правила для IP-адреса источника при протоколе MLD. Команда настройки:

Команда	Описание
Режим настройки порта	
[**no**] **ipv6 multicast destination-control access-group** <9000-10099>	Позволяет настроить правило, используемое портом при управлении источником. Отмена команды: no ipv6 multicast destination-control access-group <9000-10099> удаляет соответствующее правило
Глобальный режим	

конфигурирования.	
[**no**] **ipv6 multicast destination-control** <1-4094> <macaddr> **access-group** <9000-10099>	Позволяет настроить правило, использующее указанный VLAN-MAC при управлении источником. Отмена команды: no ipv6 multicast destination-control <1-4094> <macaddr> access-group <9000-10099> удаляет соответствующее правило
[**no**] **ipv6 multicast destination-control** <ipaddress/m> **access-group** <9000-100999>	Позволяет настроить правило, используемое при управлении источником, имеющим указанный IP-адрес или маску подсети. Отмена команды: no ipv6 multicast destination-control <ipaddress/m> access-group <9000-100999> удаляет соответствующую настройку

3. Настройка политик обслуживания группового трафика

Политики обслуживания группового трафика позволяют удовлетворить требования пользователей к приоритетам групповых данных. Следует с осторожностью использовать команду, приведенную ниже, так как она влияет на приоритет передачи групповых данных по магистрали. Команда настройки приоритета указанного группового трафика:

Команда	Описание
Глобальный режим конфигурирования	
[**no**] **ipv6 multicast policy** <ipaddress/m> <ipaddress/m> **cos** <priority>	Позволяет задать политику обслуживания группового трафика, задать приоритет источников и групп (в некотором диапазоне). Диапазон приоритетов: <0 — 7>

20.1.3 Примеры применения IPv6 DCSCM

1. Управление источником

Для предотвращения бесконтрольной отправки групповых данных пограничным коммутатором, настроим его так, чтобы только коммутатору, подключенному к порту Ethernet0/0/5, было разрешено посылать групповые данные для группы ff1e::1. При этом uplink-порт Ethernet0/0/25 сможет передавать групповые данные без каких-либо ограничений. Процедура настройки:

```
Switch(config)#ipv6 access-list 8000 permit any-source ff1e::1
Switch(config)#ipv6 access-list 8001 permit any any
Switch(config)#ipv6 multicast source-control
Switch(config)#interface Ethernet0/0/5
Switch(Config-If-Ethernet0/0/5)#ipv6 multicast source-control access-group 8000
Switch(config)#interface Ethernet0/0/25
Switch(Config-If-Ethernet0/0/25)#ipv6 multicast source-control access-group 8001
```

2. Управление назначением

Пусть требуется, чтобы пользователи сегмента fe80::203:fff:fe01:228a/64 не могли вступить в группу ff1e::1/64.

Во-первых, включим MLD snooping для VLAN, в которой это происходит (VLAN2).

```
Switch(config)#ipv6 mld snooping
Switch(config)#ipv6 mld snooping vlan 2
```

Затем настроим соответствующий список доступа ACL для управления назначением и настроим указанный IPv6-адрес для использования в списке доступа ACL.

```
Switch(config)#ipv6 access-list 9000 deny any ff1e::1/64
Switch(config)#ipv6 access-list 9000 permit any any
Switch(config)#multicast destination-control
Switch(config)#ipv6 multicast destination-control fe80::203:fff:fe01:228a/64 access-group 9000
```

Теперь пользователи этого сегмента могут вступать только в группы, отличные от 2ff1e::1/64.

3. Политика обслуживания группового трафика

Сервер 2008::1 посылает важные групповые данные в группу ff1e::1 Настройка его коммутатора доступа может быть выполнена командой:

```
Switch(config)#ipv6 multicast policy 2008::1/128 ff1e::1/128 cos 4
```

Теперь, когда групповой поток проходит через магистраль этого коммутатора в другие коммутаторы, он будет иметь приоритет 4 (обычно это наивысший приоритет, более высокий имеют только данные протокола, однако если мы выберем более высокий приоритет, при

передаче очень больших объемов групповых данных протокол коммутатора может работать неправильно).

20.1.4 Устранение неполадок IPv6 DCSCM

Модуль DCSCM реализует функции, подобные спискам доступа ACL. Проблемы возникают в основном в связи с неправильными настройками. Пожалуйста внимательно изучите приведенные выше инструкции.

20.2 Протокол MLD Snooping

20.2.1 Начальные сведения о протоколе MLD Snooping

Протокол MLD (Multicast Listener Discovery Protocol — протокол управления обнаружением с помощью прослушивания) используется для управления групповым IPv6-трафиком. Протокол MLD используется сетевыми устройствами, поддерживающими групповой трафик (например, маршрутизаторами) для прослушивания сети и обнаружения. Он также используется хостами, желающими вступить в группу и прослушивающих сеть для информирования маршрутизатора о доступности пакетов с некоторым групповым адресом. Все эти операции выполняются путем обмена сообщениями MLD. Маршрутизатор отправляет сообщения с запросами о наличии в сети членов групп (MLD Multicast listener Query message) по групповому адресу (а именно ff02::1), доступному всем хостам, прослушивающим сеть. Если хост желает вступить в группу, он отвечает по групповому адресу этой группы уведомлением о наличии в сети члена группы MLD.

MLD Snooping еще называют прослушиванием MLD. С помощью MLD Snooping коммутатор предотвращает веерную рассылку группового трафика, так как этот трафик передается только в порты, ассоциированные с групповыми устройствами. Коммутатор «прослушивает» сообщения MLD, обмен которыми идет между групповым маршрутизатором и хостами, и корректирует групповую таблицу передачи на основе результатов прослушивания. Затем он может принять решение осуществить передачу пакетов в соответствии с таблицей передачи.

Коммутаторы поддерживают MLD Snooping, так как поддерживают протокол MLD v2. Поэтому пользователь может использовать коммутатор для групповой рассылки сообщений по протоколу IPv6.

20.2.2 Последовательность настройки MLD Snooping

1. Включение протокола MLD Snooping
2. Настройка протокола MLD Snooping

1. Включение протокола MLD Snooping

Команда	Описание
Глобальный режим конфигурирования	
ipv6 mld snooping **no ipv6 mld snooping**	Включает функцию MLD Snooping. Отмена команды: “no ipv6 mld snooping” выключает функцию MLD Snooping
ipv6 mld snooping vlan <vlan-id> **no ipv6 mld snooping vlan** <vlan-id>	Включает функцию MLD Snooping на указанном VLAN. Отмена команды: “no ipv6 mld snooping vlan <vlan-id>” восстанавливает настройки, используемые по умолчанию

2. Настройка протокола MLD Snooping

Команда	Описание
Глобальный режим конфигурирования	
ipv6 mld snooping vlan <vlan-id> **limit** {**group** <g_limit> | **source** <s_limit>} **no ipv6 mld snooping vlan** <vlan-id> **limit**	Позволяет задать максимальное число групп MLD snooping, в которые может вступить хост, и максимальное число источников, которые может иметь группа. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> limit ” восстанавливает настройки, используемые по умолчанию
ipv6 mld snooping vlan <vlan-id> **l2-general-querier** **no ipv6 mld snooping vlan** <vlan-id> **l2-general-querier**	Устанавливает указанный VLAN как маршрутизатор уровня 2. Рекомендуется, чтобы в каждом сегменте мог быть сконфигурирован маршрутизатор уровня 2. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> l2-general-querier” отменяет конфигурацию маршрутизатора уровня 2

ipv6 mld snooping vlan <vlan-id> **mrouter-port interface** <interface-name> **no ipv6 mld snooping vlan** <vlan-id> **mrouter-port interface** <interface-name>	Позволяет задать статический порт mrouter. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> mrouter-port interface <interface-name>” отменяет конфигурацию порта mrouter
ipv6 mld snooping vlan <vlan-id> **mrpt** <value> **no ipv6 mld snooping vlan** <vlan-id> **mrpt**	Позволяет задать срок жизни порта the mrouter. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> mrpt” восстанавливает настройки, используемые по умолчанию
ipv6 mld snooping vlan <vlan-id> **query-interval** <value> **no ipv6 mld snooping vlan** <vlan-id> **query-interval**	Позволяет задать интервал отправки запросов. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> query-interval” восстанавливает настройки, используемые по умолчанию
ipv6 mld snooping vlan <vlan-id> **immediate-leave** **no ipv6 mld snooping vlan** <vlan-id> **immediate-leave**	Позволяет задать MLD snooping для указанного VLAN, чтобы включить функцию временного выхода. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> immediate-leave” выключает функцию временного выхода
ipv6 mld snooping vlan <vlan-id> **query-mrsp** <value> **no ipv6 mld snooping vlan** <vlan-id> **query-mrsp**	Позволяет задать максимальное время ожидания ответа на запрос. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> query-mrsp” восстанавливает настройки, используемые по умолчанию
ipv6 mld snooping vlan <vlan-id> **query-robustness** <value> **no ipv6 mld snooping vlan** <vlan-id> **query-robustness**	Позволяет задать надежность (robustness). Отмена команды: “no ipv6 mld snooping vlan <vlan-id> query-robustness” восстанавливает настройки, используемые по умолчанию
ipv6 mld snooping vlan <vlan-id> **suppression-query-time** <value> **no ipv6 mld snooping vlan** <vlan-id> **suppression-query-time**	Позволяет задать время подавления запроса. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> suppression-query-time” восстанавливает настройки, используемые по умолчани
Ipv6 mld snooping vlan <vlan-id> **static-group** <X:X::X:X> [**source** <X:X::X:X>] **interface** [**ethernet** | **port-channel**] <IFNAME> **no ipv6 mld snooping vlan** <vlan-id> **static-group** <X:X::X:X> [**source** <X:X::X:X>] **interface** [**ethernet** | **port-channel**] <IFNAME>	Позволяет задать в указанном порту статическую группу. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source <X:X::X:X>] interface [ethernet | port-channel] <IFNAME>” отменяет сделанные настройки

20.2.3 Примеры применения MLD Snooping

Пример 1: Функция MLD Snooping (Рис. 42)

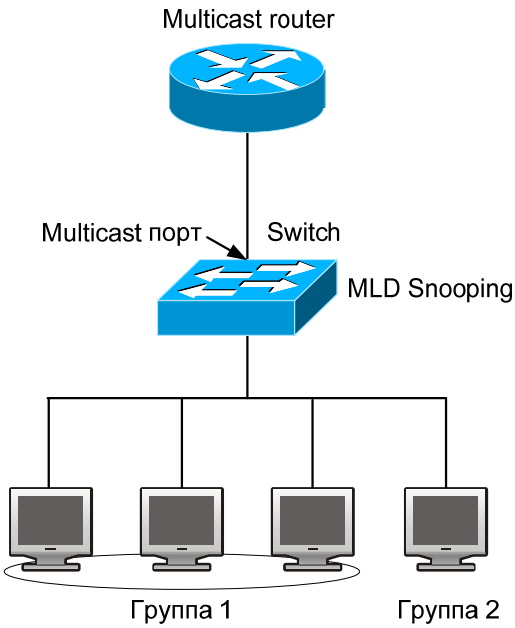

Рис. 42. Включение функции коммутатора MLD Snooping

Как показано на рисунке, на коммутаторе сформирован VLAN 100 с портами 1, 2, 6, 10 и 12. К портам 2, 6, 10, 12 подключны четыре хоста, а к порту 1 — групповой маршрутизатор. Так как MLD Snooping по умолчанию выключен (либо на коммутаторе, либо в сетях VLAN), то для включения MLD Snooping на VLAN 100, MLD Snooping должен быть сначала включен в глобальном режиме конфигурирования коммутатора; после включения MLD Snooping на VLAN 100, ее порт 1 можно установить как порт M-Router. Процедура настройки:

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

Настройка групповой рассылки сообщений:

Предположим, что имеются два сервера групповой рассылки сообщений: Групповой сервер 1 и Групповой сервер 2. Групповой сервер 1 рассылает программы 1 и 2, а Групповой сервер 2 — программу 3. Серверы используют групповые адреса групп 1, 2 и 3 соответственно. На четырех хостах одновременно функционирует групповое ПО. Два хоста, подключенные к портам 2 и 5 заказали программу 1; один хост, подключенный к порту 10 заказал программу 2; один хост, подключенный к порту 12, заказал программу 3.

Прослушивание при MLD Snooping даст следующий результат:

Протоколом IGMP Snooping на VLAN 100 будет построена таблица групп, в которой порты 1, 2, 6 будут присвоены группе 1 группового сервера 1, порты 1, 10 будут присвоены группе 2 группового сервера 1, а порты 1, 12 — группе 3 группового сервера 2.

Все четыре хоста смогут принимать заказанные программы: Порты 2, 6 не будут принимать трафик программ 2 и 3; порт 10 не будет принимать трафик программ 1 и 3; порт 12 не будет принимать трафик программ 1 и 2.

Пример 2: MLD-маршрутизатор уровня 2 (Рис. 43)

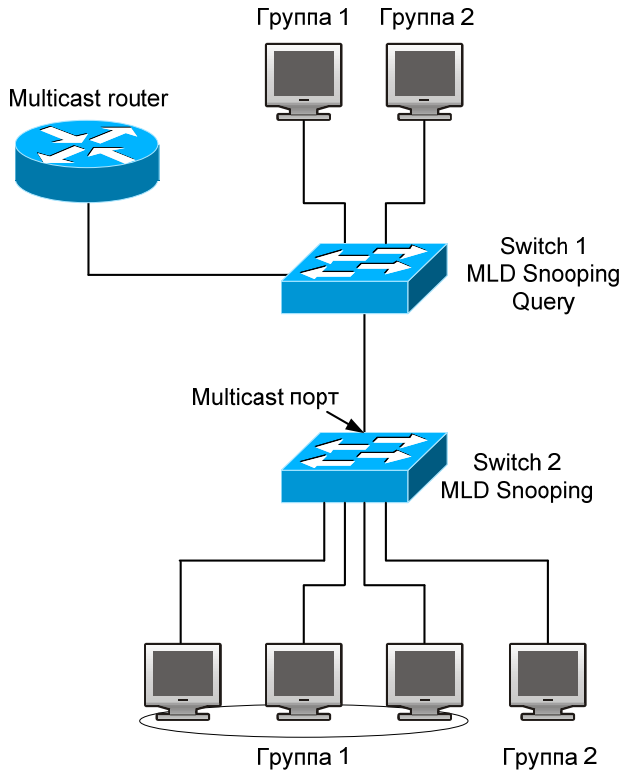

Рис. 43. Использование коммутаторов в качестве маршрутизаторов MLD

Конфигурация коммутатора Switch 2 такая же, как и в примере 1. Место группового маршрутизатора спримера 1 занимает Switch 1. Предположим, что на Switch 1 сформирован VLAN 60 с портами 1, 2, 10 и 12. Порт 1 подключен к групповому серверу, порт 2 — к коммутатору Switch 2. Для регулярной отправки запросов, MLD Snooping должен быть включен в глобальном режиме конфигурирования и на VLAN60 должен быть сформирован MLD-маршрутизатор уровня 2.

Процедура настройки:
Switch1#config
Switch1(config)#ipv6 mld snooping
Switch1(config)#ipv6 mld snooping vlan 60
Switch1(config)#ipv6 mld snooping vlan 60 l2-general-querier
Switch2#config
Switch2(config)#ipv6 mld snooping
Switch2(config)#ipv6 mld snooping vlan 100
Switch2(config)#ipv6 mld snooping vlan 100 mrouter interface ethernet 0/0/1

Конфигурация групповой рассылки: Такая же, как в примере 1.

Результат прослушивания MLD Snooping: Такой же, как в примере 1

Пример 3: совместная работа с групповыми протоколами уровня 3.

Коммутатор из примера 1 заменен маршрутизатором с теми же настройками. Настройки групповой рассылки и IGMP snooping те же, что и в примере 1. Настроим PIM-SM6 на маршрутизаторе и включим PIM-SM6 на vlan 100 (будем использовать тот же режим PIM с подключенным групповым маршрутизатором). Последовательность настройки следующая:
switch#config
switch(config)#ipv6 pim multicast-routing
switch(config)#interface vlan 100
switch(config-if-vlan100)#ipv6 pim sparse-mode

Когда включен групповой протокол уровня 3, MLD snooping не распределяет групповые пакеты. Он выполняет только следующие задачи:

- Удаляет групповые пакеты уровня 2.
- Выполняет функции маршрутизатора для уровня 3 с VLAN, при этом S и G используются, как параметры.
- Когда MLD уровня 3 выключен, снова начинается распределение групповых пакетов уровня 2.

- Рассматривая пакеты IP6MC уровня 3, можно обнаружить, что порты могут быть определены по групповым пакетам уровня 3.

Это гарантирует, что MLD snooping будет работать совместно с групповыми протоколами уровня 3.

20.2.4 Устранение неполадок MLD Snooping

В процессе настройки и использования функции MLD Snooping администраторы могут обнаружить, что сервер MLD Snooping работает неправильно — вероятно, из-за неправильно выполненных физических соединений или настройки.

Пользователь должен гарантировать следующее:

- Правильность физических соединений;
- MLD Snooping должен быть включен в глобальном режиме конфигурирования (командой ipv6 mld snooping)

Настройка Vlan (командой ipv6 mld snooping vlan <vlan-id>) должна выполняться, когда MLD Snooping уже включен в глобальном режиме конфигурирования.

Vlan используется в качестве маршрутизатора уровня 2 либо в том же сегменте задан статический mrouter.

Проверить правильность информации MLD Snooping с помощью команды show.

Если все вышеперечисленные меры не помогают решить проблемы, возникшие с MLD Snooping, попробуйте использовать команды отладки (”debug mld snooping”), затем скопируйте отладочную информацию, выведенную за 3 минуты и перешлите ее в отдел технической поддержки компании Zelax.

21 Настройка групповых VLAN

21.1 Начальные сведения о групповых VLAN

В соответствии с используемым в настоящее время методом заказа групповых программ, когда пользователи, принадлежащие различных VLAN, заказывают программы, каждый VLAN копирует в себя групповой поток. Этот метод приводит к значительным расходам пропускной способности. Сконфигурировав групповые VLAN, можно добавить в них порты коммутатора, а затем включить функцию IGMP Snooping или MLD Snooping. Теперь пользователи различных VLAN смогут совместно использовать групповые VLAN, и передача группового потока происходит только в пределах одного группового VLAN. Таким образом, будет достигнута большая экономия пропускной способности. Так как групповой VLAN и VLAN пользователя полностью изолированы, гарантируется и требуемый уровень безопасности, и требуемая пропускная способность. После того, как групповой VLAN сконфигурирован, можно гарантировать, что поток групповой информации будет посылаться пользователям без задержки.

21.2 Последовательность настройки группового VLAN

1. Включение функции группового VLAN
2. Настройка протокола IGMP Snooping
3. Настройка протокола MLD Snooping

1. Включение функции группового VLAN

Команда	Описание
Режим настройки VLAN	
multicast-vlan **no multicast-vlan**	Позволяет включить для VLAN режим группового VLAN. Команда ”no multicast-vlan” выключает режим групповой VLAN
multicast-vlan association <vlan-list> **no multicast-vlan association** <vlan-list>	Ассоциирует групповой VLAN с другими VLAN. Отмена команды: ”no multicast-vlan association <vlan-list>” удаляет ассоциированные связи сетей VLAN с групповым VLAN

2. Настройка протокола IGMP Snooping

Команда	Описание
Глобальный режим конфигурирования	
ip igmp snooping vlan <vlan-id> **no ip igmp snooping vlan** <vlan-id>	Включает функцию IGMP Snooping на групповом VLAN: Отмена команды: “no ip igmp snooping vlan <vlan-id> ” выключает функцию IGMP Snooping на групповом VLAN
ip igmp snooping **no ip igmp snooping**	Включает функцию IGMP Snooping. Отмена команды: “no ip igmp snooping” выключает функцию IGMP Snooping

3. Настройка протокола MLD Snooping

Команда	Описание
Глобальный режим конфигурирования	
ipv6 mld snooping vlan <vlan-id> **no ipv6 mld snooping vlan** <vlan-id>	Включает функцию MLD Snooping на групповом VLAN. Отмена команды: “no ipv6 mld snooping vlan <vlan-id> ” выключает функцию MLD Snooping на групповом VLAN
ipv6 mld snooping **no ipv6 mld snooping**	Включает функцию MLD Snooping. Отмена команды: “no ipv6 mld snooping” выключает функцию MLD Snooping

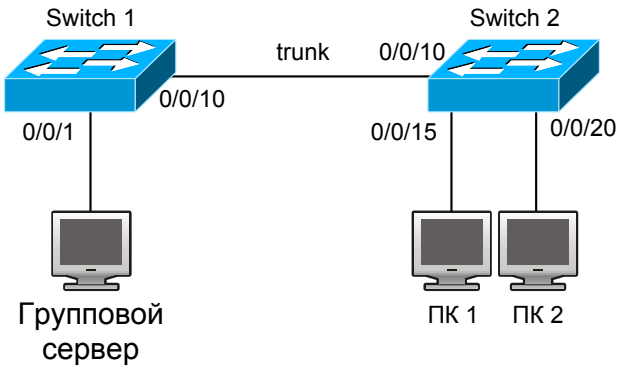

Рис. 44. Функциональная схема групповой VLAN

Как показано на Рис. 44, групповой сервер подключен к коммутатору 3 уровня switch 1 через порт 0/0/1; порт 0/0/1 принадлежит VLAN 10 коммутатора. Коммутатор 3 уровня switch 1 подключен к коммутатору уровня 2 switch 2 через порт 0/0/10, который сконфигурирован, как trunk. VLAN 100 коммутатора switch 2 содержит порт 0/0/15, VLAN 101 содержит порт 0/0/20.

ПК 1 и ПК 2 подключены соответственно к портам 0/0/15 и 0/0/20.

Коммутатор switch 2 соединен с коммутатором switch 1 через порт 0/0/10, который сконфигурирован, как магистральный.

VLAN 20 является групповым VLAN. Сконфигурировав групповой VLAN, мы можем обеспечить прием с него групповых данных на ПК 1 и ПК 2.

В процедуре настройки, приведенной ниже, допускается, что IP-адрес коммутатора switch 1 установлен и все устройства соответствующим образом соединены.

Процедура настройки:

```
Switch1#config
Switch1(config)#vlan 10
Switch1(config-vlan10)#switchport access ethernet 0/0/1
Switch1(config-vlan10)exit
Switch1(config)#interface vlan 10
Switch1(config-if-vlan10)#ip pim dense-mode
Switch1(config-if-vlan10)#exit
Switch1(config)#vlan 20
Switch1(config-vlan20)#exit
Switch1(config)#interface vlan 20
Switch1(config-if-vlan20)#ip pim dense-mode
Switch1(config-if-vlan20)#exit
Switch1(config)#ip pim multicast
Switch1(config)# interface ethernet0/0/10
Switch1(config-if-ethernet0/0/10)switchport mode trunk

Switch2#config
Switch2(config)#vlan 100
Switch2(config-vlan100)#Switchport access ethernet 0/0/15
Switch2(config-vlan100)exit
Switch2(config)#vlan 101
Switch2(config-vlan101)#Switchport access ethernet 0/0/20
Switch2(config-vlan101)exit
Switch2(config)# interface ethernet 0/0/10
Switch2(config-if-ethernet0/0/10)#Switchport mode trunk
Switch2(config-if-ethernet0/0/10)#exit
Switch2(config)#vlan 20
Switch2(config-vlan20)#multicast-vlan
Switch2(config-vlan20)#multicast-vlan association 100,101
Switch2(config-vlan20)#exit
Switch2(config)#ip igmp snooping
Switch2(config)#ip igmp snooping vlan 20
```

Когда групповой VLAN поддерживает IPv6, она используется так же, как и при IPv4, за исключением того, что применяется MLD Snooping.