Коммутаторы серии RS-XXXX

Руководство по эксплуатации

Оглавление

1 БАЗОВАЯ КОНФИГУРАЦИЯ..... 5
1.1 УПРАВЛЕНИЕ КОММУТАТОРОМ 5
1.1.1 Варианты Управления 5
1.1.2 CLI-интерфейс 9
1.2 ОСНОВНЫЕ НАСТРОЙКИ КОММУТАТОРА 13
1.2.1 Основные настройки 13
1.2.2 Управление Telnet 14
1.2.3 Настройка IP-адресов коммутатора 16
1.2.4 Настройка SNMP 17
1.2.5 Обновление ПО 22

2 КОНФИГУРИРОВАНИЕ ПОРТОВ 31
2.1 КОНФИГУРИРОВАНИЕ ПОРТОВ 31
2.1.1 Введение 31
2.1.2 Список команд для конфигурирования портов 31
2.1.3 Примеры конфигурации порта 33
2.1.4 Устранение неисправностей на порту 34
2.2 PORT ISOLATION. КОНФИГУРАЦИЯ ФУНКЦИИ ИЗОЛЯЦИИ ПОРТОВ 34
2.2.1 Введение в функцию изоляции портов 34
2.2.2 Список команд для конфигурации изоляции портов 34
2.2.3 Типовые примеры функции изоляции портов 35
2.3 КОНФИГУРАЦИЯ ФУНКЦИИ РАСПОЗНАВАНИЯ ПЕТЛИ НА ПОРТУ 35
2.3.1 Введение в функцию распознавания петли 35
2.3.2 Список команд для конфигурирования функции распознавания петли на порту 36
2.3.3 Примеры функции распознавания петли на порту 37
2.3.4 Решение проблем с функцией распознавания петли на порту 38
2.4 КОНФИГУРАЦИЯ ФУНКЦИИ udld 38
2.4.1 Общая информация о udld 38
2.4.2 Список команд для конфигурирования udld 39
2.4.3 Типовые примеры конфигурации udld 42
2.4.4 Устранение неполадок функции udld 42
2.5 НАСТРОЙКА ФУНКЦИИ LLDP 43
2.5.1 Общие сведения о функции LLDP 43
2.5.2 Список команд для конфигурирования LLDP 44
2.5.3 Типовой пример конфигурации LLDP 46
2.5.4 Устранение неисправностей функции LLDP 47
2.6 PORT CHANNEL. НАСТРОЙКА АГРЕГИРОВАНИЯ ПОРТОВ 47
2.6.1 Агрегирование портов. Общие сведения о Port channel 47
2.6.2 Общие сведения о LACP 48
2.6.3 Настройка Port channel 49
2.6.4 Примеры использования Port channel 50
2.6.5 Устранение неисправностей Port channel 52
2.7 КОНФИГУРИРОВАНИЕ MTU 52
2.7.1 Общие сведения об MTU 52
2.7.2 Конфигурирование MTU 53
2.8 ФУНКЦИЯ PORT-SECURITY. БЕЗОПАСНОСТЬ ПОРТОВ 53
2.8.1 Введение 53
2.8.2 Настройка безопасности портов 53
2.8.3 Примеры настройки Port-security 54
2.8.4 Устранение неисправностей PORT SECURITY 55
2.9 НАСТРОЙКА DDM 55
2.9.1 Введение 55
2.9.2 Список команд конфигурации DDM 57
2.9.3 Примеры применения DDM 57
2.9.4 Устранение неисправностей DDM 58
2.10 СТАТИСТИКА ПО ПОРТАМ 59

3 НАСТРОЙКА ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ (VLAN) И НАСТРОЙКА MAC ..60
3.1 Конфигурирование VLAN 60
3.1.1 Начальные сведения о VLAN 60
3.1.2 Конфигурирование VLAN 61
3.1.3 Пример типичного применения VLAN 63
3.1.4 Пример типичного применения гибридных (Hybrid) портов 65
3.2 Конфигурирование туннеля Dot1Q 66

3.2.1 Общие сведения о туннелях Dot1q....66
3.2.2 Конфигурирование туннеля Dot1q....67
3.2.3 Пример типичного применения туннеля Dot1q....68
3.2.4 Устранение неисправностей туннеля Dot1q....68
3.3 Настройка VLAN-translation....69
3.3.1 Общие сведения о трансляции VLAN'ов....69
3.3.2 Конфигурирование трансляции VLAN'а....69
3.3.3 Типовое применение трансляции VLAN'ов....69
3.3.4 Устранение неисправностей трансляции VLAN'ов....70
3.4 Конфигурация Multi-to-One VLAN-translation....70
3.4.1 Введение в Multi-to-One VLAN-трансляцию....70
3.4.2 Настройка передачи Multi-to-One VLAN....70
3.4.3 Пример типичного применения трансляции Multi-to-One VLAN....71
3.4.4 Устранение неисправностей Multi-to-One VLAN-трансляции....72
3.5 НАСТРОЙКА ТАБЛИЦЫ MAC-АДРЕСОВ....72
3.5.1 Общие сведения о таблице MAC-адресов....72
3.5.2 Конфигурирование таблицы MAC-адресов....74
3.5.3 Примеры типичной конфигурации....76
3.5.4 Устранение неисправностей, связанных с таблицей MAC-адресов....77
3.5.5 Дополнительные функции таблицы MAC-адресов....77
3.6 Динамический VLAN....79
3.6.1 Общие сведения о Динамическом VLAN....79
3.6.2 Конфигурация динамических VLAN....79

4 QoS И ПЕРЕНАПРАВЛЕНИЕ ПОТОКОВ....81
4.1 НАСТРОЙКА QOS....81
4.1.1 Общие сведения о QoS....81
4.1.2 Конфигурирование QoS....86
4.1.3 Пример QoS....90
4.1.4 Устранение неисправностей QoS....92

5 МАРШРУТИЗАЦИЯ И ARP, ND....93
5.1 КОНФИГУРИРОВАНИЕ ФУНКЦИЙ 3-ГО УРОВНЯ....93
5.1.1 Интерфейс 3-го уровня....93
5.1.2 Настройка протокола IP....93
5.1.3 ARP....96
5.2 НАСТРОЙКА ФУНКЦИИ ПРЕДОТВРАЩЕНИЯ ARP-СКАНИРОВАНИЯ....96
5.2.1 Введение в функцию предотвращения ARP-сканирования....96
5.3 КОНФИГУРАЦИЯ ЗАЩИТЫ ОТ ПОДМЕНЫ ARP (ARP Spoofing)....97
5.3.1 Обзор....97
5.3.2 Конфигурация предотвращения подмены ARP....97
5.3.3 Пример предотвращения подмены ARP, ND....98
5.4 НАСТРОЙКА DYNAMIC ARP INSPECTION (DAI)....99
5.4.1 Введение в ARP INSPECTION....99
5.4.2 Настройка Dynamic ARP inspection....99

6 КОНФИГУРАЦИЯ DHCP....101
6.1 КОНФИГУРАЦИЯ DHCP....101
6.1.1 Введение DHCP....101
6.1.2 Конфигурация DHCP-сервера....102
6.1.3 Примеры конфигурации DHCP....104
6.1.4 Поиск неисправностей DHCP....105
6.2 КОНФИГУРАЦИЯ ОПЦИИ 82 DHCP....105
6.2.1 Введение в опцию 82 DHCP....105
6.2.2 Конфигурирование опции 82 DHCP....107
6.2.3 Примеры применения опции 82 DHCP....109
6.2.4 Поиск неисправностей опции 82 DHCP....110
6.3 КОНФИГУРАЦИЯ DHCP SNOOPING....110
6.3.1 Введение в DHCP Snooping....110
6.3.2 Последовательность конфигурации DHCP Snooping....111
6.3.3 Типовое применение DHCP Snooping....116
6.3.4 Устранение неисправностей DHCP Snooping....116

7 Безопасность....117
7.1 TACACS+....117
7.1.1 Общие сведения о TACACS+....117
7.1.2 Конфигурация TACACS+....117

7.1.3 Пример типичной конфигурации TACACS+ 118
7.1.4 Устранение проблем при конфигурации TACACS+ 118
7.2 RADIUS 119
7.2.1 Общие сведения о RADIUS 119
7.2.2 Конфигурация RADIUS 120
7.2.3 Примеры типовой настройки RADIUS 122
7.2.4 Устранение проблем при конфигурации RADIUS 123
7.3 PPPoE Intermediate Agent 123
7.3.1 Общие сведения о PPPoE Intermediate Agent 123
7.3.2 Конфигурация PPPoE Intermediate Agent 124
7.3.3 Пример конфигурации PPPoE Intermediate Agent 126

8 ЗЕРКАЛИРОВАНИЕ ТРАФИКА 127
8.1 Зеркалирование трафика (SPAN) 127
8.1.1 Общие сведения о зеркалировании трафика 127
8.1.2 Конфигурация SPAN 127
8.1.3 Пример конфигурации SPAN 128
8.1.4 Решение проблем при зеркалировании трафика 128

9 Конфигурация NTP 129
9.1 NTP 129
9.1.1 Общие сведенья о NTP 129
9.1.2 Конфигурация NTP 129
9.1.3 Пример конфигурации NTP 130
9.1.4 Устранение неработоспособности функции NTP 130
9.2 Летнее время 131
9.2.1 Общие сведения о летнем времени 131
9.2.2 Конфигурация летнего времени 131
9.2.3 Пример конфигурации функции летнего времени 131
9.2.4 Устранение неработоспособности функции летнего времени 131

10 НАСТРОЙКА POE 132
10.1 Приоритезация портов PoE 132
10.2 Повышенный пусковой ток 132

11 ОБЩАЯ ИНФОРМАЦИЯ 133
11.1 Замечания и предложения 133
11.2 Техническая поддержка 133

1 БАЗОВАЯ КОНФИГУРАЦИЯ

1.1 УПРАВЛЕНИЕ КОММУТАТОРОМ

1.1.1 Варианты Управления

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

1.1.1.1 Out-Of-Band Management. Внеполосное управление.

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

Процедура управления коммутатором через консольный интерфейс, описана ниже:

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

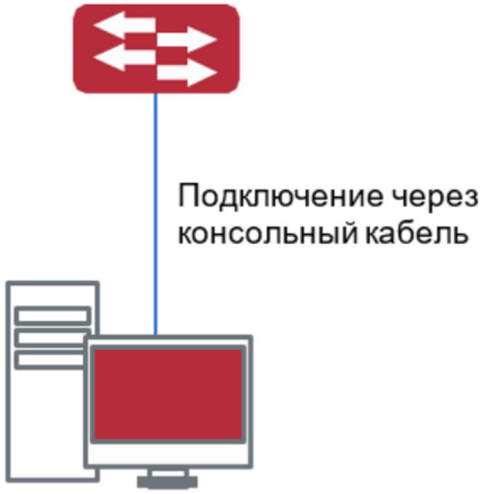


Рисунок 1.1 – Подключение ПК к консольному порту коммутатора

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

Название устройства	Описание
Персональный компьютер (PC)	Имеет функциональную клавиатуру и порт RS-232, с установленным эмулятором терминала, таким как HyperTerminal или стороннюю программу эмуляции терминала (Putty, Minicom или др.)
Коммутатор	Требуется работающий консольный порт.
Кабель серийного порта	Один конец подключается к серийному порту RS-232, а другой к порту консоли. Приотсутствии серийного порта RS-232 на ПК допустается использование USB – RS-232 адаптера

Шаг 2: Включение и настройка эмулятора терминала

Запустить программу эмуляции терминала (Putty, Minicom, HyperTerminal) и произвести следующие настройки:

1. Выбрать соответствующий Serial порт компьютера.
2. Установить скорость передачи данных 115200.
3. Задать формат данных: 8 бит данных, 1 стоповый бит, без контроля четности.
4. Отключить аппаратное и программное управление потоком данных.

Включите коммутатор, после чего в окне эмулятора терминала должно появиться следующее сообщение – это режим конфигурации для коммутатора.

> *Login:*

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

Имя пользователя и пароль, установленные по-умолчанию, указаны на этикетке коммутатора.

1.1.1.2 In-band Management. Внутриполосное управление.

In-band управление относится к удалённому управлению посредством доступа к коммутатору с использованием таких протоколов как Telnet, SSH, HTTP, а также SNMP. В случаях, когда In-band управление из-за изменений, сделанных в конфигурации коммутатора, работает со сбоями, для управления и конфигурирования коммутатора можно использовать Out-band управление (Console/Management port).

1.1.1.2.1 Управление по Telnet

Для управления коммутатором по Telnet, должны выполняться следующие условия:

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

Коммутатор третьего уровня может быть настроен с несколькими IPv4/IPv6-адресами, метод настройки описан в посвященной этому главе.

Следующий пример предполагает состояние коммутатора после поставки с заводскими настройками, где присутствует только VLAN1.

Последующие шаги описывают подключение Telnet-клиента к интерфейсу VLAN1 коммутатора посредством Telnet (пример адреса IPv4):

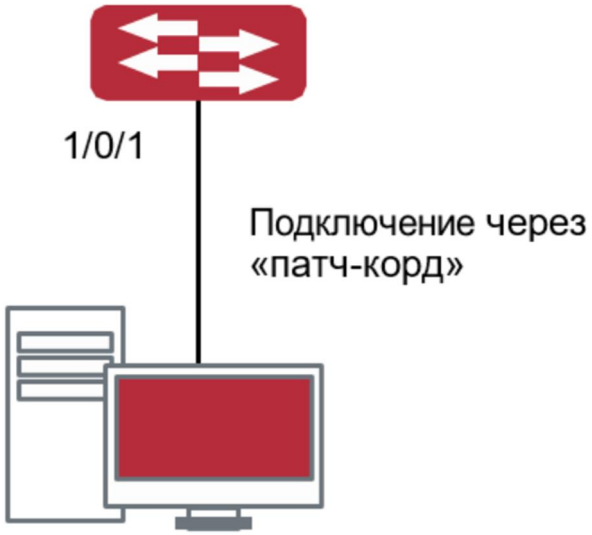


Рисунок 1.2 – Управление коммутатором по Telnet

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

- Первым делом идет настройка IP-адреса хоста. Он должен быть в том же сегменте сети, что и IP-адрес VLAN1 интерфейса коммутатора. Предположим, что IP-адрес интерфейса VLAN1 коммутатора 192.168.17.7/24. Тогда IP-адрес хоста может быть 192.168.17.252/24. С помощью команды «ping 192.168.17.7» можно проверить, доступен коммутатор или нет.
- Команды настройки IP-адреса для интерфейса VLAN1 указаны ниже. Перед началом In-band управления, IP-адрес коммутатора должен быть настроен посредством Out-band управления (например, через порт Console). Команды конфигурирования следующие (Далее считается, что все приглашения режима конфигурирования коммутатора начинаются со слова «rotek», если отдельно не указано иного):

```
rotek>enable rotek#config
rotek(config)#interface vlan 1
rotek(Config-if-Vlan1)#ip address 192.168.1.2 255.255.255.0
rotek(Config-if-Vlan1)#no shutdown
```

Для активации функции Telnet-сервера пользователь должен включить её в режиме глобального конфигурирования, как показано ниже:

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

Шаг 2: Запуск программы Telnet Client

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

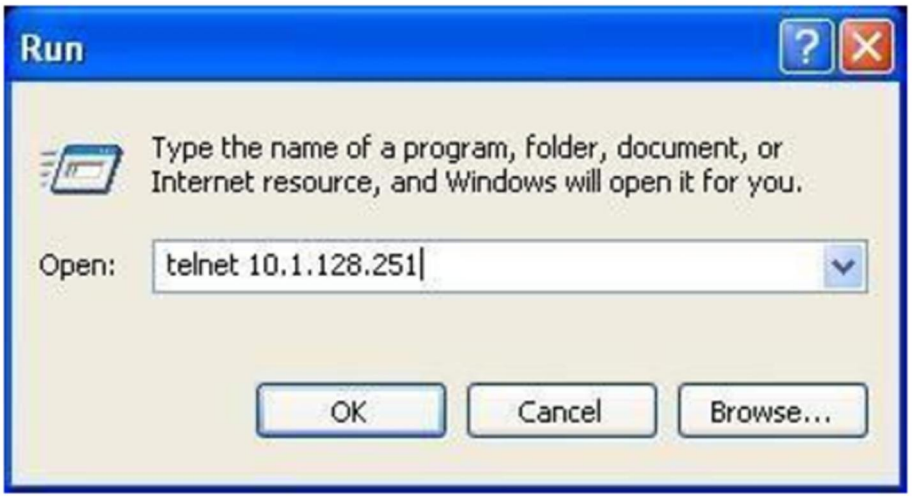


Рисунок 1.3 – Запуск программы Telnet-клиент в Windows.

Шаг 3: Получить доступ к коммутатору.

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

> *«username <username> privilege <privilege> [password (0|7) <password>]».*

Для локальной аутентификации можно использовать следующую команду:

> *authentifcation line vty login local.*

Для доступа в привилегированный режим необходимо и задан уровень привилегий 15.

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

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

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



Рисунок 1.4 – Настройка Telnet-интерфейса

1.1.1.2.2 Управление коммутатором через сетевое управление SNMP

Необходимые требования:

1. Коммутатор должен иметь сконфигурированный IPv4/IPv6-адрес.
2. IP-адрес хоста (HTTP-клиент) и VLAN-интерфейс коммутатора, должны иметь IPv4/IPv6-адреса в одном сегменте сети.

3. Если второй пункт не может быть выполнен, HTTP-клиент должен быть подключен к IPv4/IPv6-адресу коммутатора с других устройств, таких как роутер.

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

1.1.2 CLI-интерфейс

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

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

Возможности Shell для коммутаторов описаны ниже:

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

1.1.2.1 Режимы настройки

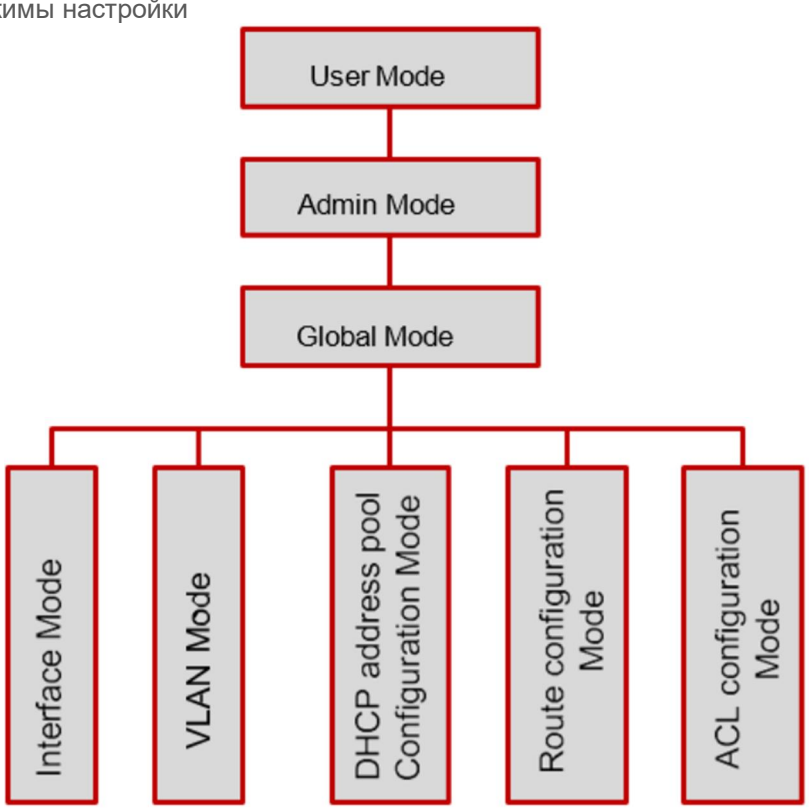


Рисунок 1.5 – Режимы настройки Shell

1.1.2.1.1 Режим пользователя

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

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

1.1.2.1.2 Режим администратора

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

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

1.1.2.1.3 Режим глобального конфигурирования.

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

режим глобального конфигурирования. Пользователь может выполнять глобальные настройки конфигурации в этом режиме, такие как настройка таблиц MAC-адресов, зеркалирование портов, создание VLAN, запуск IGMP Snooping и STP, и т. д. Также пользователь может войти в режим конфигурирования порта для настройки всех интерфейсов.

1.1.2.1.3.1 Режим конфигурирования интерфейса

Использование команды интерфейса в режиме глобального конфигурирования позволяет входить в режим конфигурирования указанного интерфейса. Коммутатор поддерживает три типа интерфейсов: 1. VLAN; 2. Ethernet-порт.

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

1.1.2.1.3.2 Режим VLAN

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

1.1.2.2 Настройка синтаксиса

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

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

Расшифровка: **cmdtxt** жирным шрифтом указывает на ключевое слово команды;

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

Вот примеры некоторых актуальных команд конфигурации:

> *show version, параметры не требуется. Это команда, состоящая только из ключевых слов и без параметров.*
> *vlan <vlan-id>, необходим ввод значения параметров после ключевого слова.*
> *firewall {enable | disable}, этой командой пользователь может включить или выключить брандмауэр, следует лишь выбрать нужный параметр.*

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

> *snmp-server community ro public*
> *snmp-server community rw private*

1.1.2.3 Сочетания клавиш

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

Клавиша (и)	Функция	
Back Space	Удалить символ перед курсором. Курсор перемещается назад.	
Вверх «↑»	Показать предыдущую введенную команду. Отображение до десяти недавно набранных команд.	
Вниз «↓»	Показать следующую введенную команду. При использовании клавиши вверх «↑», вы получаете ранее введенные команды, при использовании клавиши вниз «↓», вы возвращаетесь к следующей команде.	
Влево «←»	Курсор перемещается на один символ влево.	Вы можете использовать клавиши влево «←» и вправо «→» для изменения введенных команд.
Вправо «→»	Курсор перемещается на один символ вправо.	
Ctrl +z	Вернуться в Режим администратора непосредственно из других режимов настройки (за исключением пользовательского режима)	
Ctrl +c	Остановка непрерывных процессов команд, таких как ping и т.д.	
Tab	В процессе ввода команды Tab может быть использован для ее завершения, если нет ошибок.	

1.1.2.4 Справка

Существуют способ получить доступ к справочной информации: Командой «?».

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

1.1.2.5 Проверка ввода

1.1.2.5.1 Отображаемая информация: успешное выполнение (successfull)

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

1.1.2.5.2 Отображаемая информация: ошибочный ввод (error)

Отображаемое сообщение ошибки	Пояснение
Parse error	Введенной команды не существует или есть ошибка в параметре масштаба, типа или формата.
Invalid command or parameter	Команда существует (признается), но задан неправильный параметр.
Incomplete command	Команда существует (признается),но введены не все необходимые параметры
This command is not existing in current mode	Команда существует (признается), но не может быть использована в данном режиме.

1.1.2.6 Поддержка языка нечеткой логики (Fuzzy math)

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

> Команда «show interface ethernet status», будет работать даже в том случае, если набрать «sh in ethernet status».

Однако, при наборе команды «show running-config» как «show r» система сообщит «Incomplete command», т.к. Shell будет не в состоянии определить, что имелось ввиду «show radius» или «show running-config». Таким образом, Shell сможет правильно распознать команду только если будет набрано «sh ru»

1.2 ОСНОВНЫЕ НАСТРОЙКИ КОММУТАТОРА

1.2.1 Основные настройки

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

Команда	Пояснение
Обычный пользовательский режим/Режим администратора	
Enable [<1-15>] disable	Пользователь использует команду enable для того, чтобы войти в режим администратора. А команду disable для выхода из него.
Режим администратора	
config [terminal]	Входит в режим глобального конфигурирования из режима администратора.
Различные режимы	
exit	Выход из текущего режима и вход в предыдущий режим, например, если применить эту команду в режиме глобального конфигурирования, то она вернет вас в режим администратора,

	если набрать еще раз (уже находясь в режиме администратора), то попадете в пользовательский режим.
show privilege	Показывает привилегии для определенных пользователей
Расширенный пользовательский режим/Режим администратора	
end	Выход из текущего режима и возвращение в режим администратора, только когда пользователь находится не в пользовательском/администраторском режимах.
Режим администратора	
clock set <HH:MM:SS> [YYYY.MM.DD]	Установка даты и времени.
show version	Отображение версии коммутатора.
write	Сохраняет текущую конфигурацию на Flash-память.
reload	Перезагрузка коммутатора.
show cpu usage	Показывает степень использования CPU.
show memory usage	Показывает степень использования памяти.

1.2.2 Управление Telnet

1.2.2.1 Telnet

1.2.2.1.1 Введение в Telnet

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

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

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

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

1.2.2.1.2 Команды конфигурирования Telnet

1. Настройка Telnet-сервера.

1. Настройка Telnet-сервера.

Команда	Описание
Режим глобального конфигурирования	
telnet-server enable no telnet-server enable	Активирует функцию Telnet-сервера на коммутаторе, команда «no» деактивирует эту функцию.
username <user-name> [privilege <privilege>] [password [0 | 7] <password>] no username <username>	Настраивает имя пользователя и пароль для доступа по Telnet. Команда «no» удаляет данные авторизации выбранного пользователя.
authentication ip access-class {<numstd>|<name>} no authentication ip access-class	Связывает стандартный IP ACL с Telnet/SSH/Web; команда «no» отменяет предыдущую команду.
authentication line {console | vty | web} login {local | radius | tacacs} no authentication line {console | vty | web} login	Настройка режима аутентификации Telnet.
authentication enable method1 [method2 …] no authentication enable	Настройка включения списков методов аутентификации.

1.2.2.2 SSH

1.2.2.2.1 Введение в SSH

SSH (англ. ***S**ecure **SH**ell* — «безопасная оболочка») является протоколом, который обеспечивает безопасный удаленный доступ к сетевым устройствам. Он основан на надежном TCP/IP-протоколе. Он поддерживает такие механизмы как распределение ключей, проверка подлинности и шифрования между SSH-сервером и SSH-клиентом, установка безопасного соединения. Информация, передаваемая через это соединение защищена от перехвата и расшифровки. Для доступа к коммутатору, соответствующему требованиям SSH2.0, необходимо SSH2.0 клиентское программное обеспечение, такое, как SSH Secure Client и PuTTY. Пользователи могут запускать вышеперечисленное программное обеспечение для управления коммутатором удаленно. Коммутатор в настоящее время поддерживает аутентификацию RSA, 3DES и SSH шифрование протокола, пароль пользователя аутентификации и т.д.

1.2.2.2.2 Список команд для конфигурирования SSH-сервера на коммутаторе

Команда	Описание
Режим глобального конфигурирования	
ssh-server enable	Активация функции на коммутаторе; команда

no ssh-server enable	«no» отменяет предыдущую команду.
username <username> [privilege <privilege>] [password [0 | 7] <password>] no username <username>	Настраивает имя пользователя и пароль для доступа к коммутатору через SSH-клиент. Команда «no» удаляет данные авторизации выбранного пользователя.
ssh-server host-key create rsa modulus <moduls>	Создание нового RSA-ключа хоста на SSH-сервере.

1.2.2.2.3 Пример настройки SSH-сервера

Пример 1:

Задачи:

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

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

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

1.2.3 Настройка IP-адресов коммутатора

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

- ручная;
- BOOTP;

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

В BOOTP/DHCP-режиме, коммутатор работает как BOOTP/DHCP-клиент, отправляет широковещательные пакеты BOOTP-запроса на BOOTP/DHCP-сервера и BOOTP/DHCP-сервер назначает адрес отправителю запроса, кроме того, коммутатор может работать в качестве DHCP-сервера и динамически назначать параметры сети, такие, как IP-адреса, шлюз и адреса DNS-серверов DHCP-клиентам, что подробно описано в последующих главах.

1.2.3.1 Список команд для настройки IP-адресов

1. Включение VLAN-режима.
2. Ручная настройка.

3. Динамическое получение IP-адреса по протоколу DHCP (DHCP-конфигурация).

1. Включение VLAN-режима.

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

2. Ручная настройка.

Команда	Описание
VLAN-режим	
ip address <ip_address> <mask> [secondary] no ip address <ip_address> <mask> [secondary]	Настройка IP-адреса VLAN-интерфейса; команда «no» удаляет IP-адреса VLAN-интерфейса.

3. Динамическое получение IP-адреса по протоколу DHCP (DHCP-конфигурация).

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

1.2.4 Настройка SNMP

1.2.4.1 Введение в SNMP

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

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

SNMP-протокол использует режим станции-агента. В этой структуре есть две составляющие: NMS (Network Management Station) и агент. NMS является рабочей станцией, на которой стоит клиентская программа SNMP. Это ядро SNMP-управления сетью. Агент серверного программного обеспечения работает на устройствах, которые

нуждаются в управлении. NMS управляет всеми объектами через агентов. Коммутатор поддерживает функции агента.

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

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

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

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

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

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

1.2.4.2 Введение в MIB

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

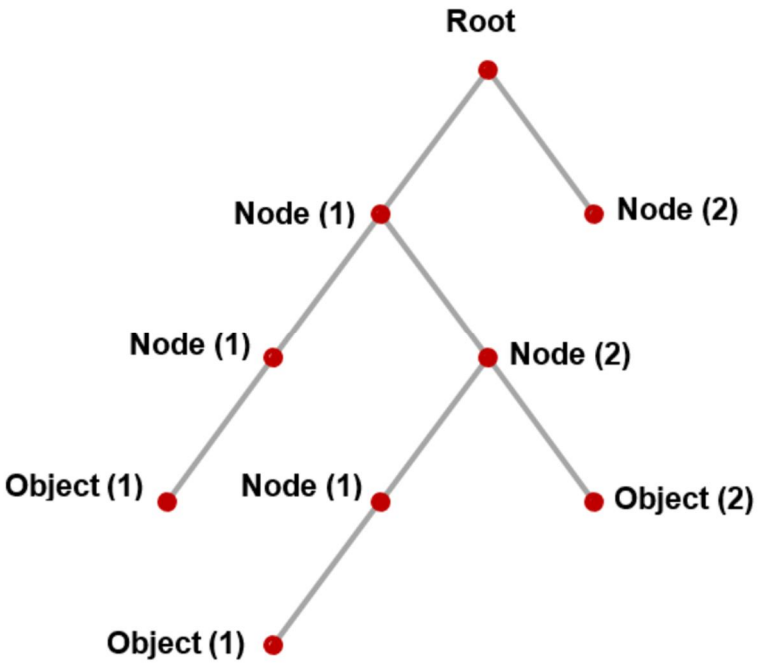


Рисунок 2.1 – Пример дерева ASN.1

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

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

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

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

1.2.4.3 Введение в RMON

RMON является наиболее важным расширением стандартного SNMP-протокола. RMON является набором определений MIB и используется для определения стандартных средств и интерфейсов для наблюдения за сетью, позволяет осуществлять связь между терминалами управления SNMP и удаленными управляемыми коммутаторами. RMON обеспечивает высокоэффективный метод контроля действий внутри подсети. . Объекты RMON MIB включают дополнительные счетчики ошибок в пакетах, более гибкие средства анализа трендов и статистики, более мощные средства фильтрации для захвата и анализа отдельных пакетов, а также более сложные условия установления сигналов предупреждения. Агенты RMON MIB более интеллектуальны по сравнению с агентами

MIB-I или MIB-II и выполняют значительную часть работы по обработке информации об устройстве, которую раньше выполняли менеджеры.

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

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

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

1.2.4.4 Настройка SNMP

1.2.4.4.1 Список команд для настройки SNMP

1. Включение и отключение функции SNMP-агента.
2. Настройка строки сообщества в SNMP.
3. Настройка IP-адреса станции управления SNMP.
4. Настройка engine ID.
5. Настройка пользователя.
6. Настройка группы.
7. Настройка вида.
8. Настройка TRAP.
9. Включение/выключение RMON.

1. Включение и отключение функции SNMP-агента.

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

1. Настройка строки сообщества в SNMP.

Команда	Описание
Режим глобального конфигурирования	
snmp-server community {ro|rw} {0 | 7} <string> [read <read-view-name>] [write <write-view- name>]	Настройка строки сообщества в SNMP для коммутатора. Команда «no» удаляет эту строку.

no snmp-server community {0 | 7} <string>	

1. Настройка TRAP.

Команда	Описание
Режим глобального конфигурирования	
snmp-server enable traps no snmp-server enable traps	Включить отправку Trap-сообщений. Эта команда используется для SNMP v1/0/v2/v3.
snmp-server host {<hostipv4-address> | <host-ipv6address>} {v1 | v2c | {v3 {noauthnopriv | authnopriv | authpriv}}} <user-string> no snmp-server host {<hostipv4- address> | <host-ipv6address>} {v1 | v2c | {v3 {noauthnopriv | authnopriv | authpriv}}} <user-string>	Установка IPv4/IPv6-адреса хоста, который используется для получения информации SNMP Trap. Для SNMP v1/0/v2, эта команда также настраивает строку сообщества для Trap; для SNMP v3, эта команда также настраивает имя пользователя и уровень безопасности Trap. Команда "no", отменяет этот IPv4- или IPv6-адрес.
snmp-server trap-source {<ipv4- address> | <ipv6address>} no snmp-server trap-source {<ipv4- address> | <ipv6address>}	Установка IPv4- или IPv6-адреса источника, который используется для отправки trap-пакетов, команда «no» удаляет конфигурацию.

1.2.4.5 Типичные примеры настройки SNMP

В приведенных примерах IP-адрес NMS – 1.1.1.5, IP-адрес коммутатора (агента) – 1.1.1.9.

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

Конфигурация коммутатора, записана ниже:

> *rotek(config)#snmp-server enable*
> *rotek(config)#snmp-server community rw private*
> *rotek(config)#snmp-server community ro public*

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

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

Конфигурация коммутатора, изложена ниже:

> *rotek(config)#snmp-server enable*
> *rotek(config)#snmp-server host 1.1.1.5 v1 usertrap*
> *rotek(config)#snmp-server enable traps*

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

1.2.4.6 Поиск неисправностей SNMP

Когда пользователи настраивают SNMP, SNMP-сервер может не работать должным образом из-за отказа физического соединения и неправильной конфигурации и т.д.

Пользователи могут устранить проблемы, выполнив требования, указанные ниже:

- Убедиться в надежности физического соединения.
- Убедиться, что интерфейс и протокол передачи данных находятся в состоянии

«up» (используйте команду "Show interface"), а также связь между коммутатором и хостом может быть проверена путем пинга (используйте команду "ping").

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

1.2.5 Обновление ПО

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

1.2.5.1 Системные файлы коммутатора

Системные файлы включают в себя файлы образа системы (system image) и загрузочные (BootRom) файлы. Обновление системных файлов коммутатора подразумевает собой перезапись старых файлов новыми.

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

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

Коммутатор предоставляет пользователю два режима обновления: 1. BootROM-режим; 2. TFTP- и FTP-обновление в режиме CLI. Эти два способа обновления будут описаны подробно в следующих двух разделах.

1.2.5.2 BootROM обновление

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

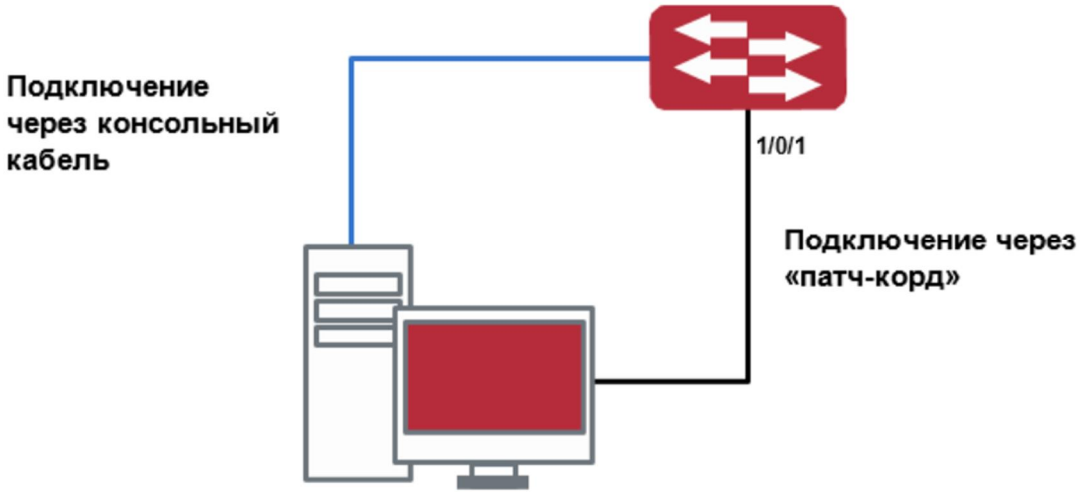


Рисунок 2.2 – Типичная топология для обновления коммутатора в режиме BootROM

Процедура обновления перечислена ниже:

Шаг 1:

Как показано на рисунке, используется консольный кабель для подключения ПК к порту управления на коммутаторе и Ethernet подключение к одному из портов коммутатора. ПК должен иметь программное обеспечение FTP/TFTP-сервера, а также файл image необходимый для обновления.

Шаг 2:

Нажмите "Esc" во время загрузки коммутатора для переключения в режим BootROM-монитора. Результат операции показан ниже:

> *RTL838x#*

Шаг 3:

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

> *setenv ipaddress 192.168.1.2*
> *setenv serverip 192.168.1.66*
> *saveenv*

Шаг 4:

Включить FTP/TFTP-сервер на ПК. Для TFTP запустите программу сервера TFTP, для FTP запустите программу FTP-сервер. Прежде, чем начать загрузку файла обновления на коммутатор, проверьте соединение между сервером и коммутатором с помощью пинга с сервера. Далее начнётся запуск файла ПО непосредственно с TFTP-сервера после выполнения команд:

> *rtk network on*
> *upgrade runtime1 192.168.1.66:vmlinux.bix*
> *TFTP from server 192.168.1.66; our IP address is 192.168.1.2 Filename 'vmlinux.bix'.*
> *Load address: 0x81000000*

Шаг 5:

После удачной загрузки, произведите обновление коммутатора из CLI режима. См. пункт «Примеры настройки FTP/TFTP».

1.2.5.3 Обновление FTP/TFTP

1.2.5.3.1 Введение в FTP/TFTP

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

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

Существует два типа таких соединений: активные и пассивные соединения.

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

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

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

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

Вот некоторые термины, часто используемые в FTP/TFTP.

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

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

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

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

Bootimage file: Загрузчик. Необходим для загрузки и запуска коммутатора.

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

Start up configuration file: это последовательность команд конфигурации, используемая при запуске коммутатора. Файл начальной конфигурации хранится в энергонезависимой памяти. Имя файла начальной конфигурации должно быть startup-config.

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

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

1.2.5.3.2 Настройка FTP/TFTP

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

Порядок настройки:

1. Настройка FTP/TFTP-клиента:
    - Загрузка файлов FTP/TFTP-клиентом:
    - Просмотр доступных файлов на FTP-сервере.
2. Настройка FTP сервера:
    - Запуск FTP сервера;
    - Настройка имени пользователя и пароля для входа на FTP-сервер.
    - Изменение времени ожидания FTP-сервера.
3. Настройка TFTP-сервера:
    - Запуск TFTP сервер;
    - Изменение времени ожидания TFTP-сервера;
    - Настройка количества раз ретрансляции до таймаута для неповрежденных пакетов.

1. Настройка FTP/TFTP-клиента.
    - Загрузка файлов FTP/TFTP-клиентом.

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

- Просмотр доступных файлов на FTP-сервере.

Команда	Пояснение

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

1. Настройка FTP-сервера.
    - Запуск FTP-сервера.

Команда	Пояснение
Глобальный режим	
ftp-server enable no ftp-server enable	Запуск сервера, команда «no» выключает сервер

- Изменение времени ожидания FTP-сервера.

Команда	Пояснение
Глобальный режим	
ftp-server timeout <seconds> no ftp-server timeout	Выставляет время ожидания до разрыва связи, "no" возвращает значение по умолчанию

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

Команда	Пояснение
Глобальный режим	
ip ftp username <username> password [0 | 7] <password> no ip ftp username <username>	Настройка имени пользователя и пароля для входа на FTP-сервер. Команда «no» удалит имя пользователя и пароль

1. Настройка TFTP-сервера.
    - Запуск TFTP-сервера.

Команда	Пояснение
Глобальный режим	
tftp-server enable no tftp-server enable	Запуск сервера, команда «no» выключает сервер

- Изменение времени ожидания TFTP-сервера.

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

- Настройка количества раз ретрансляции до таймаута для неповрежденных пакетов.

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

1.2.5.3.3 Примеры настройки FTP/TFTP

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

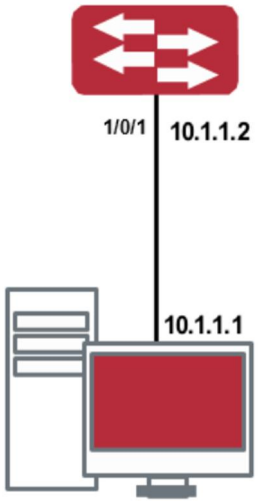


Рисунок 2.3 – Загрузка nos.img файла FTP/TFTP-клиентом

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

Настройка компьютера:

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

Настройка коммутатора:

```
rotek(config)#interface vlan 1
rotek(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
rotek(Config-if-Vlan1)#no shut
rotek(Config-if-Vlan1)#exit
```

rotek(config)#exit
rotek#copy ftp://PC:superuser@10.1.1.1/0/file.txt flash://file.txt

Для TFTP-сервера последняя команда соответственно заменяется на:

rotek# copy tftp://10.1.1.1/0/file.txt flash://file.txt

Сценарий 2: Использование коммутатора в качестве FTP-сервера. Коммутатор работает как сервер и подключается одним из своих портов к компьютеру, который является клиентом. Требуется передать файл «file.txt» с коммутатора на компьютер и сохранить его как «12_25_ file.txt».

Далее описана процедура настройки коммутатора:

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

Настройка компьютера:

Зайдите на коммутатор с любого FTP-клиента с именем пользователя «admin» и паролем «superuser», используйте команду «get file.txt» для загрузки файла «file.txt» с коммутатора на компьютер.

Сценарий 3: Использование коммутатора в качестве TFTP-сервера. Коммутатор работает как TFTP-сервер и соединяется одним из своих портов с компьютером, который является TFTP-клиентом. Требуется передать файл «file.txt» с коммутатора на компьютер. Далее описана процедура настройки коммутатора:

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

Настройка компьютера:

Зайдите на коммутатор с любого TFTP-клиента, используйте команду «tftp» для загрузки «file.txt» файла с коммутатора на компьютер.

1.2.5.3.4 Обновление ПО коммутатора с помощью FTP/TFTP

- Обновление системного ПО или загрузчика

Команда	Пояснение
Глобальный режим	
update (system | bootloader) <source-url>	Скачать файл ПО из <source-url> и записать в соответствующий раздел FLASH. Указать system для обновления системного ПО или bootloader для обновления загрузчика
copy <source-url> (system.img | bootloader.img)	Скопировать файл в RAM коммутатора и обновить полученным файлом ПО коммутатора. Указать system.img для обновления системного ПО или bootloader.img для обновления загрузчика.

1.2.5.3.4.1 Пример обновления ПО

Сценарий 1: Обновить системное ПО с удаленного TFTP-сервера. Файл прошивки расположен на сервере 192.168.1.5 и называется vmlinux.bix:

rotek(config)#update system tftp://192.168.1.5/vmlinux.bix

Необходимо учитывать, что обновление ПО занимает продолжительное время, около 5-10 минут.

Сценарий 2: Обновить загрузчик с удаленного TFTP-сервера. Файл прошивки расположен на сервере 192.168.1.5 и называется u-boot.bin:

rotek(config)#copy tftp://192.168.1.5/u-boot.bin bootloader.img

1.2.5.3.5 Устранение неисправностей FTP/TFTP

1.2.5.3.5.1 Поиск неисправностей FTP

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

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

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

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

1.2.5.3.5.2 Поиск неисправностей TFTP

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

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

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

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

> *begin to receive file, wait...*
> *recv 1526037*
> **********
> *write ok transfer complete*

> *close tftp client.*

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

2 КОНФИГУРИРОВАНИЕ ПОРТОВ

2.1 КОНФИГУРИРОВАНИЕ ПОРТОВ

2.1.1 Введение

В коммутаторе существуют кабельные и SFP-порты.

Если пользователь хочет сконфигурировать сетевой порт, он может ввести команду

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

2.1.2 Список команд для конфигурирования портов

1. Вход в режим конфигурации порта.
2. Конфигурация параметров сетевого порта.
    - Конфигурация режима combo для combo-портов.
    - Включить/выключить порты.
    - Конфигурация имени порта.
    - Конфигурация типа кабеля на порту.
    - Конфигурация скорости и дуплекса на порту.
    - Конфигурация контроля полосы пропускания.
    - Конфигурация управления траффиком.
    - Включение/выключение функции распознавания петли.
    - Конфигурация контроля широковещательных штормов на коммутаторе.
    - Конфигурация режима сканирования порта.
    - Конфигурация контроля нарушения скорости на порту.
    - Конфигурация интервала сбора статистики по скорости порта.
3. Виртуальный тест кабеля.

1. Вход в режим конфигурации Ethernet-порта

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

2. Конфигурация параметров сетевого порта.

Команда	Описание
Режим порта	
shutdown no shutdown	Включение/выключение указанного порта.
description <string> no description	Назначение или отмена имени порта.
speed-duplex {auto [10 [100 [1000]] | force10-half | force10-full | force100half | force100-full | force100-fx [module-type {auto-detected | no-phyintegrated | phy- integrated}] | {{force1g-half | force1g-full} [nonegotiate [master | slave]]}| force10g- full} no speed-duplex	Установка скорости и дуплекса на порту для 100/1000 BASE-TX или 100 BASE-F. С оператором NO данная команда восстанавливает параметры порта по умолчанию, то есть договорную скорость и автоматическое определение дуплекса.
negotiation {on|off}	Включение/выключение функции автоматического определения параметров для 1000 BASE-FX.
bandwidth control <bandwidth> [both | receive | transmit] no bandwidth control	Установка или отмена значения полосы пропускания, используемой для входящего/исходящего трафика для указанных портов.
flow control no flow control	Включение/выключение функции контроля траффика для указанных портов.
loopback no loopback	Включение/выключение функции петли для указанных портов.
storm-control {unicast | broadcast | multicast} <Kbits>	Включение функции контроля штормов для широковещательных, многопользовательских и персональных пакетов с неизвестным адресом назначения (коротких для широковещательного) и установка допустимого числа широковещательных пакетов; формат NO данной команды отключает функцию контроля широковещательных штормов.
rate-violation {unicast | broadcast | multicast | all } <10-2000000> no rate-violation	Включение функции защиты от штормов для пакетов разных типов и установка допустимого числа пакетов; формат NO данной команды отключает функцию защиты от штормов.
rate-violation control {block | shutdown} recovery <0-86400>	Устанавливает максимальную скорость приема пакетов на порту. Если скорость принятия пакетов превышает разрешенную, команда выключает этот порт и конфигурирует время восстановления порта (по умолчанию 300 с). Команда NO отключает установку.

3. Виртуальный тест кабеля.

Команда	Описание
Режим конфигурации порта	
virtual-cable-test interface ethernet	Тест виртуального кабеля на порте.

2.1.3 Примеры конфигурации порта

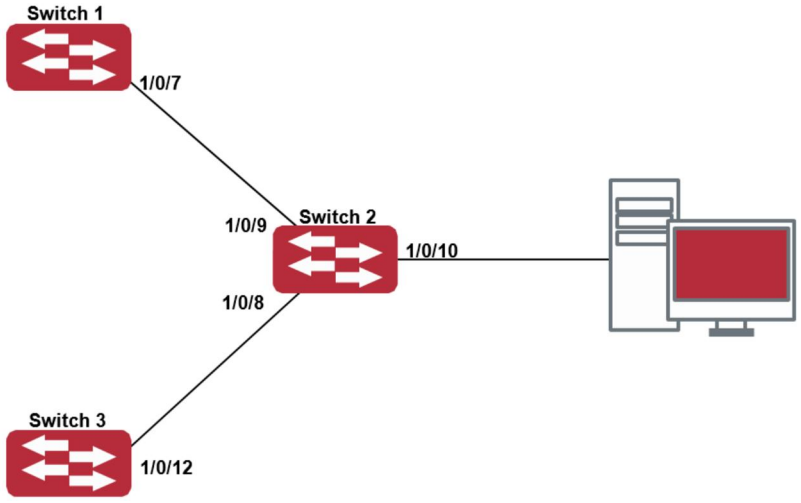


Рисунок 3.1 – Пример конфигурации порта

VLAN не сконфигурированы на коммутаторе. По умолчанию используется VLAN1.

Коммутатор	Порт	Свойства
Switch1	1/0/7	Лимит входящей полосы: 50 Мбит
Switch2	1/0/8	Зеркалированный порт источника
	1/0/9	100 Мбит/с full, зеркалированный порт источника
	1/0/10	1000 Мбит/с full, зеркалированный порт назначения
Switch3	1/0/12	100 Мбит/с full

Конфигурация приведена ниже:

Switch1:

```
Switch1(config)#interface ethernet 1/0/7
Switch1(Config-If-Ethernet1/0/7)#bandwidth control 50000 receive
```

Switch2:

```
Switch2(config)#interface ethernet 1/0/9
Switch2(Config-If-Ethernet1/0/9)#speed-duplex force100-full
Switch2(Config-If-Ethernet1/0/9)#exit
Switch2(config)#interface ethernet 1/0/10
Switch2(Config-If-Ethernet1/0/10)#speed-duplex force1g-full
Switch2(Config-If-Ethernet1/0/10)#exit
Switch2(config)#monitor session 1 source interface ethernet1/0/8;1/0/9
Switch2(config)#monitor session 1 destination interface ethernet 1/0/10
```

Switch3:

```
Switch3(config)#interface ethernet 1/0/12
```

Switch3(Config-If-Ethernet1/0/12)#speed-duplex force100-full
Switch3(Config-If-Ethernet1/0/12)#exit

2.1.4 Устранение неисправностей на порту

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

- Два соединенных оптических интерфейса не поднимаются если один интерфейс настроен на автоопределение, а на втором жестко установлены скорость и дуплекс. Это определяется стандартом IEEE 802.3.

Не рекомендуется следующая конфигурация: включение контроля трафика и одновременно установление лимита для многопользовательских пакетов на том же порту; установка одновременно контроля за широковещательными, многопользовательскими и персональными пакетами с неизвестным назначением и ограничения полосы на порту. Если такие комбинации установлены, пропускная способность порта может оказаться меньше ожидаемой.

2.2 PORT ISOLATION. КОНФИГУРАЦИЯ ФУНКЦИИ ИЗОЛЯЦИИ ПОРТОВ

2.2.1 Введение в функцию изоляции портов

Изоляция портов (Port Isolation) — это независимая порто-ориентированная функция, работающая между портами, которая изолирует потоки различных портов друг от друга. С помощью этой функции пользователь может изолировать порты в пределах VLAN для сохранения ресурсов VLAN и усиления секретности сети. После того, как эта функция будет сконфигурирована, порты в группе изолированных портов будут изолированы друг от друга, в то время как порты из различных групп изоляции или неизолированных могут пересылать данные друг другу совершенно нормально. На коммутаторе может быть сконфигурировано не более 16 групп изоляции портов.

2.2.2 Список команд для конфигурации изоляции портов

1. Создать группу изолированных портов.
2. Добавить Ethernet-порты в группу.
3. Отобразить конфигурацию группы изоляции портов.

1. Создать группу изолированных портов.

Команда	Описание
Режим глобального конфигурирования	
isolate-port group <WORD> no isolate-port group <WORD>	Создает группу изолированных портов. С оператором NO эта команда удаляет группу изолированных портов.

2. Добавить Ethernet-порты в группу.

Команда	Описание
Режим глобального конфигурирования	
isolate-port group <WORD> switchport interface [ethernet | port-channel] <IFNAME>	Добавляет один порт или группу портов в группу изолированных портов, которые будут изолированы от

no isolate-port group <WORD> switchport interface [ethernet | port-channel] <IFNAME>	других портов в группе. Оператор NO удаляет один порт или группу портов из группы изолированных портов.

3. Отобразить конфигурацию группы изоляции портов.

Команда	Описание
Режим администратора, Режим глобального конфигурирования	
show isolate-port group [<WORD>]	Показывает конфигурацию групп изолированных портов, включая все сконфигурированные группы изолированных портов и Ethernet-порты в каждой группе.

2.2.3 Типовые примеры функции изоляции портов

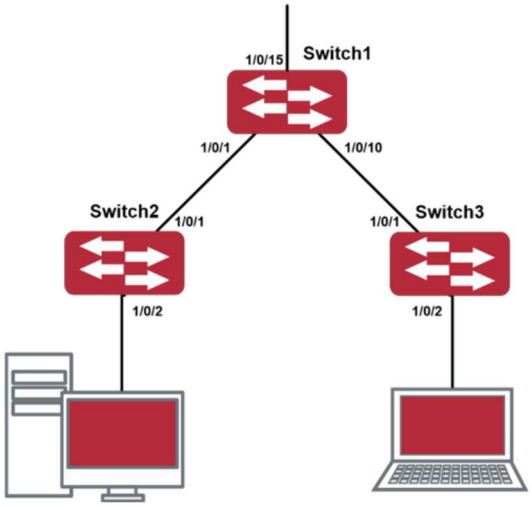


Рисунок 4.1 – Типовые примеры функции изоляции портов

Топология и конфигурация коммутаторов показана на рисунке выше. Порты 1/0/1, 1/0/10 и 1/0/15 все принадлежат к VLAN 100. Требование заключается в том, чтобы после включения функции изоляции портов на коммутаторе Switch1 порты 1/0/1 и 1/0/10 на этом коммутаторе не могли связываться друг с другом и оба могли связываться с портом 1/0/15, смотрящим в сеть. То есть связи между любыми парами downlink-портов - нет, и в то же время связь между любым downlink-портом и uplink - работает. Вышестоящий порт может работать с любым портом нормально.

Конфигурация коммутатора SWITCH:

> *rotek(config)#isolate-port group test*
> *rotek(config)#isolate-port group test switchport interface ethernet 1/0/1;1/0/10*

2.3 КОНФИГУРАЦИЯ ФУНКЦИИ РАСПОЗНАВАНИЯ ПЕТЛИ НА ПОРТУ

2.3.1 Введение в функцию распознавания петли

С развитием сетевых устройств все больше и больше пользователей подключаются к сети через Ethernet-коммутаторы. В промышленных сетях пользователи получают доступ через коммутаторы 2-го уровня, что предъявляет строгие требования к взаимодействию между устройствами как внешней, так и внутренней сети. Когда требуется

взаимодействие на 2-м уровне, сообщение должно отправляться точно в соответствии с MAC-адресом для корректной работы между пользователями. Устройства второго уровня запоминают MAC-адреса, изучая входящие MAC-адреса источников пакетов и при поступлении пакета с неизвестным адресом источника они записывают его MAC-адрес в таблицу, закрепляя его за портом, откуда пришел этот пакет. Таким образом следующий пакет с данным MAC-адресом в качестве порта назначения будет отправлен сразу на этот порт. То есть адрес сразу фиксируется на порту для отправки всех пакетов.

Когда пакет с MAC-адресом источника, уже изученным коммутатором, приходит через другой порт, запись в таблице MAC-адресов изменяется таким образом, чтобы пакеты с данным MAC-адресом направлялись через новый порт. В результате, если на участке между двумя адресатами существует какая-либо петля, все MAC-адреса из сети второго уровня будут пересылаться на тот порт, где существует петля (обычно MAC-адреса в этом случае с высокой частотой переключаются с одного порта на другой), что вызывает перегрузку и потерю работоспособности сети 2-го уровня. Вот почему необходимо проверять наличие петли на сетевых портах. Когда на порту определяется петля, обнаружившее ее устройство должно послать предупреждение в систему управления сетью, позволяя сетевому администратору обнаружить, локализовать и решить проблему в сети.

Поскольку система обнаружения петель (Loopback detection) может автоматически принимать решения о наличии петли в соединении и ее исчезновении, устройства с функциями контроля на портах (таких как изоляция портов и контроль за запоминанием MAC-адресов) могут значительно снизить нагрузку сетевого администратора, а также уменьшить время реакции на проблему, минимизируя воздействие петли на сеть.

2.3.2 Список команд для конфигурирования функции распознавания петли на порту

1. Конфигурирование временного интервала распознавания петли.
2. Включение функции распознавания петли.
3. Конфигурирование режима порта при распознавании петли.
4. Вывод отладочной информации по распознаванию петли.
5. Конфигурирование режима восстановления при распознавании петли.

1. Конфигурирование временного интервала распознавания петли.

Команда	Описание
Режим глобального конфигурирования	
loopback-detection interval-time <loopback> <no-loopback> no loopback-detection interval-time	Конфигурирование временного интервала распознавания петли

2. Конфигурирование режима порта при распознавании петли.

Команда	Описание
Режим конфигурирования порта	
loopback-detection control {shutdown |block} no loopback-detection control	Включение и выключение определенного режима порта при распознавании петли.

3. Вывод отладочной информации по распознаванию петли.

Команда	Описание
Режим администратора	
debug loopback-detection no debug loopback-detection	Вывод отладочной информации по распознаванию петли. С оператором NO данная команда прекращает вывод отладочной информации.
show loopback-detection [interface <interface-list>]	Показывает статус и результаты распознавания петли на всех портах, если других параметров не вводится; в противном случае показывается статус и результат распознавания петли для конкретных портов

4. Конфигурирование режима восстановления при распознавании петли.

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

2.3.3 Примеры функции распознавания петли на порту

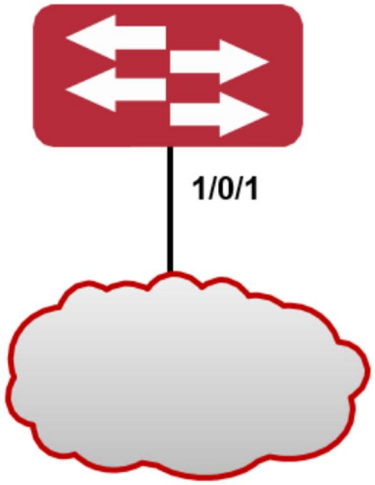


Рисунок 5.1 – Типичный пример подключения

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

Последовательность конфигурации коммутатора:

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

Если выбран метод блокировки при определении петли, должен быть глобально включен протокол MSTP на всей сети, а также должны быть сконфигурированы соответствующие связи между протоколом связующего дерева и VLAN.

```
rotek(config)#spanning-tree
rotek(config)#spanning-tree mst configuration
rotek(Config-Mstp-Region)#instance 1 vlan 1
rotek(Config-Mstp-Region)#instance 2 vlan 2
rotek(Config-Mstp-Region)#
```

2.3.4 Решение проблем с функцией распознавания петли на порту

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

2.4 КОНФИГУРАЦИЯ ФУНКЦИИ udld

2.4.1 Общая информация о udld

Однонаправленное соединение (Unidirectional Link) — это распространенная проблема в сети, особенно для оптических соединений. Под однонаправленным соединением понимается ситуация, когда один порт соединения может принимать сообщения от другого порта, а тот не может получать их от первого. Если на физическом уровне соединение установлено, проблема связи между устройствами не может быть обнаружена. Как показано на рисунке, проблема оптического соединения не может быть обнаружена посредством механизмов физического уровня, таких как автоматическое согласование параметров.

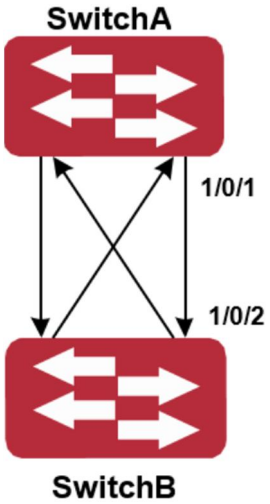


Рисунок 6.1 – Перекрестное подключение двунаправленного оптического соединения

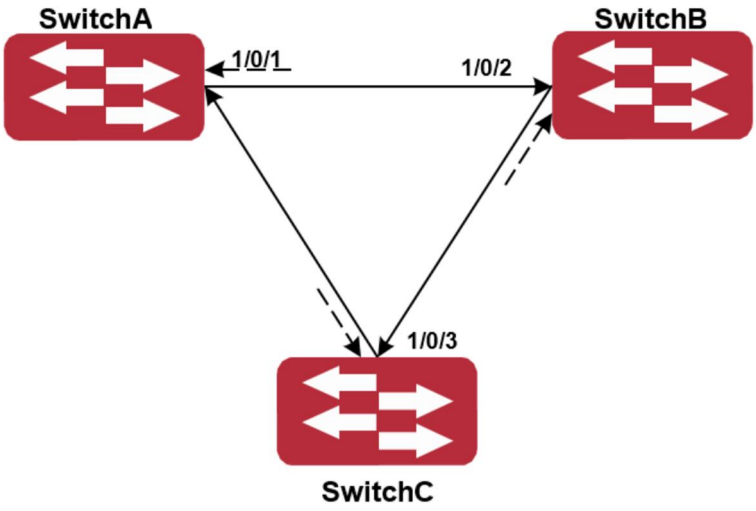


Рисунок 6.2 – Один из концов каждого двухнаправленного оптического соединения не подключен

Такой вид проблем часто возникает в ситуации, когда или интерфейс, или GBIC (Giga Bitrate Interface Converter – конвертер интерфейса со скоростью 1 Гбит) имеют программные проблемы, в этом случае оборудование становится недоступным или работает неправильно. Однонаправленное соединение может вызывать целую серию проблем, таких как зацикливание связующего дерева или широковещательным штормам (broadcast black hole).

UDLD (Unidirectional Link Detection Protocol – протокол обнаружения однонаправленных соединений) может помочь обнаружить неисправность, которая возникает в ситуациях, перечисленных выше. В коммутаторе, подключенном через оптическую или медную Ethernet линию (такую как витая пара пятой категории), udld может мониторить статус физических соединений. В случае, если обнаружено однонаправленное соединение, он посылает предупреждение пользователям и может выключить порт автоматически, или вручную, в зависимости от конфигурации пользователя.

Функция udld в коммутаторе распознает удаленные устройства и проверяет корректность соединений, используя интерактивную систему собственных сообщений. Когда udld включен на порту, механизм определения статуса порта запускается, что подразумевает посылку сообщений различного вида, которые посылаются различными подпрограммами этого механизма для проверки статуса соединений путем обмена информацией с удаленными устройствами. udld может динамически определять интервал, с которым удаленное устройство посылает свои уведомления и подстраивает в соответствии с ним свой локальный интервал. Кроме того, udld обеспечивает механизм рестарта, если порт был заблокирован udld, также соединение может быть проверено еще раз после рестарта. Временной интервал посылки уведомлений и рестарта порта в udld может конфигурироваться пользователями, таким образом udld может быстрее реагировать на проблемы соединений в различном сетевом окружении. Показателем правильной работы udld является работа соединения в дуплексном режиме, это значит, что udld включен на обоих концах соединения и использует одинаковый метод авторизации и пароль.

2.4.2 Список команд для конфигурирования udld

1. Включение функции udld на коммутаторе.
2. Включение функции udld на порту.
3. Конфигурация агрессивного режима на коммутаторе.
4. Конфигурация агрессивного режима на порту.
5. Конфигурация метода выключения однонаправленного соединения.
6. Конфигурация интервала уведомлений (Hello messages).

7. Конфигурация интервала восстановления.
8. Рестарт порта, выключенного функцией udld.
9. Демонстрационная и отладочная информация функции udld.

1. Включение функции udld на коммутаторе.

Команда	Описание
Режим глобального конфигурирования	
udld enable udld disable	Включение или выключение функции udld на коммутаторе.

2. Включение функции udld на порту.

Команда	Описание
Режим конфигурирования порта	
udld enable udld disable	Включение или выключение функции udld на порт.

3. Конфигурация агрессивного режима на коммутаторе.

Команда	Описание
Режим глобального конфигурирования	
udld aggressive-mode no udld aggressive-mode	Устанавливает режим работы функции на коммутаторе.

4. Конфигурация агрессивного режима на порту

Команда	Описание
Режим конфигурирования порта	
udld aggressive-mode no udld aggressive-mode	Устанавливает режим работы функции на порту.

5. Конфигурация метода выключения однонаправленного соединения.

Команда	Описание
Режим глобального конфигурирования	
udld manual-shutdown no udld manual-shutdown	Конфигурирует метод выключения однонаправленного соединения.

6. Конфигурация интервала уведомлений (Hello messages).

Команда	Описание

Режим глобального конфигурирования	
udld hello-interval <integer> no udld hello-interval	Конфигурация интервала уведомлений (Hello messages), диапазон от 5 до 100 секунд. Значение по умолчанию - 10 с

7. Конфигурация интервала восстановления.

Команда	Описание
Режим глобального конфигурирования	
udld recovery-time <integer> no udld recovery-time <integer>	Конфигурирует интервал восстановительного рестарта. Диапазон от 30 до 86400 секунд. Значение по умолчанию — 0 секунд.

8. Рестарт порта, выключенного функцией udld.

Команда	Описание
Режим глобального конфигурирования или режим конфигурирования порта	
udld reset	Рестартует все порты в режиме глобального конфигурирования. Рестартует конкретный порт в режиме конфигурирования порта.

9. Демонстрационная и отладочная информация функции udld.

Команда	Описание
Режим администратора	
show udld [interface ethernet IFNAME]	Показывает информацию по udld. Для отображения общей udld информации параметров нет. При задании конкретного порта выводится общая информация и информация о соседях по данному порту.
debug udld fsm interface Ethernet <IFname> no debug udld fsm interface Ethernet <IFname>	Включение или выключение вывода отладочной информации по определенному порту.
debug udld error no debug udld error	Включение или выключение отладочной информации об ошибках
debug udld event no debug udld event	Включение или выключение отладочной информации о событиях
debug udld packet {receive|send} no debug udld packet {receive|send}	Включение или выключение вывода отладочной информации по типу сообщений
debug udld {hello|probe|echo|unidir|all} [receive|send] interface ethernet <IFname> no debug udld {hello|probe|echo|unidir|all} [receive|send] interface ethernet <IFname>	Включение или выключение вывода детальной информации об определенном типе сообщений, которые могут посылаться или приниматься на определенном порту.

2.4.3 Типовые примеры конфигурации udld

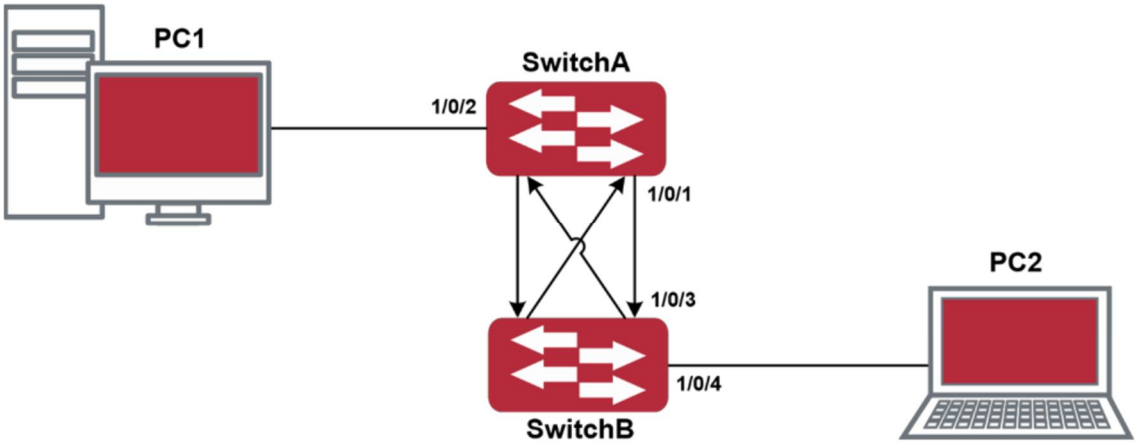


Рисунок 6.3 – Перекрестное подключение двунаправленного оптического соединения

В сетевой топологии на рисунке порт 1/0/1 на коммутаторе A, а также порт 1/0/3 на коммутаторе B – оптические. И соединение имеет перекрестный тип. Физический уровень включен и работает нормально, но соединение на уровне данных неработоспособно. udld может определить и заблокировать такой тип ошибки на соединении. Конечным результатом будет то, что порт 1/0/1 на коммутаторе A, а также порт 1/0/3 на коммутаторе B будут заблокированы функцией udld. Порты смогут работать (не будут заблокированы) только если соединение будет корректным.

Последовательность конфигурации коммутатора A:

> *SwitchA(config)#udld enable*
> *SwitchA(config)#interface ethernet 1/0/1*
> *SwitchA (Config-If-Ethernet1/0/1)#udld enable*
> *SwitchA (Config-If-Ethernet1/0/1)#exit*

Последовательность конфигурации коммутатора B:

> *SwitchB(config)#udld enable*
> *SwitchB(config)#interface ethernet1/0/3*
> *SwitchB(Config-If-Ethernet1/0/3)#udld enable*
> *SwitchB(Config-If-Ethernet1/0/3)#exit*

В результате порт 1/0/1 на коммутаторе A будет заблокирован функцией udld и на дисплее терминала PC1 появится следующая информация.

> *%Oct 27 11:09:50 2022 A unidirectional link is detected! Port Ethernet1/0/1 need to be shutted down!*
>
> *%Oct 27 11:09:50 2022 Unidirectional port Ethernet1/0/1 shut down!*

Порт 1/0/3 на коммутаторе B будет заблокирован функцией udld и на дисплее терминала PC2 появится следующая информация.

> *%Oct 27 11:09:50 2022 A unidirectional link is detected! Port Ethernet1/0/3 need to be shutted down!*
> *%Oct 27 11:09:50 2022 Unidirectional port Ethernet1/0/3 shutted down!*

2.4.4 Устранение неполадок функции udld

Замечания по конфигурации:

- Для уверенности, что udld сможет определить, что один из оптических портов не подключен или порты некорректно соединены, порты должны работать в дуплексном режиме и иметь одинаковую скорость.
- Если механизм автоматического определения параметров оптических портов, один из которых включен некорректно, определит рабочий режим и скорость, udld не сможет отработать корректно, вне зависимости от того, включен он или нет. В данной ситуации порт помечается как выключенный.
- Для уверенности в том, что ответный порт корректно сконфигурирован и однонаправленное соединение сможет быть корректно определено, необходимо, чтобы на обоих концах соединения udld был включен и использовался одинаковый метод авторизации и пароль. В нашем примере пароль с обеих сторон не установлен.
- Интервал отправки hello-сообщений может быть изменен (это 10 секунд по умолчанию и колеблется от 5 до 100 секунд), так что udld могут быстрее реагировать на ошибки подключения линий в различных условиях работы сети. Но этот интервал должен быть меньше 1/3 от времени конвергенции STP. Если интервал слишком длинный, петля STP будет сформирована до того, как udld обнаружит и отключит порт однонаправленного соединения. Если интервал слишком короткий, сетевая нагрузка на порт будет увеличена, что означает снижение пропускной способности. udld не обрабатывает события LACP. Он обрабатывает каждое соединение группы TRUNK (например, port-channal, TRUNK порты) независимо друг от друга. udld не работает с похожими протоколами других производителей. Это означает, что пользователи не могут использовать udld на одном конце и использовать другие подобные протоколы на другом конце соединения. udld-функция отключена по умолчанию. После включения функции udld в режиме глобального конфигурирования можно включить вывод отладочных сообщений. Существует несколько команд отладки (DEBUG) для вывода отладочной информации. Например, информацию о событиях, состоянии, ошибках и сообщениях. Различные типы отладочных сообщений также могут быть выведены в соответствии с различными значениями параметров.
- Таймер восстановления по умолчанию выключен и может быть включен только в случае, когда пользователь задал время восстановления (30 – 86400 секунд).

Команда рестарта и механизм перезагрузки порта воздействуют только на порт, который был выключен функцией udld.

2.5 НАСТРОЙКА ФУНКЦИИ LLDP

2.5.1 Общие сведения о функции LLDP

Протокол исследования соединительного уровня (Link Layer Discovery Protocol – LLDP) — это новый протокол канального уровня, описанный в спецификации 802.1ab. Он позволяет соседним устройствам посылать уведомления о своем статусе другим устройствам и на всех портах любого устройства сохранять информацию об этом. Если необходимо, порты так же могут посылать информацию об изменении статуса устройствам, непосредственно подключенным к ним. Эта информация будет сохранена в стандартных MIB SNMP. Система управления сетью может проверять состояние соединений второго уровня по информации из MIB. LLDP не конфигурирует или контролирует элементы сети или потоки, он только описывает конфигурацию второго уровня. В спецификации 802.1ab также описывается, как используется информация, предоставляемая LLDP для обнаружения конфликтов на втором уровне. Институт стандартизации (IEEE) в настоящее время использует существующую физическую топологию, интерфейсы и наборы MIB IETF.

Упрощенно, LLDP – протокол обнаружения соседних устройств. Он определяет стандартный метод, позволяющий Ethernet устройствам, таким, как коммутаторы, маршрутизаторы и точки доступа уведомлять о своем существовании другие узлы сети и

сохранять информацию обо всех соседних устройствах. Как следствие, детальная информация о конфигурации устройства и о найденных соседях может объявляться посредством данного протокола.

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

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

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

Информация, собранная на 2 уровне, содержит сведения об устройствах, их портах и о том какие коммутаторы с какими соединены и т. п. Она так же может показывать маршруты между клиентами, коммутаторами, маршрутизаторами и сетевыми серверами. Такие данные очень важны для определения и исследования источника проблем на сети.

LLDP является полезным инструментом управления, предоставляющим точную информацию о зеркалировании сети, отображении потоков данных и поиске сетевых проблем.

2.5.2 Список команд для конфигурирования LLDP

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

1. Включение LLDP на устройстве.

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

2. Включение функции LLDP на порту.

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

3. Конфигурация статуса LLDP на порту.

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

4. Конфигурация интервала обновления сообщений LLDP.

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

5. Конфигурация множителя времени поддержки сообщений LLDP.

Команда	Описание
Режим глобального конфигурирования	
lldp msgTxHold <value> no lldp msgTxHold	Конфигурация множителя времени поддержки сообщений LLDP как определенной величины или значения по умолчанию.

6. Конфигурация задержки отправки обновляющих сообщений.

Команда	Описание
Режим глобального конфигурирования	
lldp transmit delay <seconds> no lldp transmit delay	Конфигурация задержки отправки обновляющих сообщений как определенной величины или значения по умолчанию.

7. Конфигурация интервалов посылки TRAP-пакетов.

Команда	Описание

Режим глобального конфигурирования	
lldp notification interval <seconds> no lldp notification interval	Конфигурация интервалов посылки TRAP-пакетов как определенной величины или значения по умолчанию.

8. Отображение отладочной информации по функции LLDP.

Команда	Описание
Admin, Режим глобального конфигурирования	
show lldp	Отображение текущей конфигурации функции LLDP.
show lldp interface ethernet <IFNAME>	Отображение информации о конфигурации LLDP на конкретном порту
show lldp neighbors interface ethernet <IFNAME>	Отображение информации о LLDP соседях на данном порту.
show debugging lldp	Отображение всех портов с включенной функцией отладки LLDP

2.5.3 Типовой пример конфигурации LLDP

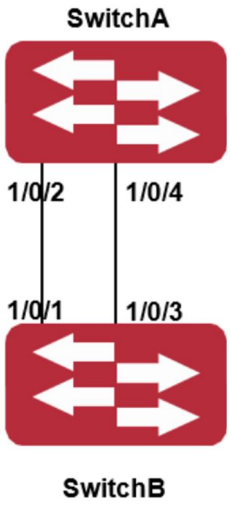


Рисунок 7.1 – Типовой пример конфигурации функции LLDP

На схеме сетевой топологии, приведенной выше, порт 1,3 на коммутаторе B подключен к порту 2,4 коммутатора A. Порт 1 коммутатора B сконфигурирован в режиме приема пакетов. Опция TLV на порту 4 коммутатора A сконфигурирована как portDes и SysCap (передача информации об описании порта и возможностях системы.).

Коммутатор A. Последовательность команд конфигурации:

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

Коммутатор B. Последовательность команд конфигурации:

```
SwitchB(config)#lldp enable
SwitchB(config)#interface ethernet1/0/1
```

```
SwitchB(Config-If-Ethernet1/0/1)# lldp mode receive
SwitchB(Config-If-Ethernet1/0/1)#exit
```

2.5.4 Устранение неисправностей функции LLDP

Функция LLDP по умолчанию выключена. После ее включения в режиме глобального конфигурирования, пользователи могут включить режим отладки «debug lldp» для проверки отладочной информации. Используя команду «show» функции LLDP можно вывести информацию о конфигурировании в глобальном режиме конфигурирования, либо в режиме настройки интерфейсов.

2.6 PORT CHANNEL. НАСТРОЙКА АГРЕГИРОВАНИЯ ПОРТОВ

2.6.1 Агрегирование портов. Общие сведения о Port channel

Агрегирование портов - это процесс объединения нескольких портов с одинаковой конфигурацией и для использования их логически в качестве одного физического порта – порт-канала (Port-Channel), что позволяет суммировать полосу пропускания в одном логическом линке и использовать резервирование.

Для понимания термина порт-канала (Port channel) надо ввести понятие группы портов. Группа портов – это группа физических портов на конфигурационном уровне. Только физические порты в группе портов могут быть частью объединенного канала и стать участниками Port channel. Логически группа портов является не портом, а набором портов. При определенных условиях физические порты в группе портов позволяют посредством объединения портов сформировать Port channel, который обладает всеми свойствами логического порта и таким образом становится независимым логическим портом. Агрегация портов — это абстрактное понятие, подразумевающее по собой объединение набора портов с одинаковыми свойствами в логический порт. Port channel — это набор физических портов, который логически используется как один физический порт. Он может использоваться пользователем как обычный порт. Он не может не только добавить пропускной способности на сеть, но и способен обеспечить резервирование соединений. Обычно объединение портов используется, когда коммутатор подключен к маршрутизатору, клиентской станции или другим коммутаторам.

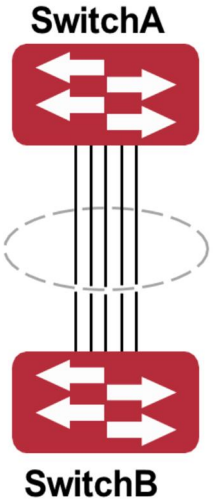


Рисунок 8.1 – Агрегирование портов

Как показано выше, коммутатор SwitchA объединил порты в Port channel. Пропускная полоса Port channel равна сумме пропускных способностей четырех портов. Когда необходимо передать трафик с коммутатора SwitchA на SwitchB, распределение трафика будет определяться на основе MAC-адреса источника и младшего бита MAC-адреса

приемника. В результате вычислений определяется, какой порт будет передавать трафик. Если один порт в Port channel неисправен, трафик будет перераспределяться на другие порты посредством алгоритма распределения. Данный алгоритм поддерживается аппаратно.

Коммутатор предлагает два метода конфигурации объединения портов: ручное создание Port channel и динамическое посредством протокола контроля объединения соединений

(Link Aggregation Control Protocol – LACP). Объединение возможно только для портов, работающих в режиме полного дуплекса.

Для правильной работы Port channel необходимо соблюдать следующие условия:

- Все порты работают в режиме полного дуплекса.
- Все порты имеют одинаковую скорость.
- Все порты являются портами доступа и принадлежат одному VLAN, или все они являются транковыми портами или они все гибридные порты.
- Если все порты являются транковыми или гибридными, тогда сконфигурированные на них допустимые VLAN и основной VLAN должны быть у всех одинаковыми.

Если Port channel сконфигурирован на коммутаторе вручную иди динамически, система автоматически назначает порт с наименьшим номером мастер-портом порт-канала. Если на коммутаторе активирован протокол spanning tree (STP), протокол построения дерева воспринимает Port channel как логический порт и посылает BPDU-пакеты через мастер-порт.

Объединение портов жестко связано с аппаратной частью коммутатора. Коммутатор позволяет агрегировать соединения между любыми двумя коммутаторами. Максимально возможно создать 128 групп по 8 портов к каждой.

После того, как порты агрегированы, их можно использовать, как обычный порт. Коммутатор имеет встроенный режим конфигурирования интерфейса агрегации, пользователь может создавать соответствующую конфигурацию в этом режиме точно также, как при конфигурировании VLAN или физического интерфейса.

2.6.2 Общие сведения о LACP

LACP (Link Aggregation Control Protocol) – протокол, базирующийся на стандарте IEEE 802.3ad, и реализующий механизм динамического объединения каналов. Протокол LACP использует пакеты LACPDU (Link Aggregation Control Protocol Data Unit) для обмена информацией с ответными портами.

После того, как протокол LACP включен на порту, данный порт посылает пакеты LACPDU на ответный порт соединения, уведомляя о приоритете системы, MAC-адресе системы, приоритете порта, идентификаторе порта и ключе операции. Когда ответный порт получает эту информацию, она сравнивается с информацией о других портах, которые могут быть объединены. Соответственно, обе стороны соединения могут достичь соглашения о включении или исключении порта из динамической объединенной группы.

Ключ операции создается протоколом в соответствии с комбинацией параметров конфигурации (скорость, дуплекс, базовая конфигурация, ключ управления) портов, которые будут объединяться.

После включения протокола динамического объединения портов (LACP), ключ управления по умолчанию равен 0. После статического объединения портов посредством LACP, ключ управления порта такой же, как ID объединенной группы.

При динамическом объединении портов все члены одной группы имеют одинаковый ключ операции. При статическом объединении только активные порты имеют одинаковый ключ операции.

2.6.2.1 Статическое объединение LACP

Статическое объединение выполняется путем конфигурирования пользователем и не требует протокола LACP. При конфигурировании статического LACP-объединения, используется режим «on» для включения порта в группу агрегации.

2.6.2.2 Динамическое объединение LACP

1. Общие положения динамического объединения LACP.

Динамическое объединение — это объединение, создаваемое/удаляемое системой автоматически. Оно не позволяет пользователям самостоятельно добавлять или удалять порты из динамического объединения LACP. Порты, которые имеют одинаковые параметры скорости и дуплекса, подключенные к одним и тем же устройствам, имеющие одинаковую конфигурацию могут быть динамически объединены в группу. В случае, если только один порт может создавать динамическое объединение, это называется однопортовым объединением. При динамическом объединении LACP-протокол на порту должен быть включен.

LACP использует LACPDU сообщения для обмена информацией с соседней стороной.

После включения LACP порт посылает LACPDU, уведомляя ответную сторону о приоритете и MAC адресе системы, приоритете и адресе порта и ключе операции. Когда ответный порт получает эту информацию, он сравнивает её с информацией о своих портах, настроенных на агрегацию. Таким образом обе стороны достигают соглашения о включении или исключении порта из динамической группы агрегации.

2. Режимы портов в динамической группе объединения.

В динамической группе объединения порты имеют два статуса — выбранный (selected) или «в ожидании» (standby). Оба типа портов могут посылать и принимать пакеты протокола LACP, но порты в статусе «ожидания» не могут пересылать данные.

Поскольку существует ограничение на максимальное количество портов в группе агрегации, если текущий номер порта превышает предел в группе, тогда устройство на одном конце соединения договаривается с устройством на другом конце для определения статуса порта в соответствии с идентификатором порта.

Этапы согласования, следующие:

1. Сравнение идентификаторов (ID) устройств (приоритет системы и MAC-адрес системы). Сначала сравниваются приоритеты систем. Если они одинаковые, тогда сравниваются MAC-адреса устройств. Устройство с меньшим идентификатором имеет высший приоритет.
2. Затем идет сравнение идентификаторов портов (приоритет порта и идентификатор порта). Для каждого порта на стороне устройства с наивысшим приоритетом системы сначала сравниваются приоритеты портов. Если приоритеты одинаковые, тогда сравниваются идентификаторы портов. Порт с наименьшим идентификатором порта становится выбранным (selected), а остальные становятся в режим «ожидание» (standby).
3. В группе объединения порт с наименьшим идентификатором и статусом «выбранный» становится мастер-портом. Другие порты со статусом «выбранный» становятся участниками группы.

2.6.3 Настройка Port channel

1. Создание группы портов (Port-Group) в режиме глобального конфигурирования.
2. Добавление портов в определенную группу из режима конфигурирования порта.
3. Вход в режим конфигурирования port-channel.
4. Задание метода балансировки для группы портов.
5. Задание приоритета системы в LACP-протоколе.

6. Задание приоритета для конкретного порта в LACP-протоколе.
7. Задание режима таймаута на порту в LACP-протоколе.

1. Создание группы портов.

Команда	Описание
Режим глобального конфигурирования	
port-group <port-group-number> no port-group <port-group-number>	Создание или удаление группы портов.

2. Добавление портов в определенную группу.

Команда	Описание
Режим конфигурирования порта	
port-group <port-group-number> mode {active | passive | on} no port-group	Добавляет порты в группу и устанавливает их режим.

3. Задание метода балансировки для устройства.

Команда	Описание
Режим глобального конфигурирования	
load-balance {dst-src-mac | dst-src-ip | dst-src- mac-ip}	Задание метода балансировки для устройства, изменения начинают действовать на группе портов и ECMP функции сразу.

4. Задание приоритета для конкретного порта в LACP-протоколе.

Команда	Описание
Режим конфигурирования порта	
lacp port-priority <port-priority> no lacp port-priority	Задание приоритета для конкретного порта в LACP-протоколе. команда no возвращает значение по умолчанию.

5. Задание режима таймаута на порту в LACP-протоколе.

Команда	Описание
Режим конфигурирования порта	
lacp timeout {short | long} no lacp timeout	Задание режима таймаута на порту в LACP-протоколе. команда no возвращает значение по умолчанию.

2.6.4 Примеры использования Port channel

Вариант 1. Настройка Port channel для протокола LACP.

Имеется два коммутатора SWITCHA и SWITCHB. Порты 1,2,3,4 на коммутаторе SWITCHA

- порты доступа и добавлены в группу1 (port-group 1) в активном режиме. Порты 6,8,9,10 на коммутаторе SWITCHB – тоже порты доступа и добавлены в группу 2 (port-group 2) в пассивном режиме. Все порты соединены кабелями.

Этапы конфигурации показаны ниже:

```
Switch1#config
Switch1(config)#interface ethernet 1/0/1-4
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 ethernet 1/0/6
Switch2(Config-If-Ethernet1/0/6)#port-group 2 mode passive
Switch2(Config-If-Ethernet1/0/6)#exit
Switch2(config)#interface ethernet 1/0/8-10
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)#
```

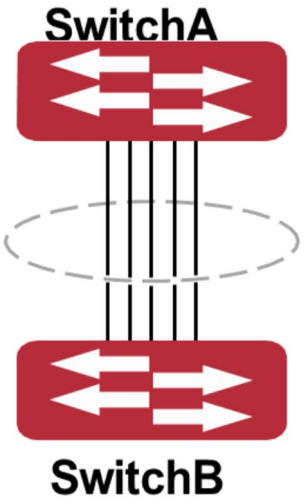


Рисунок 8.2 – Конфигурация Port-Channel

Результат конфигурации:

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

Вариант 2. Конфигурация Port channel в режиме ON.

Как показано на рисунке, порты 1,2,3,4 коммутатора SwitchA – порты доступа и будут добавлены в группу1 (port-group 1) с режимом ON. Порты 6,8,9,10 коммутатора SwitchB – тоже порты доступа и будут добавлены в группу2 (port-group 2) с режимом ON.

Этапы конфигурации показаны ниже:

```
Switch1#config
Switch1(config)#interface ethernet 1/0/1
Switch1(Config-If-Ethernet1/0/1)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/1)#exit
Switch1(config)#interface ethernet 1/0/2
```

```
Switch1(Config-If-Ethernet1/0/2)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/2)#exit
Switch1(config)#interface ethernet 1/0/3
Switch1(Config-If-Ethernet1/0/3)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/3)#exit
Switch1(config)#interface ethernet 1/0/4
Switch1(Config-If-Ethernet1/0/4)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/4)#exit
```

```
Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/0/6
Switch2(Config-If-Ethernet1/0/6)#port-group 2 mode on
Switch2(Config-If-Ethernet1/0/6)#exit
Switch2(config)#interface ethernet 1/0/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode on
Switch2(Config-If-Port-Range)#exit
```

Результат конфигурации:

Порты 1,2,3,4 на коммутаторе SwitchA добавлены по порядку в группу портов 1 в режиме ON. Коммутатору на удаленном конце не требуется обмен пакетами LACP для завершения объединения. Агрегация завершается сразу, когда выполняется команда добавления порта 2 в группу 1. Порты 1 и 2 объединяются в port channel 1. Когда порт 3 вступает в группу 1, port channel 1 из портов 1 и 2 разбирается и пересобирается с портом 3 опять в port channel 1. Когда порт 4 вступает в группу 1, port channel 1 из портов 1, 2 и 3 разбирается и пересобирается с портом 4 опять в port channel 1 (надо отметить, что каждый раз, когда новый порт вступает в группу объединения портов, группа разбирается и собирается заново). Теперь все 4 порта на обоих коммутаторах объединены в режиме

«ON».

2.6.5 Устранение неисправностей Port channel

Если во время конфигурации объединения портов возникли проблемы, в первую очередь проверьте следующее:

- Убедитесь, что все порты в группе имеют одинаковые настройки, например, они все в режиме полного дуплекса, имеют одинаковую скорость и настройки VLAN. Если обнаружены несоответствия, исправьте это.

Некоторые команды (arp, bandwigth, ip, ip-forward и т.д.) не могут быть использованы на портах в port channel.

2.7 КОНФИГУРИРОВАНИЕ MTU

2.7.1 Общие сведения об MTU

MTU (Maximal Transmition Unit) – максимальный размер кадра данных, который может быть передан без фрагментации. По умолчанию коммутатор отправляет\принимает кадры данных размером не более 1500 байт. Пакет, имеющий размер от 1519 до 9000, принято называть JUMBO-фрейм.

В настоящий момент Jumbo-фрейм не имеет определяющего стандарта в сетевых технологиях (в частности, не были стандартизированы формат пакета и длина). При использовании таких пакетов, скорость передачи данных в сети увеличивается на 2 % – 5 %. Технически JUMBO – это удлиненный фрейм, посылаемый и принимаемый коммутатором. Однако, учитывая длину, такие фреймы не могут быть посланы на процессор устройства. Мы исключаем посылку больших фреймов процессору во время приема пакетов.

2.7.2 Конфигурирование MTU

1. Включение функции MTU.

Команда	Описание
Общий режим	
mtu [<mtu-value>] no mtu enable	Включает функцию приема/посылки JUMBO-фреймов. Команда NO выключает функцию приема/посылки JUMBO-фреймов.

2.8 ФУНКЦИЯ PORT-SECURITY. БЕЗОПАСНОСТЬ ПОРТОВ

2.8.1 Введение

Port-Security — это механизм, основывающийся на MAC-адресе для управления доступом к сети. Это расширение существующих аутентификаций 802.1x и MAC. Он контролирует доступ неавторизированных устройств сети, проверяя MAC-адрес источника полученного кадра и доступ к неавторизированным устройствам, проверяя MAC-адрес устройства назначения в кадре. С Port-Security, пользователь может настраивать различные режимы безопасности порта для того, чтобы устройство обучалось только легальным MAC-адресам источника. Если после включения Port-Security устройство обнаруживает фрейм с неверным MAC-адресом, это вызывает соответствующую функцию Port-Security и выполняет предопределенные действия автоматически. Данный функционал снижает объем пользовательского обслуживания и значительно повышает безопасность системы.

2.8.2 Настройка безопасности портов

1. Базовые настройки безопасности портов.

Команда	Описание
Режим конфигурирования порта	
switchport port-security no switchport port-security	Настройка безопасности портов на интерфейсе.
switchport port-security mac-address <macaddress> [vlan <vlan-id>] no switchport port-security mac-address <macaddress> [vlan <vlan-id>]	Настройка статического безопасного MAC-адреса на интерфейсе
switchport port-security maximum <value> [vlan <vlan-list>] no switchport port-security maximum <value> [vlan <vlan-list>]	Настройка максимального числа безопасных MAC-адресов, разрешенных на интерфейсе

switchport port-security violation {protect | restrict | shutdown} no switchport port-security violation	Когда превышено максимальное число настроенных MAC-адресов, MAC-адрес доступа к интерфейсу не принадлежит этому интерфейсу в таблице MAC-адресов или MAC-адрес настроен на несколько интерфейсов в одном VLAN, они оба будут нарушать безопасность MAC-адресов.
switchport port-security aging {static | time <value> | type {absolute | inactivity}} no switchport port-security violation aging {static | time | type}	Включает время или тип старения port-security на интерфейсе.
Режим администратора	
clear port-security {all | configured | dynamic | sticky} [[address <mac-addr> | interface <interface-id>] [vlan <vlan-id>]]	Стирает введенные безопасные MAC-адреса на интерфейсе.
show port-security [interface <interface-id>] [address | vlan]	Показывает конфигурацию.

2.8.3 Примеры настройки Port-security

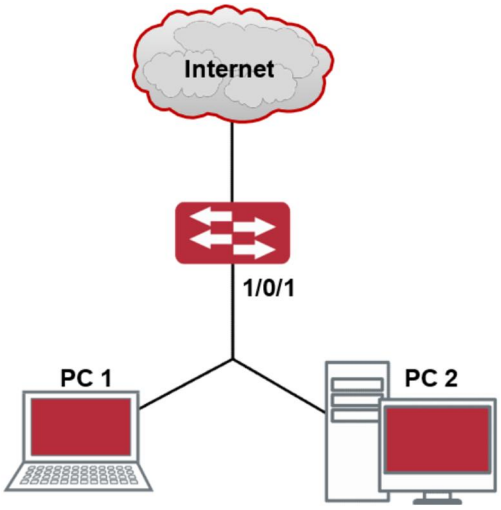


Рисунок 10.1 – Типичная схема топологии для безопасности порта.

На интерфейсе включена функция безопасности порта, настроено максимальное число разрешенных источников MAC-адресов на интерфейсе равное 10, и интерфейс разрешает доступ 10 пользователям в интернет. Если превышено максимальное количество, то новый пользователь не получит доступ в интернет, что не только отграничит число пользователей, но и сделает доступ в интернет безопасным. Если сделать настройку максимального числа безопасных MAC-адресов равной 1, то только PC1 или PC2 получат доступ в сеть.

Процесс настройки:

> *#Configure the switch.*
> *rotek(config)#interface Ethernet 1/0/1*

```
rotek(config-if-ethernet1/0/1)#switchport port-security
rotek(config-if- ethernet1/0/1)#switchport port-security maximum 10
rotek(config-if- ethernet1/0/1)#exit
rotek(config)#
```

2.8.4 Устранение неисправностей PORT SECURITY

Если возникают проблемы с настройкой безопасности, проверьте не являются ли они следствием следующих причин:

- Проверьте включен ли PORT SECURITY.

Убедитесь в настройке максимального количества MAC-адресов.

2.9 НАСТРОЙКА DDM

2.9.1 Введение

2.9.1.1 Краткое введение в DDM

DDM (Digital Diagnostic Monitor) реализует функцию подробной цифровой диагностики по стандарту SFF-8472 MSA. DDM контролирует параметры сигнала и оцифровывает его на интерфейсном оптическом модуле. После чего информация может быть считана коммутаторов для мониторинга.

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

Применение DDM предоставляет следующие возможности:

1. Прогноз продолжительности жизни модуля.

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

- Высокое напряжение Vcc приведет к поломке CMOS, низкое – к неправильной работе.
- Высокая RX-мощность приведёт к повреждению принимающего модуля, из-за низкой RX-мощности модуль не сможет нормально работать.
- Высокая температура приведет к быстрому старению аппаратных средств.
- Контроль мощности, получаемой по волокну, помогает проверить возможности линии и удаленного коммутатора.

2. Определение места повреждения.

В оптоволоконной линии определение неисправности имеет важное значение для быстрой перезагрузки сервиса, изолирование неисправности помогает администратору быстро найти местоположение неисправности в модуле (локальный или удаленный модули) или на линии, что также сокращает время восстановления системы после неисправности.

Анализируя статусы оповещения и сигнализации в режиме реального времени по параметрам (температура, напряжение, ток смещения, TX-мощность и RX-мощность) можно быстро обнаружить неисправность с помощью функции цифровой диагностики.

Кроме того, состояние Tx Fault и Rx LOS имеет важное значение для анализа неисправности.

3. Проверка совместимости.

Проверка совместимости используется для анализа, является ли конфигурация оборудования, включающего оптический модуль, согласованной вручную или совместима с соответствующим стандартом, поскольку возможности модуля могут быть реализованы только с совместимой конфигурацией включающего в себя данный модуль оборудования.

Иногда параметры включающего модуль оборудования превышают установленные вручную или стандарт соответствия, что приведет к уменьшению возможностей модуля и ошибке передачи.

Включающее модуль оборудование не совместимо:

- Напряжение превышает установленный диапазон.
- Rx power приводит к перезагрузке или к меньшей чувствительности приемопередатчика.
- Температура превышает диапазон рабочей температуры.

2.9.1.2 Функции DDM

Описание DDM показано в следующем примере:

1. Просмотр информации мониторинга на приемопередатчике.

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

2. Определение значения порога пользователем.

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

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

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

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

3. Контроль трансивера.

Кроме проверки состояния работы трансивера в реальном масштабе времени, пользователю нужно следить за подробной информацией о состоянии, такой как последнее время неисправности и ее тип. Контроль трансивера помогает пользователю найти последнее состояние неисправности через проверку логов и запросить последнее

состояние неполадки через выполнение команд. Когда пользователь находит информацию о неполадке оптического модуля, то информация об оптическом модуле может быть перепроверена после обработки информации о неисправности, здесь пользователь может знать информацию о неисправности и возобновить мониторинг.

2.9.2 Список команд конфигурации DDM

Настройка DDM:

1. Просмотр информации контроля в реальном масштабе времени.
2. Настройка значений порога сигнализации или оповещения каждого параметра для трансивера.
3. Настройка состояния мониторинга трансивера.
    - Настройка интервала мониторинга трансивера.
    - Настройка состояния включения мониторинга трансивера.
    - Просмотр информации мониторинга трансивера.
    - Очистка информации мониторинга трансивера.

1. Просмотр информации контроля в реальном масштабе времени.

Команда	Описание
Режим конфигурирования порта, режим администратора или глобальный режим	
show transceiver [interface ethernet <interface-list>] [detail]	Просмотр мониторинга состояния трансивера.

2.9.3 Примеры применения DDM

Пример 1:

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

- Просмотр информации о всех интерфейсах, которые могут читать параметры в режиме реального времени (при отсутствии оптического модуля или оптический модуль не поддерживается, информация не будет показана), для примера:

> *rotek#show transceiver*

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

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

> *rotek#show transceiver detail*

Ethernet 1/0/21 transceiver detail information:
Base information:
SFP found in this port, manufactured by company, on Sep 29 2010.
Type is 1000BASE-SX, Link length is 550 m for 50um Multi-Mode Fiber.
Link length is 270 m for 62.5um Multi-Mode Fiber.
Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.
Brief alarm information:
RX loss of signal Voltage high
RX power low
Detail diagnostic and threshold information:

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

Ethernet 1/0/22 transceiver detail information: N/A
Ethernet 1/0/24 transceiver detail information:
Base information:
SFP found in this port, manufactured by company, on Sep 29 2010.
Type is 1000BASE-SX,
Link length is 550 m for 50um Multi-Mode Fiber.
Link length is 270 m for 62.5um Multi-Mode Fiber.
Nominal bit rate is 1300 Mb/s,
Laser wavelength is 850 nm.
Brief alarm information: N/A
Detail diagnostic and threshold information: N/A

2.9.4 Устранение неисправностей DDM

Если при настройке DDM возникают проблемы, – пожалуйста, проверьте является ли эта проблема следствием следующих причин:

- Убедитесь, что трансивер на оптическом модуле был включен на порте, иначе конфигурация DDM не будет показана.
- При отсутствии оповещения по SNMP, убедитесь, что SNMP корректно сконфигурирован на коммутаторе;
- Не все коммутаторы поддерживают SFP с DDM или XFP с DDM, проверьте технические характеристики используемого коммутатора и убедитесь в использовании устройства с поддержкой соответствующей функции.
- Использование команд **show transceiver** или **show transceiver detail** может занять много времени, так как коммутатор будет проверять все порты, поэтому рекомендуется запрашивать информацию о трансивере на определенный порт.

Убедитесь, что установленный пользователем порог является действующим. При любой ошибке порогового значения трансивер будет посылать сигнализацию в соответствии со значением, установленным по умолчанию.

2.10 СТАТИСТИКА ПО ПОРТАМ

Статистика портов коммутатора (трафик, ошибки, состояние) — ключевой инструмент для мониторинга сети и диагностики неисправностей. Она позволяет выявить перегруженные интерфейсы, сбои кабелей и неправильные настройки. Ниже приведены команды для просмотра статистики по портам.

Команда	Описание
Режим глобального конфигурирования	
show interface ethernet status	Показать статус всех портом коммутатора.
show interface ethernet counter (packet | rate)	Показать счетчики портов.
Режим порта	
show interface ethernet <PORT:port> statistics	Получение статистики по порту.
show interface ethernet (<PORT:port> | <PORT_RANGE:ports>) detail	Получить детальную информацию о порте.

3 НАСТРОЙКА ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ (VLAN) И НАСТРОЙКА MAC

3.1 Конфигурирование VLAN

3.1.1 Начальные сведения о VLAN

VLAN (Virtual Local Area Network – виртуальная локальная сеть) – технология, разделяющая логические адреса устройств в сети для отделения сегментов сети в зависимости от функций, выполняемых устройствами, приложений или требований управления. Широковещательный, многоадресный и одноадресный трафик в одном VLAN отделен от других VLAN. Таким образом, виртуальные локальные группы могут формироваться независимо от физического расположения устройств. Для стандартизации применения VLAN IEEE опубликовал протокол IEEE 802.1Q. VLAN на коммутаторе работает в соответствии с этим протоколом.

Основная идея технологии VLAN в том, чтобы разделить динамически большую локальную сеть на несколько независимых широковещательных доменов в соответствии с требованиями, предъявляемыми к сети.

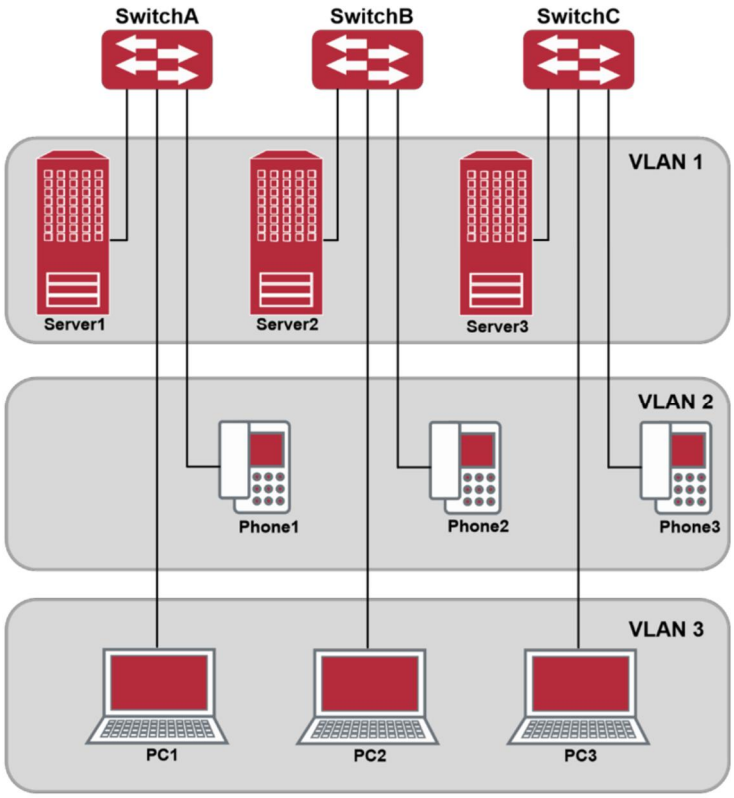


Рисунок 12.1 – Логическое определение сети VLAN

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

Благодаря вышеперечисленным особенностям, технология VLAN обеспечивает следующие преимущества:

- улучшается производительность сети;

- экономятся сетевые ресурсы;
- упрощается управление сетью;
- снижается стоимость сети;
- улучшается безопасность сети.

Ethernet-порты коммутатора могут работать в трех различных режимах: Access, Hybrid и Trunk. Каждый режим имеет свой способ пересылки пакетов, с меткой или без.

Access. Порты типа Access принадлежат только одному VLAN. Обычно они используются для подключения конечных устройств, таких как ПК или WI-FI маршрутизатор в квартире или офисе.

Trunk. Порты типа Trunk позволяют пересылать пакеты нескольких VLAN'ов. Они могут использоваться для соединения между коммутаторами или подключения пользовательских устройств. Обычно используется для соединения коммутаторов.

Hybrid. Порты типа Hybrid, также как и Trunk, позволяют пересылать пакеты нескольких VLAN'ов. Они могут использоваться для соединения между коммутаторами или подключения пользовательских устройств.

Порты типов Hybrid и Trunk принимают данные по одному алгоритму, но методы отправки данных отличаются: порты типа Hybrid могут отправлять пакеты в различные VLAN'ы без метки VLAN'а, тогда как порты типа Trunk отправляют пакеты различных VLAN только с меткой VLAN'а, за исключением VLAN, прописанного на порту как native.

Применение VLAN и GVRP (GARP VLAN Registration Protocol – протокол регистрации GARP VLAN) на коммутаторе описывается в стандарте 802.1Q. Данная глава детально объясняет использование и конфигурацию VLAN'ов и GVRP.

3.1.2 Конфигурирование VLAN

1. Создание или удаление VLAN.
2. Установка или удаление имени VLAN'а.
3. Присоединение порта коммутатора к VLAN'у.
4. Установка типа порта коммутатора.
5. Настройка транкового порта.
6. Настройка порта доступа.
7. Настройка гибридного порта.
8. Включение/выключение правил обработки входных пакетов VLAN на портах.
9. Конфигурация приватного VLAN'а.
10. Настройка связей приватного VLAN'а.
11. Определение внутреннего идентификатора VLAN'а.

1. Создание или удаление VLAN.

Команда	Описание
Режим глобального конфигурирования	
vlan WORD no vlan WORD	Создание/удаление VLAN'а или вход в режим VLAN'а

2. Установка или удаление имени VLAN’а.

Команда	Описание
VLAN Mode	
name <vlan-name> no name	Установка или удаление имени VLAN’а

3. Присоединение порта коммутатора к VLAN’у.

Команда	Описание
VLAN Mode	
switchport interface <interface-list> no switchport interface <interface-list>	Назначение порта коммутатора VLAN’у

4. Установка типа порта коммутатора.

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

5. Настройка транкового порта.

Команда	Описание
Режим конфигурирования порта	
switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD} no switchport trunk allowed vlan	Установка/удаление VLAN’ов, приписанных к этому транку. Команда «no» восстанавливает значение по умолчанию.
switchport trunk native vlan <vlan-id> no switchport trunk native vlan	Установка/удаление PVID для транкового порта.
vlan-trunking enable no vlan-trunking enable	Установка режима прозрачной передачи VLAN сетей на транковых интерфейсах без их создания

6. Настройка порта доступа.

Команда	Описание
Режим конфигурирования порта	
switchport access vlan <vlan-id> no switchport access vlan	Добавляет текущий порт к указанному VLAN’у. Команда NO восстанавливает значение по умолчанию.

7. Настройка гибридного порта.

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

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

Команда	Описание
Режим конфигурирования порта	
vlan ingress enable no vlan ingress enable	Включение/выключение входящих правил на VLAN'е.

9. Конфигурация приватного VLAN'а.

Команда	Описание
VLAN mode	
private-vlan {primary | isolated | community} no private-vlan	Конфигурация VLAN'а как текущего приватного. Команда NO удаляет приватный VLAN.

10. Настройка связей приватного VLAN'а.

Команда	Описание
VLAN mode	
private-vlan association <secondary-vlan-list> no private-vlan association	Установка/удаление связей приватного VLAN'а.

11. Определение внутреннего идентификатора VLAN'а.

Команда	Описание
Режим глобального конфигурирования	
vlan <2-4094> internal	Определяет идентификатор внутреннего VLAN'а.

3.1.3 Пример типичного применения VLAN

В соответствии с требованиями приложений и безопасности существующую локальную сеть необходимо разделить на три VLAN (Рисунок 12.2). Три VLAN имеют идентификаторы VLAN2, VLAN100 и VLAN200. Эти три VLAN охватывают два различных физических места размещения: площадки A и B.

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

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

Порты коммутоторов A и B в режиме trunk подключены к транковому каналу для передачи между узлами трафика VLAN. Остальные устройства подключены к другим портам VLAN'ов.

В данном примере порты 1 и 12 свободны и могут быть использованы для управляющих портов или других целей.

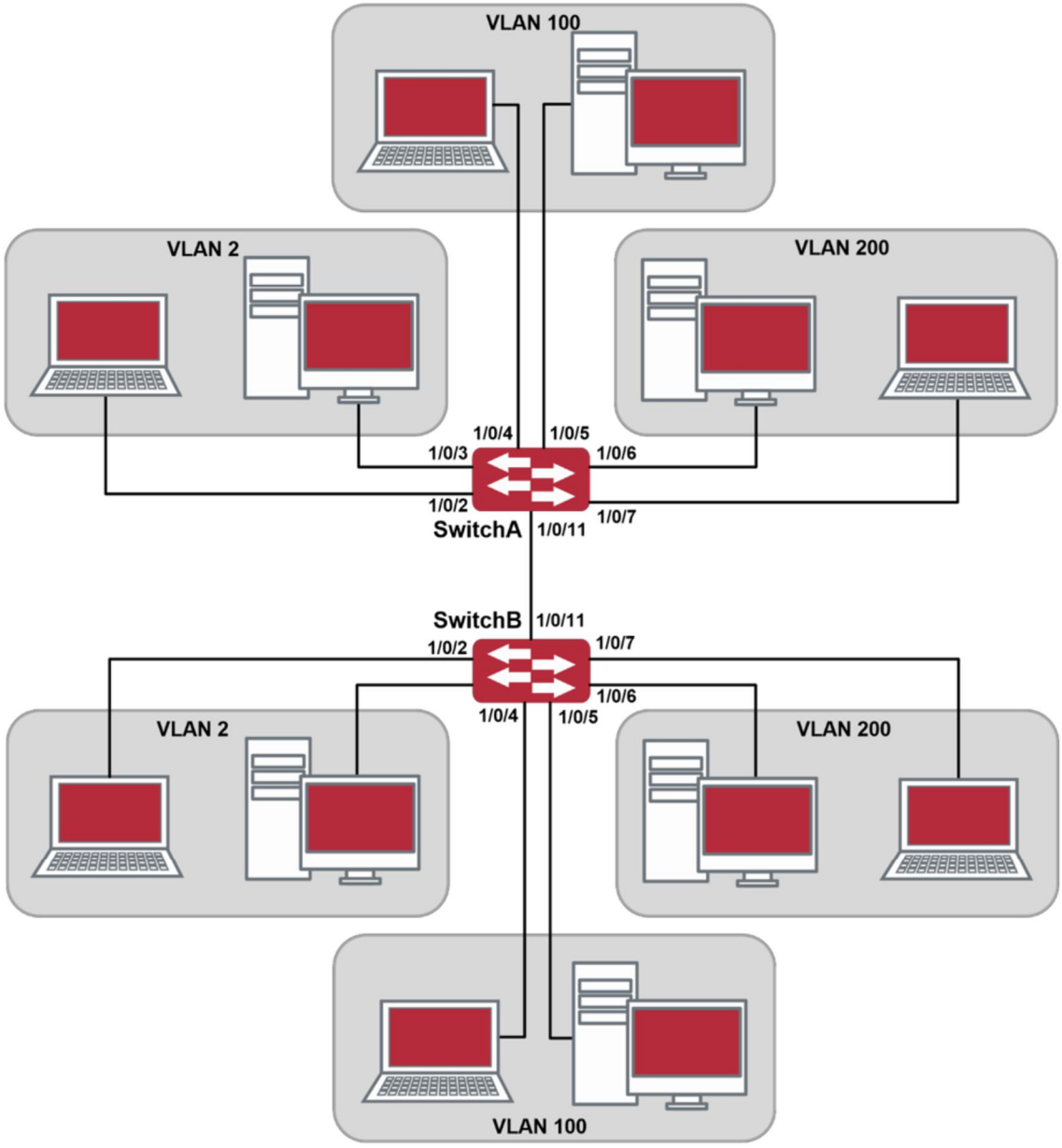


Рисунок 12.2 – Типичная топология применения VLAN’a

Шаги конфигурации описаны ниже:

Коммутатор A:

```
rotek(config)#vlan 2
rotek(Config-Vlan2)#switchport interface ethernet 1/0/2-3
rotek(Config-Vlan2)#exit
```

```
rotek(config)#vlan 100
rotek(Config-Vlan100)#switchport interface ethernet 1/0/4-5
rotek(Config-Vlan100)#exit rotek(config)#vlan 200
rotek(Config-Vlan200)#switchport interface ethernet 1/0/6-7
rotek(Config-Vlan200)#exit rotek(config)#interface ethernet 1/0/11
rotek(Config-If-Ethernet1/0/11)#switchport mode trunk
rotek(Config-If-Ethernet1/0/11)#exit
rotek(config)#
```

Коммутатор B:

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

3.1.4 Пример типичного применения гибридных (Hybrid) портов

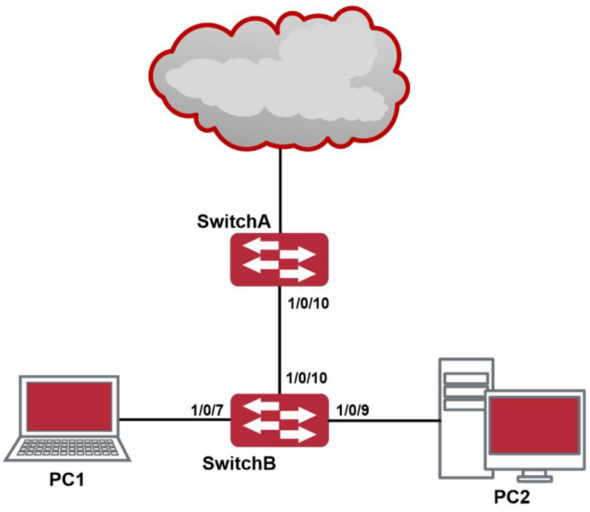


Рисунок 12.3 – Типичное применение гибридного порта

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

Требуется, чтобы PC1 и PC2 не видели друг друга по требованиям безопасности, но должны иметь доступ к другим сетевым ресурсам через шлюз коммутатора A.

Мы можем реализовать эту схему через гибридный порт. Конфигурация объектов как описано ниже:

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

Шаги конфигурации описаны ниже:

Коммутатор A:

```
rotek(config)#vlan 10
rotek(Config-Vlan10)#switchport interface ethernet 1/0/10
```

Коммутатор B:

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

3.2 Конфигурирование туннеля Dot1Q

3.2.1 Общие сведения о туннелях Dot1q

Туннель Dot1q, также называемый QinQ (802.1q-in-802.1q), является расширением протокола 802.1q. Основная идея заключается в упаковке метки клиентского VLAN (CVLAN tag) в метку VLAN сервис-провайдера (SPVLAN tag). Пакет с двумя метками VLAN’а передается через магистральную сеть интернет-провайдера, таким образом обеспечивая простой туннель второго уровня для пользователя. Это просто и легко для управления, применимо только на статических конфигурациях и специально адаптировано для небольших офисных или метро-сетей, использующих коммутаторы третьего уровня как магистральное оборудование.

После включения на клиентском порту, туннель Dot1q присваивает каждому пользователю идентификатор SPVLAN (SPVID). Здесь идентификатор пользователя – 3. Такой же SPVID может быть присвоен таким же пользователям на других PE (Рисунок 13.1). Когда пакет приходит с CE1 на PE1, он несет метки VLAN’ов 200-300 внутренней сети пользователя. Когда туннель Dot1q включен, клиентский порт на PE1 добавляет в пакет дополнительные метки VLAN’ов, у которых идентификатором является назначенный пользователю SPVID. Потом пакет будет направлен только в VLAN3, который уходит в сеть интернет-провайдера, и будет нести две метки VLAN’ов

(внутренняя метка добавлена, когда пакет пришел на PE1, и другая является SPVID), в то время как информация о клиентских VLAN открыта для провайдера сети. Когда пакет достигнет PE2 и перед отправкой на CE2 с клиентского порта на PE2, внешняя метка VLAN'а удаляется и пакет, пришедший на CE2, становится полностью идентичен пакету, отправленному с CE1. Для пользователя роль оператора сети между PE1 и PE2 заключается в обеспечении канала второго уровня.

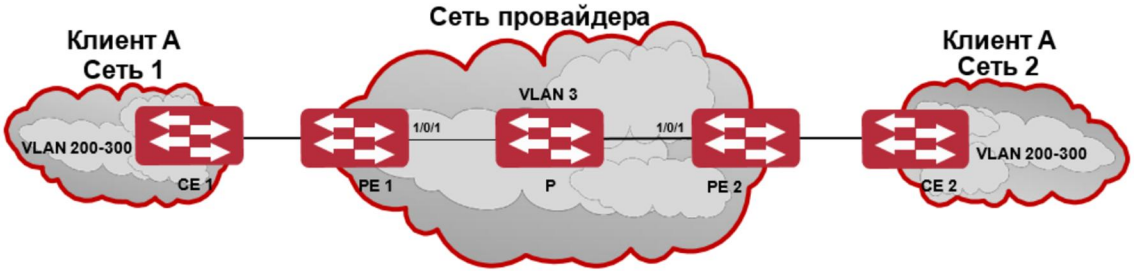


Рисунок 13.1 – Межсетевое взаимодействие на основе Dot1q-туннеля

Технология туннеля Dot1q позволяет интернет-сервис-провайдеру поддерживать множество клиентских VLAN'ов с помощью одного своего VLAN'а. Провайдер и клиент могут конфигурировать свои VLAN'ы независимо друг от друга.

Технология туннеля Dot1q имеет следующие характеристики:

- Обеспечение простого L2-канала для пользователя требует небольших ресурсов как со стороны настройки\обслуживания и со стороны аппаратных возможностей оборудования.
- Применима через простую статическую конфигурацию, не нужны сложная конфигурация и манипуляции.
- Оператор присваивает один SPVID каждому пользователю, что увеличивает количество одновременно поддерживаемых пользователей; в то же время пользователи имеют полную свободу при выборе и управлении идентификаторов VLAN (пользователь выбирает из диапазона от 1 до 4096).
- Клиентская сеть полностью независима. Когда интернет-сервис-провайдер модернизирует свою сеть, клиентские сети не требуют изменения конфигурации.

3.2.2 Конфигурирование туннеля Dot1q

1. Конфигурирование функции туннеля Dot1q на порту.
2. Конфигурирование типа протокола (TPID) на порту.

1. Конфигурирование функции туннеля Dot1q на порту.

Команда	Описание
Режим конфигурирования порта	
dot1q-tunnel enable no dot1q-tunnel enable	Включение / отключение режима туннеля dot1q на порту

2. Конфигурирование типа протокола (TPID) на порту.

Команда	Описание
Режим конфигурирования порта	

dot1q-tunnel tpid {0x8100|0x9100|0x9200|<1- 65535>}	Конфигурирование типа протокола на магистральном порту.

3.2.3 Пример типичного применения туннеля Dot1q

Сценарий:

Пограничные узлы PE1 и PE2 интернет-провайдера пересылают данные VLAN'ов 200-300. Между CE1 и CE2 клиентской сети через VLAN3. Порт PE1 подключен к CE1, порт 10 подключен к публичной сети, TPID подключенного оборудования – 9100; Порт 1 PE2 подключен к CE2, порт 10 подключен к публичной сети.

Объект конфигурации	Описание конфигурации
VLAN3	Порт 1/0/1 узлов PE1 и PE2.
dot1q-tunnel	Порт 1/0/1 узлов PE1 и PE2.
tpid	9100

Процедура конфигурации описана ниже:

PE1:

```
rotek(config)#vlan 3
rotek(Config-Vlan3)#switchport interface ethernet 1/0/1
rotek(Config-Vlan3)#exit
rotek(Config)#interface ethernet 1/0/1
rotek(Config-Ethernet1/0/1)# dot1q-tunnel enable
rotek(Config-Ethernet1/0/1)# exit
rotek(Config)#interface ethernet 1/0/10
rotek(Config-Ethernet1/0/10)#switchport mode trunk
rotek(Config-Ethernet1/0/10)#dot1q-tunnel tpid 0x9100
rotek(Config-Ethernet1/0/10)#exit
rotek(Config)#
```

PE2:

```
rotek(config)#vlan 3
rotek(Config-Vlan3)#switchport interface ethernet 1/0/1
rotek(Config-Vlan3)#exit
rotek(Config)#interface ethernet 1/0/1
rotek(Config-Ethernet1/0/1)# dot1q-tunnel enable
rotek(Config-Ethernet1/0/1)# exit
rotek(Config)#interface ethernet 1/0/10
rotek(Config-Ethernet1/0/10)#switchport mode trunk
rotek(Config-Ethernet1/0/10)#dot1q-tunnel tpid 0x9100
rotek(Config-Ethernet1/0/10)#exit
rotek(Config)#
```

3.2.4 Устранение неисправностей туннеля Dot1q

- Включение туннеля Dot1q на порту в режиме Trunk делает метку пакета данных непредсказуемой, что не подходит для использования. Поэтому не рекомендуется использовать туннель Dot1q на транковом порту.
- Использование туннеля совместно с STP/MSTP не поддерживается.
- Использование туннеля совместно с PVLAN (Private VLAN) не поддерживается.
- После изменении настроек VLAN необходимо переинициализировать функцию dot1q на затронутых портах следующими командами (в режиме конфигурации порта):

no dot1q-tunnel enable
dot1q-tunnel enable

3.3 Настройка VLAN-translation

3.3.1 Общие сведения о трансляции VLAN’ов

Функция VLAN-translation (трансляция VLAN’ов), как следует из названия, транслирует оригинальный идентификатор VLAN’а в новый в соответствии с требованиями пользователя или для обмена данными между различными VLAN’ами. Трансляция может применяться как для входящей, так и исходящей информации. Данное оборудование поддерживает изменение идентификатора VLAN’а только на входе.

3.3.2 Конфигурирование трансляции VLAN’а

1. Конфигурирование функции трансляции VLAN’а на порту.
2. Конфигурирование соответствий трансляции VLAN’а на порту.
3. Просмотр конфигурации соответствий трансляции VLAN’а.

1. Конфигурирование функции трансляции VLAN’а на порту.

Команда	Описание
Режим конфигурирования порта	
vlan-translation enable no vlan-translation enable	Включает или выключает режим трансляции VLAN

2. Конфигурирование соответствий трансляции VLAN’а на порту.

Команда	Описание
Режим конфигурирования порта	
vlan-translation <old-vlan-id> to <new-vlan-id> (in | out) no vlan-translation old-vlan-id (in | out)	Добавление/удаление соответствий трансляции VLAN’ов.

3. Просмотр конфигурации соответствий трансляции VLAN’а.

Команда	Описание
Режим администратора	
show vlan-translation	Просмотр сконфигурированных соответствий трансляции VLAN’ов

3.3.3 Типовое применение трансляции VLAN’ов

Сценарий:

Пограничные узлы PE1 и PE2 интернет-провайдера поддерживают VLAN данных 20 между CE1 и CE2 из клиентской сети, через VLAN 3. Порт 1/0/1 PE1 Подключен к CE1,

порт 1/0/10 подключен к публичной сети, порт 1/0/1 PE2 подключен к CE2, порт 1/0/10 подключен к публичной сети.

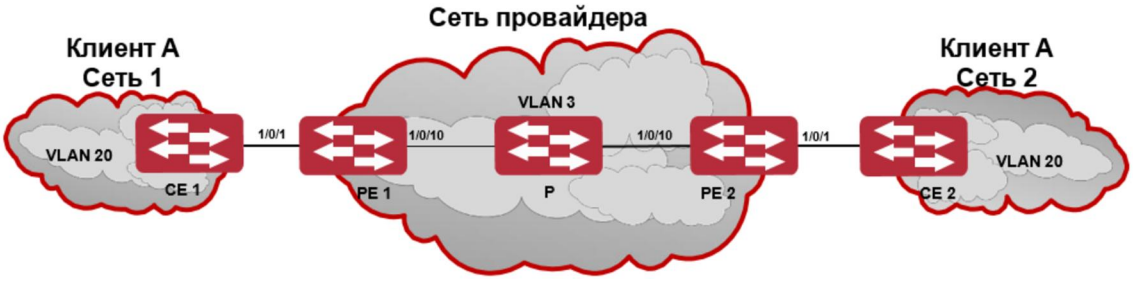


Рисунок 14.1 – Топология сети с трансляцией VLAN’ов

Объект конфигурации	Описание конфигурации
VLAN-translation	Порт 1/0/1 узлов PE1 и PE2.
Trunk port	Порты 1/0/1 и 1/0/10 узлов PE1 и PE2.

Процедура конфигурирования указана ниже:

PE1, PE2:

```
rotek(Config)#interface ethernet 1/0/1
rotek(Config-Ethernet1/0/1)#switchport mode trunk
rotek(Config-Ethernet1/0/1)# vlan-translation enable
rotek(Config-Ethernet1/0/1)# vlan-translation 20 to 3 in
rotek(Config-Ethernet1/0/1)# vlan-translation 3 to 20 out
rotek(Config-Ethernet1/0/1)# exit
rotek(Config)#interface ethernet 1/0/1
rotek(Config-Ethernet1/0/1)#switchport mode trunk
rotek(Config-Ethernet1/0/1)#exit rotek(Config)#
```

3.3.4 Устранение неисправностей трансляции VLAN’ов

Обычно трансляция VLAN применяется на транковых портах.

Приоритеты между трансляцией VLAN’ов и входящей фильтрацией VLAN’ов распределяются так: Трансляция VLAN’ов выше входящей фильтрации VLAN’ов.

3.4 Конфигурация Multi-to-One VLAN-translation

3.4.1 Введение в Multi-to-One VLAN-трансляцию

Трансляция Multi-to-One VLAN – это трансляция исходного VLAN ID в новом VLAN ID в соответствии с требованиями пользователей на восходящий (uplink) траффик и возвращение исходного VLAN ID на нисходящий (downlink) траффик.

3.4.2 Настройка передачи Multi-to-One VLAN

1. Настройка Multi-to-One VLAN-передачи на порте.
2. Просмотр настроек и Multi-to-One VLAN-передач.

1. Настройка Multi-to-One VLAN-передачи на порте.

Команда	Описание

Режим конфигурирования порта	
vlan-translation n-to-1 <WORD> to <new-vlan-id> no vlan-translation n-to-1 <WORD>	Включение/отключение трансляции Multi-to-One VLAN

2. Просмотр настроек Multi-to-One VLAN-передачи.

Команда	Описание
Режим администратора	
show vlan-translation n-to-1	Показывает связанные настройки трансляции Multi-to- One VLAN

3.4.3 Пример типичного применения трансляции Multi-to-One VLAN

Сценарий:

Пользователи 1, 2 и 3 принадлежат VLAN 1, 2 и 3 соответственно. Входящий траффик данных, пользователей 1, 2 и 3 будет переведен в VLAN100 на интерфейсе Ethernet1/0/1 со стороны SwitchA. Таким же образом будет передан траффик данных пользователей 4, 5 и 6.

Элемент конфигурации	Описание
VLAN	SwitchA, SwitchB
Trunk Port	Нисходящий порт 1/0/1 и восходящий порт 1/0/5 на SwitchA и SwitchB
Multi-to-One VLAN-трансляция	Нисходящий порт 1/0/1 на SwitchA и SwitchB

Процедура настройки:

> *Switch1, Switch2:*
> *rotek(Config)# vlan 1-3;100*
> *rotek(Config-Ethernet1/0/1)#switchport mode trunk*
> *rotek(Config-Ethernet1/0/1)# vlan-translation n-to-1 1-3 to 100*
> *rotek(Config)#interface ethernet 1/0/5*
> *rotek(Config-Ethernet1/0/5)#switchport mode trunk*
> *rotek(Config-Ethernet1/0/5)#exit*

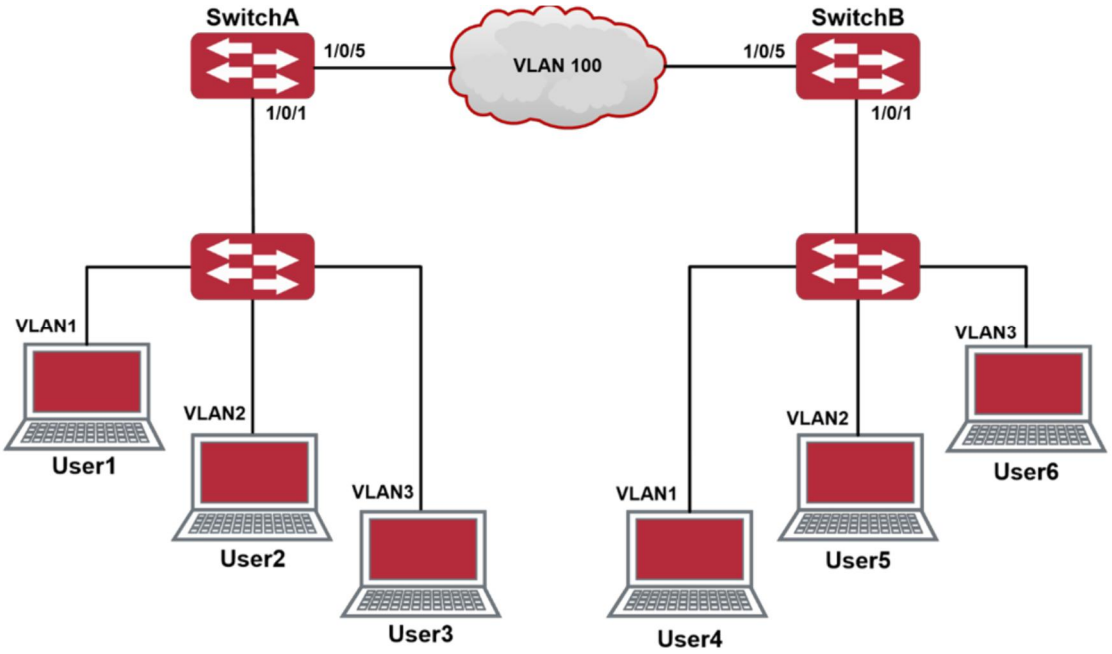


Рисунок 15.1 – Типичное применение трансляции VLAN

3.4.4 Устранение неисправностей Multi-to-One VLAN-трансляции

- Нельзя использовать Multi-to-One VLAN-трансляцию одновременно с Dot1q-tunnel.
- Нельзя использовать Multi-to-One VLAN-трансляцию одновременно с VLAN-translation.
- одинаковые MAC-адреса не должны существовать в оригинальном и транслированном VLAN.
- Убедитесь, что аппаратный чип может поддерживать нормальную работу клиентов.
- Превышение предела обучения MAC-адресам может повлиять на Multi-to-One VLAN-трансляцию.

Multi-to-One VLAN-трансляция должна быть включена после MAC-обучения.

3.5 НАСТРОЙКА ТАБЛИЦЫ MAC-АДРЕСОВ

3.5.1 Общие сведения о таблице MAC-адресов

Таблица MAC-адресов — это таблица соответствий MAC-адресов устройств назначения портам коммутатора. MAC-адреса делятся на статические и динамические. Статические MAC-адреса вручную сконфигурированы пользователем, имеют наивысший приоритет и действуют постоянно (они не могут быть замещены динамическим MAC-адресами). Динамические адреса запоминаются коммутатором при передаче пакетов данных, и они действуют ограниченное время. Когда коммутатор получает фрейм данных для пересылки, он сохраняет MAC-адрес источника фрейма и соответствующий ему порт назначения. Когда таблица MAC-адресов опрашивается на предмет MAC-адреса приемника, при нахождении нужного адреса, пакет данных отправляется на соответствующий порт, в противном случае коммутатор пересылает пакет на свой широковещательный домен. Если динамический MAC-адрес не встречается в пакетах для пересылки длительное время, запись о нем удаляется из таблицы MAC-адресов коммутатора.

Для таблицы MAC-адресов определены две операции:

1. Получение MAC-адреса.
2. Отправка или фильтрация пакета данных в соответствии с таблицей MAC-адресов.

3.5.1.1 Получение таблицы MAC-адресов

Таблица MAC-адресов может быть построена статически или динамически. Статическим конфигурированием настраивается соответствие между MAC-адресами и портами. Динамическое обучение – это процесс, когда коммутатор изучает связи между MAC-адресами и портами и регулярно обновляет таблицу MAC-адресов. В данном подразделе мы остановимся на процессе динамического построения таблицы MAC-адресов.

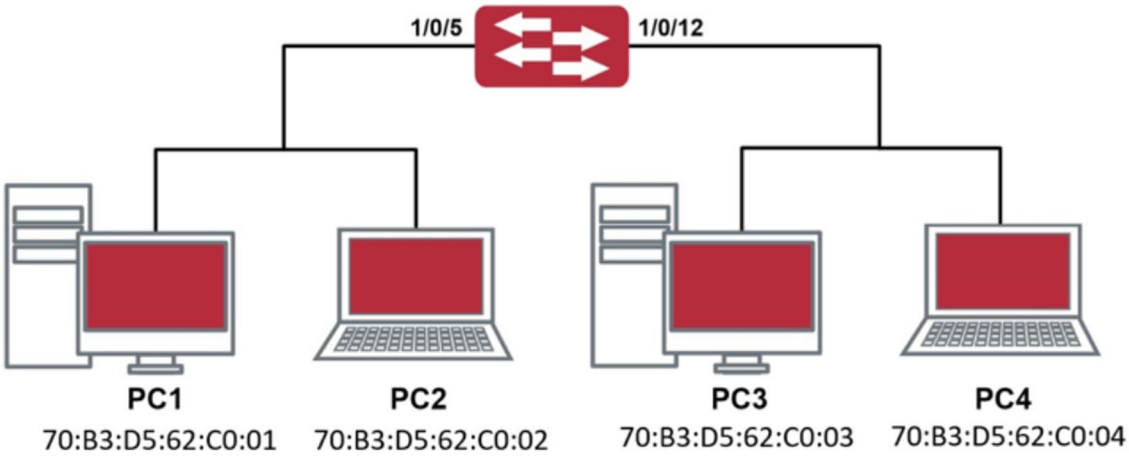


Рисунок 16.1 – Динамическое построение таблицы MAC-адресов

Топология описанного примера представлена на рисунке выше: 4 ПК подключены к коммутатору, где PC1 и PC2 принадлежат одному физическому сегменту (домену коллизий), физический сегмент подключен к порту 1/0/5 коммутатора, PC3 и PC4 принадлежат к другому физическому сегменту, подключенному к порту 1/0/12 коммутатора.

Начальная таблица MAC-адресов не содержит никаких значений. Возьмем для примера процесс связи между PC1 и PC3. Процесс обучения MAC-адресам, следующий:

1. Когда PC1 посылает сообщение к PC3, MAC-адрес источника 70:B3:D5:62:C0:01 и порт 1/0/5 из этого сообщения заносятся в таблицу MAC-адресов коммутатора.
2. В то же время коммутатору надо понять, как доставить сообщение на адрес 70:B3:D5:62:C0:03. Так как таблица содержит запись только для адреса 70:B3:D5:62:C0:01 и порта 1/0/5, а для адреса 70:B3:D5:62:C0:04 никаких записей нет, коммутатор рассылает данное сообщение на все свои порты (предполагаем, что все порты принадлежат по умолчанию VLAN1).
3. PC3 и PC4 получают сообщение, посланное PC1, но PC4 не отвечает на это сообщение, так как адрес приемника 70:B3:D5:62:C0:03, и отвечать на него будет только PC3. Когда порт 1/0/12 получает сообщение, отправленное PC3, в таблицу MAC-адресов добавляется запись о MAC-адресе 70:B3:D5:62:C0:03 и соответствующем ему порте 1/0/12.
4. Теперь таблица MAC-адресов имеет две динамические записи: MAC-адрес 70:B3:D5:62:C0:01 – порт 1/0/5 и 70:B3:D5:62:C0:03 – порт 1/0/12.
5. После обмена пакетами между PC1 и PC3, коммутатор больше не получает пакетов, отправленных PC1 и PC3. И записи в таблице MAC-адресов, соответствующие этим устройствам удаляются через 300 или 2×300 секунд (т.е. простое или двойное время жизни). 300 секунд здесь это время жизни по умолчанию для записей в таблице MAC-адресов. Время жизни может быть изменено на коммутаторе.

3.5.1.2 Пересылка или фильтрация кадров

Коммутатор посылает или отфильтровывает принимаемые пакеты данных в соответствии с таблицей MAC-адресов. Рассматривая для примера рисунок выше, предполагаем, что коммутатор изучил адреса PC1 и PC3, и пользователь вручную настроил соответствие портов для PC2 и PC4. Таблица MAC-адресов коммутатора будет следующей:

MAC-адрес	Номер порта	Кем добавлена запись
70:B3:D5:62:C0:01	1/0/5	Динамическое обучение
70:B3:D5:62:C0:02	1/0/5	Статическая конфигурация
70:B3:D5:62:C0:03	1/0/12	Динамическое обучение
70:B3:D5:62:C0:04	1/0/12	Статическая конфигурация

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

Если PC1 посылает пакет к PC3, коммутатор отправляет данные, полученные с порта 1/0/5 на порт 1/0/12

2. Фильтрация данных в соответствии с таблицей MAC-адресов.

Если PC1 посылает сообщение PC2, коммутатор, проверив таблицу MAC-адресов, находит PC2 и PC1 в одном физическом сегменте и отфильтровывает это сообщение (то есть сбрасывает это сообщение).

Коммутатором могут пересылаться три типа кадров:

- Широковещательные – Broadcast frames;
- Многоадресные – Multicast frames;
- Одноадресные – Unicast frames.

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

1. Broadcast frame: Коммутатор может определять коллизии в домене, но только не для широковещательных доменов. Если VLAN’ы не установлены, все устройства, подключенные к коммутатору, считаются находящимися в одном широковещательном домене. Когда коммутатор получает Broadcast frame, он пересылает его во все порты. Если VLAN’ы сконфигурированы, таблица MAC-адресов адаптируется в соответствии с дополнительной информацией о VLAN’ах. В этом случае коммутатор отправляет фрейм только на порты, находящиеся в том же VLAN’е.
2. Multicast frame: если многопользовательский домен неизвестен, коммутатор рассылает фрейм в том же VLAN’е, но, если включена функция IGMP snooping или сконфигурирована статическая многопользовательская группа, коммутатор будет посылать этот фрейм в порты многопользовательской группы.
3. Unicast frame: если VLAN’ы не сконфигурированы, то, если MAC-адрес приемника есть в таблице MAC-адресов коммутатора, коммутатор напрямую пересылает пакет в соответствующий порт. Если же адрес приемника в таблице не найден, коммутатор делает широковещательную рассылку этого фрейма. Если VLAN’ы сконфигурированы, коммутатор рассылает Unicast frame только внутри одного VLAN’а. Если MAC-адрес найден в таблице, но принадлежит другому VLAN’у, коммутатор делает широковещательную рассылку фрейма в том VLAN’е, к которому принадлежит фрейм.

3.5.2 Конфигурирование таблицы MAC-адресов

1. Конфигурирование времени жизни MAC-адресов.

2. Конфигурирование статической фильтрации или пересылки.
3. Конфигурирование функции ограничения количества динамических MAC-адресов
4. Очистка динамической таблицы MAC-адресов.
5. Настройка обучения MAC-адресов через управление процессором.
6. Настройка защиты от коллизий

1. Конфигурирование времени жизни MAC-адресов.

Команда	Описание
Режим глобального конфигурирования	
mac-address-table aging-time <0|aging-time> no mac-address-table aging-time	Конфигурирование времени жизни MAC-адресов

2. Конфигурирование статической фильтрации или пересылки.

Команда	Описание
Общий режим	
mac-address-table {static | static-multicast | blackhole} address <mac-addr> vlan <vlan-id> [interface [ethernet | portchannel] <interfacename>] | [source|destination|both] no mac-address-table {static | static-multicast | blackhole | dynamic} [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet | portchannel] <interface-name>]	Конфигурирование статических записей для MAC-адресов, статических многопользовательских записей, записей фильтрации пакетов.

3. Конфигурирование функции ограничения количества динамических MAC-адресов

Команда	Описание
Режим конфигурации порта	
switchport mac-address dynamic maximum no switchport mac-address dynamic maximum	Включение/отключение функции ограничения количества динамических MAC-адресов. Команда no отключает эту функцию.

4. Очистка динамической таблицы MAC-адресов.

Команда	Описание
Режим администратора	
clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet	Очистка динамической таблицы MAC-адресов

| portchannel] <interface-name>]	

5. Настройка обучения MAC-адресов через управление процессором.

Команда	Описание
Режим глобального конфигурирования	
mac-address-learning cpu-control no mac-address-learning cpu-control	Включение/отключение обучения MAC-адресов через управление CPU

6. Настройка защиты от коллизий.

Команда	Описание
Режим глобального конфигурирования	
mac-address-table avoid-collision no mac-address-table avoid-collision	Включение/отключение функции таблицы коллизии MAC-адресов, выданных ffp
show collision-mac-address-table	Показывает таблицу коллизий MAC-адресов
Режим администратора	
clear collision-mac-address-table	Очистить таблицу MAC-адресов

3.5.3 Примеры типичной конфигурации

Сценарий:

Четыре компьютера, как показано на рисунке, подключены к портам 1/0/5, 1/0/7, 1/0/9, 1/0/11 коммутатора. Все 4 компьютера принадлежат по умолчанию VLAN1. В соответствии с требованиями к сети, включено обучение динамическим адресам. PC1 содержит важные данные, и недоступен для других компьютеров из других физических сегментов; PC2 и PC3 статически приписаны к портам 7 и 9, соответственно.

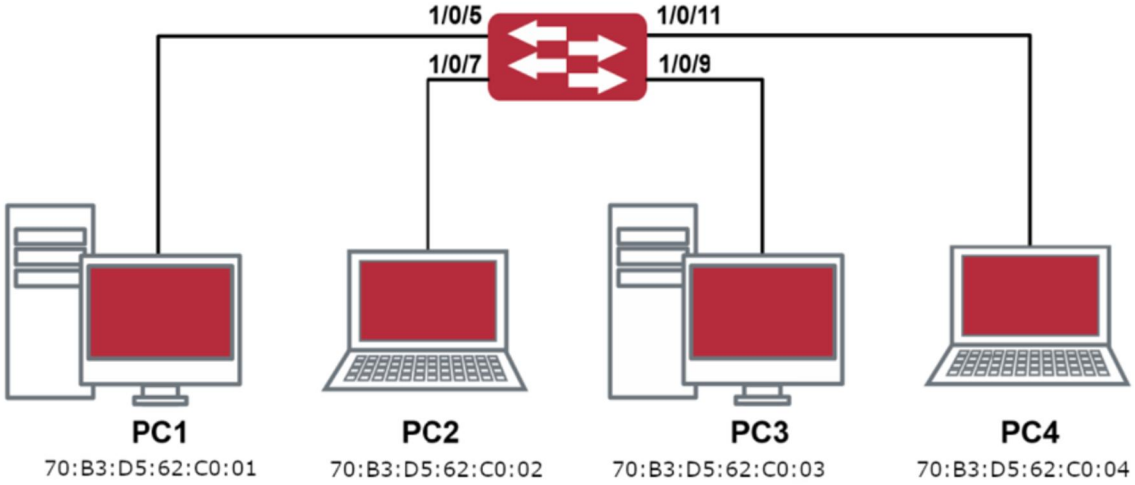


Рисунок 16.2 – Типовой пример конфигурации таблицы MAC-адресов Этапы конфигурации показаны ниже:

1. Установка MAC-адреса 70:B3:D5:62:C0:01 PC1 как фильтруемого.

```
rotek(config)#mac-address-table static 70:B3:D5:62:C0:01 discard vlan 1
```

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

```
rotek(config)#mac-address-table static address 70:B3:D5:62:C0:02 vlan 1 interface ethernet 1/0/7
rotek(config)#mac-address-table static address 70:B3:D5:62:C0:03 vlan 1 interface ethernet 1/0/9
```

3.5.4 Устранение неисправностей, связанных с таблицей MAC-адресов

При использовании команды show mac-address-table, было выяснено, что на порту произошел сбой обучения MAC-адресам устройств, подключенных к нему.

Возможные причины:

- Подключенный кабель поврежден.
- На порту включен Spanning Tree в статусе «discarding» или порт только что подключился и Spanning Tree пока в статусе вычисления дерева. Дождитесь, пока вычисление структуры закончится и порт обучится MAC-адресу.
- Если проблемы, описанные выше, не обнаружены, проверьте порт коммутатора и, при необходимости, свяжитесь с тех.поддержкой для решения проблемы.

3.5.5 Дополнительные функции таблицы MAC-адресов

3.5.5.1 Привязка MAC-адресов

3.5.5.1.1 Общие сведения о привязке MAC-адресов

Большинство коммутаторов поддерживают режим обучения MAC-адресам. Каждый порт может динамически запомнить несколько MAC-адресов, таким образом возможна передача потоков данных между известными MAC-адресами внутри порта. Если срок жизни MAC-адреса истек, пакет, направленный на этот адрес, будет разослан широковещательно.

Другими словами, MAC-адрес, которому обучился порт, будет использоваться для передачи пакетов к этому порту. Если соединение переключено на другой порт, коммутатор снова выполнит обучение MAC-адресу и будет передавать данные новому порту.

Однако, в некоторых случаях политика управления или секретности может требовать, чтобы MAC-адреса были прикреплены к портам, и только потоки с привязанных MAC-адресов будут пропускаться к пересылке на порт. То есть, после привязки MAC-адреса к порту, в этот порт могут передаваться только данные, предназначенные для данного MAC-адреса. Потоки данных, предназначенные для других MAC-адресов, не привязанных к данному порту, не будут пропускаться через порт.

3.5.5.1.2 Настройка привязки MAC-адресов

1. Включение функции привязки MAC-адресов на порту.
2. Привязка MAC-адреса к порту.
3. Конфигурация параметров функции привязанных MAC-адресов.
4. Конфигурация SNMP-трапов для уведомлений о MAC-адресах.

1. Включение функции привязки MAC-адресов на порту.

Команда	Описание
Режим конфигурирования порта	
switchport port-security no switchport port-security	Включение функции привязки MAC-адреса на порту и фиксация порта. Когда порт зафиксирован, функция обучения MAC-адресам выключена: Команда «no switchport port-security» выключает функцию привязки MAC-адреса на порту и восстанавливает функцию обучения MAC-адресам на порту

2. Фиксация MAC-адреса на порту.

Команда	Описание
Режим конфигурирования порта	
switchport port-security aging no switchport port-security aging	Включает функцию таймера фиксации порта. Команда «no switchport port-security aging» восстанавливает значение по умолчанию.
switchport port-security mac-address [<macaddress> | sticky] no switchport port-security mac-address [<mac-address> | sticky]	Добавляет статические безопасные MAC-адреса. Команда «no switchport port-security macaddress» удаляет статические безопасные MAC-адреса.
Режим администратора	
clear port-security dynamic [address <macaddr> | interface <interface-id>]	Очищает динамические MAC-адреса, выученные на указанном порту.

3. Конфигурация параметров привязки MAC-адресов.

Команда	Описание
Режим конфигурирования порта	
switchport port-security maximum <value> no switchport port-security maximum <value>	Устанавливает максимальное число безопасных MAC-адресов на порту; команда «no switchport port-security maximum» восстанавливает значение по умолчанию.
switchport port-security violation {protect | restrict | shutdown} [recovery] no switchport port-security violation	Установка режима нарушения на порту; команда «no switchport port-security violation» восстанавливает значение по умолчанию.

3.5.5.1.3 Устранение проблем привязки MAC-адресов

Включение привязки MAC-адресов на порту может быть неудачным по нескольким причинам. Ниже приводится несколько возможных причин и их устранение:

- Если привязанный MAC-адрес недоступен на порту, убедитесь, что порт не входит в port-aggregation и не сконфигурирован как транковый. Привязанный MAC-адрес уникален в конкретной конфигурации. Если вы хотите привязать MAC-адрес, функции, упомянутые выше, должны быть выключены.

Если безопасный адрес установлен как статический адрес и удален, тогда этот безопасный адрес не может быть использован, хотя он и будет существовать. Исходя из этого, рекомендуется избегать назначения статических адресов для портов, для которых включена привязка MAC-адресов.

3.6 Динамический VLAN

3.6.1 Общие сведения о Динамическом VLAN

Динамический VLAN - это обобщенное понятие, названное так в противопоставление статическому VLAN (применяемому статически на порт). Динамический **VLAN** включает в себя **VLAN** основанный на MAC-адресах, **VLAN** подсетей и протокольный **VLAN**.
VLAN, основанный на MAC-адресах (MAC VLAN) - это технология, позволяющая распределять трафик по **VLAN** на основе MAC-адреса: каждый хост с различным MAC-адресом может быть назначен определенному **VLAN**, в зависимости от обозначенных требований. Это дает возможность отказаться от настройки VLAN при изменении местоположения пользователя: в не зависимости от местоположения, трафик пользователя будет определен в свой VLAN.
VLAN подсетей (IP-subnet VLAN) - технология, позволяющая распределять трафик по различным **VLAN** на основе IP-адреса источника и маске его подсети. Его преимущество такое же, как у **VLAN** на основе MAC: пользователю не нужно изменять конфигурацию при изменении своего местоположения.
Разделение **VLAN на основе протокола сетевого уровня (Protocol VLAN)** будет удобен для тех администраторов, которые хотят разделять пользователей по приложениям или сервисам. Его удобство состоит в том, что пользователь может изменять свое местоположение в сети, сохраняя при этом свое членство во **VLAN**.

3.6.2 Конфигурация динамических VLAN

1. Включение функции Динамических VLAN на интерфейсе
2. Выбор VLAN в качестве MAC VLAN
3. Настройка соответствия между MAC-адресом и VLAN
4. Включение IP-subnet VLAN на интерфейсе
5. Настройка соответствия между IP маской и VLAN
6. Настройка соответствия между протоколом сетевого уровня и VLAN
7. Настройка приоритета для Динамических VLAN

1. Включение функции Динамического VLAN на интерфейсе

Команда	Описание
В режиме конфигурации порта	
switchport mac-vlan enable	Включить функцию динамических VLAN на интерфейсе
no switchport mac-vlan enable	Выключить функцию динамических VLAN на интерфейсе

2.Выбор VLAN в качестве MAC VLAN

Команда	Описание
В режиме глобальной конфигурации	
mac-vlan vlan <vlan-id>	назначить VLAN в качестве MAC-based VLAN

no mac-vlan	удалить MAC-based VLAN

3. Настройка соответствия между MAC-адресом и VLAN

Команда	Описание
В режиме глобальной конфигурации	
mac-vlan mac <mac-address> <mac-mask> vlan <vlan-id> priority <priority-id> no mac-vlan {mac <mac-address> <mac-mask>|all}	Создать соответствие между MAC-адресом и VLAN Удалить соответствие между MAC-адресом и VLAN

5. Настройка соответствия между IP маской и VLAN

Команда	Описание
В режиме глобальной конфигурации	
subnet-vlan ip-address <ipv4-address> mask <subnet-mask> vlan <vlan-id> priority <priority-id> no subnet-vlan {ip-address <ipv4-addrss> mask <subnet-mask>|all}	Добавить соответствие между IP-подсетью и VLAN Удалить соответствие между IP-подсетью и VLAN

6. Настройка соответствия между протоколом сетевого уровня и VLAN

Команда	Описание
В режиме глобальной конфигурации	
protocol-vlan mode {ethernetii etype <etype-id>|llc {dsap <dsap-id> ssap <ssap-id>}|snap etype <etype-id>} vlan <vlan-id> priority <priority-id> no protocol-vlan {mode {ethernetii etype <etype-id>|llc {dsap <dsap-id> ssap <ssap-id>}|snap etype <etype-id>}|all}	Добавить соответствие между протоколом и VLAN Удалить соответствие между протоколом и VLAN

4 QoS И ПЕРЕНАПРАВЛЕНИЕ ПОТОКОВ

4.1 НАСТРОЙКА QOS

4.1.1 Общие сведения о QoS

QoS (Quality of Service – качество сервиса) – набор возможностей которые позволяют создавать разделенные полосы для передаваемых по сети данных, тем самым обеспечивая лучший сервис для выбранного сетевого трафика. QoS – гарантия качества последовательной и предсказуемой передачи данных для обеспечения требований программ. QoS не создает дополнительной полосы передачи, но обеспечивает более эффективное управление полосой в соответствии с требованиями приложений и политикой управления сетью.

4.1.1.1 Термины QoS

QoS: Качество сервиса, обеспечение гарантированного качества сервиса для последовательной и предсказуемой передачи данных и выполнения требований программ.

Домен QoS: Домен QoS поддерживает устройства с QoS для формирования сетевой топологии, которая обеспечит качество сервиса. Такая топология называется доменом QoS.

CoS: Класс сервиса - классификационная информация, передаваемая фреймами 802.1Q на втором уровне. Занимает три бита поля Tag в заголовке фрейма и называется уровнем пользовательского приоритета в диапазоне от 0 до 7.

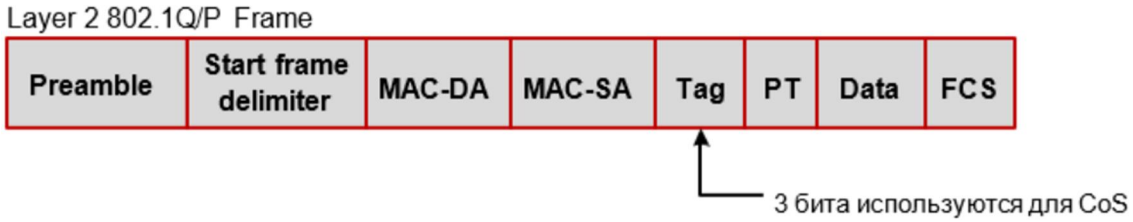


Рисунок 17.1 – Приоритеты Класса сервиса

ToS: Тип сервиса. Однобайтовое поле, передаваемое в заголовке пакета IPv4 на третьем уровне для объявления типа сервиса IP-пакета. Значением поля ToS может быть приоритет IP (IP Precedence) или значение DSCP.



Рисунок 17.2 – Приоритет ToS

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

DSCP (Differentiated Services Code Point): коды разделенных сервисов, классификационная информация, передающаяся в заголовке IP-пакета третьего уровня, занимает 6 бит, имеет значение от 0 до 63 и обратно совместима с приоритетом IP.

MPLS TC(EXP) : Поле MPLS означает класс обслуживания, имеет 3 бита для диапазона от 0 до 7.



Рисунок 17.3

Internal Priority: Внутренний приоритет, устанавливаемый процессором коммутатора. Возможный диапазон значений зависит от типа процессора. Сокращенно Int-Prio или IntP.

Drop Precedence: Приоритет сброса. При обработке пакетов первыми сбрасываются пакеты с большим приоритетом сброса. Имеет значение 0 или 1. Сокращенно обозначается Drop-Prec или DP.

Classification: основное назначение механизма QoS, классифицирует передаваемые пакеты в соответствии с классификационной информацией, содержащейся в пакетах и списками контроля доступа (ACL).

Policing: действие механизма QoS на входе, которое устанавливает политики трафика и управляет классифицированными пакетами.

Remark: действие механизма QoS на входе, выполняющее пропуск, остановку или сброс пакета в соответствии с политиками трафика.

Scheduling: действие механизма QoS на выходе. Добавляет пакеты в соответствующие исходящие очереди основываясь на внутреннем приоритете. И принимает решение о посылке или сбросе пакетов в соответствии с приоритетом сброса, алгоритмом посылки и важностью соответствующей очереди в исходящем потоке.

In-Profile: Траффик в рамках политики QoS (полоса пропускания или дополнительной полосой) называется In-Profile.

Out-of-Profile: Траффик в рамках политики QoS (полосы пропускания или дополнительной полосы) называется Out-of-Profile.

4.1.1.2 Реализация QoS

Для выполнения на коммутаторе программного QoS необходимо рассмотреть основную базовую модель. QoS не создает новой полосы в канале, но может максимально подстраивать конфигурацию текущих канальных ресурсов. Полная реализация QoS дает возможность полностью управлять сетевым трафиком. Ниже, как можно точнее, описывается сам принцип QoS.

Спецификация передачи данных в IP покрывает только адресацию и сервисы источника и приемника, а также коррекцию передачи пакетов с помощью протоколов 4 уровня модели OSI и выше, таких как TCP. Однако, в большинстве случаев протокол IP использует максимально возможную пропускную способность вместо механизма поддержки и защиты полосы пакетной передачи. Это применимо для таких сервисов как почта и FTP, но при увеличении передачи мультимедийных коммерческих данных и электронных бизнес-сервисов, метод максимальной загрузки не может удовлетворить требования необходимой полосы и низких задержек.

Базируясь на различных методах, QoS определяет приоритет для каждого входящего пакета. Классификационная информация содержится в заголовках IP-пакетов третьего уровня и в заголовках фреймов 802.1Q второго уровня. QoS обеспечивает одинаковый сервис для пакетов одинакового приоритета, в то время как для пакетов с различающимися приоритетами предлагаются различающиеся операции. Маршрутизатор или коммутатор, поддерживающие сервис QoS, могут обеспечивать различную пропускную способность в соответствии с информацией о классификации, помечать трафик в соответствии с настроенной политикой, а также сбрасывать некоторые низкоприоритетные пакеты в случае нехватки полосы пропускания.

Конфигурация QoS является гибкой, более простой или сложной в зависимости от топологии сети и устройств, а также глубины анализа входящего/исходящего трафика.

4.1.1.3 Базовая модель QoS

Базовая модель QoS состоит из 4 частей: Классификация (Classification), Применение политик (Policing), Пометка (Remark) и Планирование (Scheduling), где классификация, применение политик и пометки – последовательные действия на входе, а работа с очередями и планирование – действия QoS на выходе.

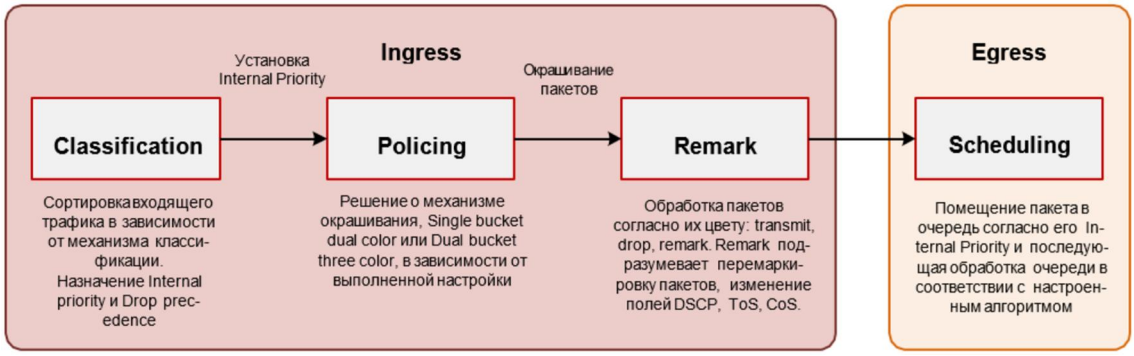


Рисунок 17.4 – Базовая модель QoS

Классификация (Classification): Классифицирует трафик в соответствии с классификационной информацией пакетов и генерирует значение внутреннего приоритета, основанное на классификационной информации. Для различных типов пакетов классификация обеспечивается различным образом. Схема ниже показывает это.

Применение политик (Policing) и пометка (Remark): Каждый пакет в классифицированном входящем трафике получает значение внутреннего приоритета и может далее подвергаться действию политик и помечаться.

Применение политик может быть выполнено на потоке данных для обеспечения различной полосы пропускания для различных классов трафика. Назначенная пропускная политика может быть «одна корзина-два цвета» (single bucket dual color) или «две корзины-три цвета» (dual bucket three color). Трафику присваиваются различные цвета и в соответствии с ними он может сбрасываться или пропускаться. К пропущенным пакетам применяется действие пометки, когда пакету назначается новый, более низкий внутренний приоритет для замены существовавшего ранее более высокого внутреннего приоритета. Поля COS и DSCP будут модифицированы в соответствии с новым внутренним приоритетом на выходе. Следующая схема описывает эти операции.

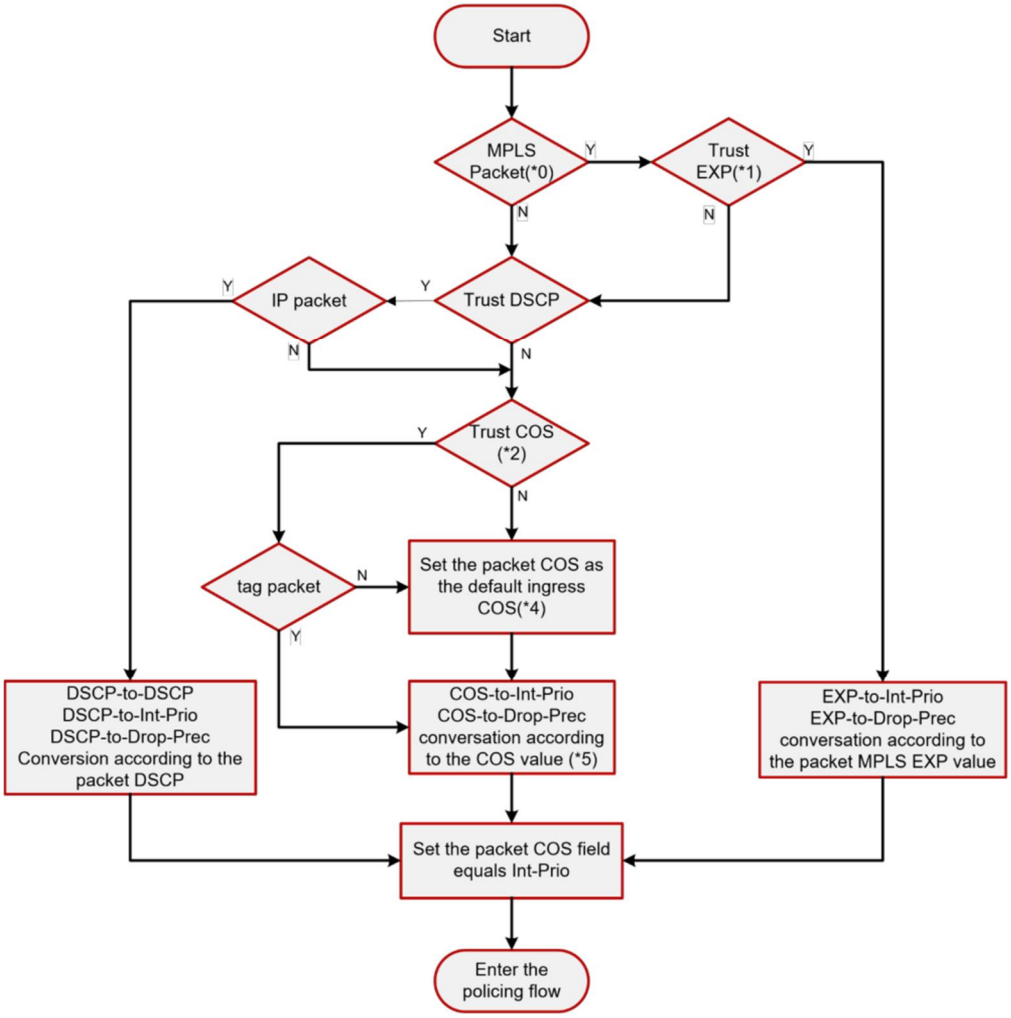


Рисунок 17.5 – Процесс классификации

Замечание 1: Значение CoS рассчитывается исходя из свойств пакета и никак не связано со значением внутреннего приоритета, полученным для потока.

Замечание 2: Если одновременно сконфигурированы проверка DSCP и CoS, то приоритет DSCP важнее COS.

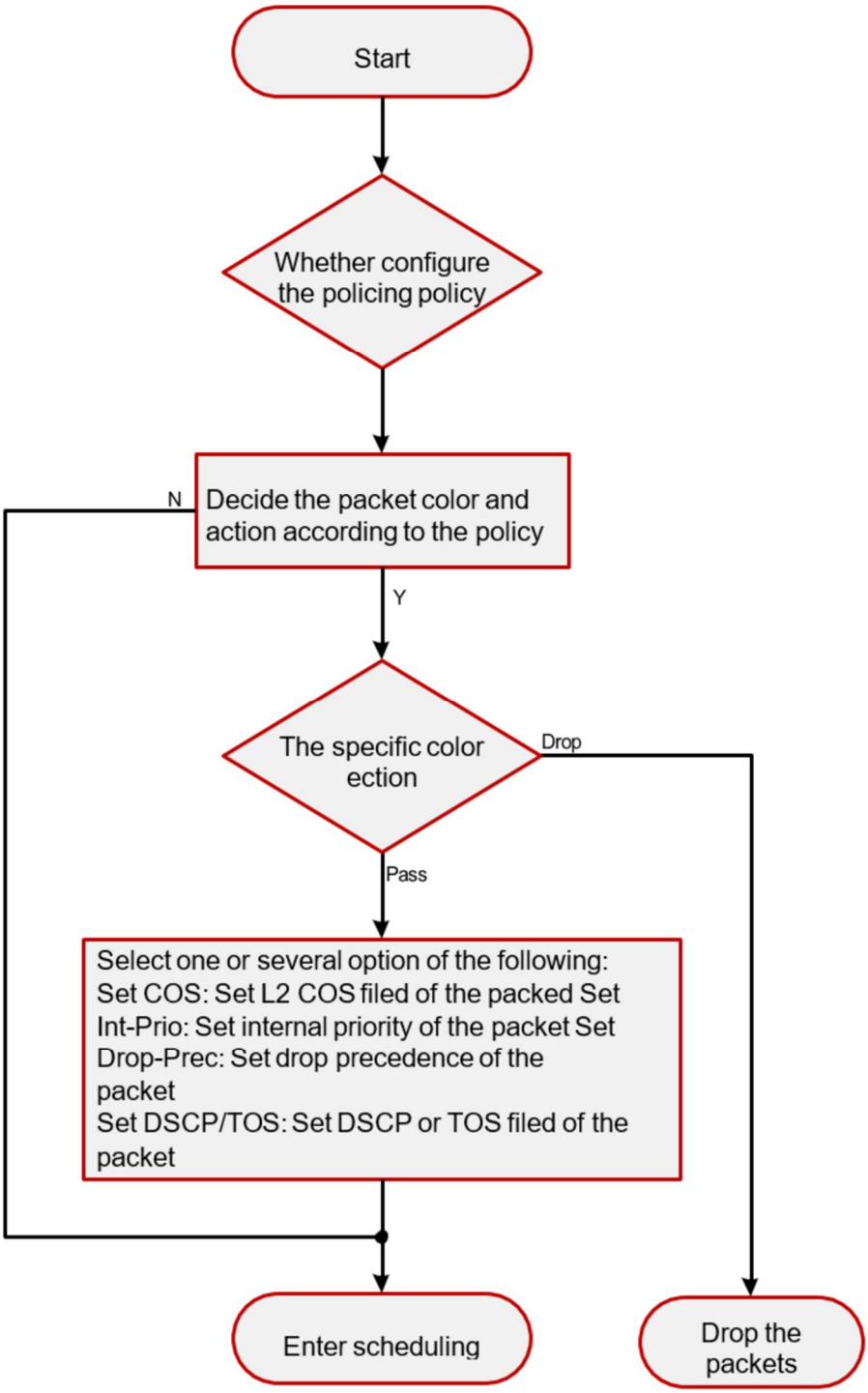


Рисунок 17.6 – Процессы Регулирования и пометки

Замечание 1. Внутренний приоритет будет скрыт после установки. Установка внутреннего приоритета на трафик с определенным цветом покрывает установку внутреннего приоритета на трафик, не связанный с цветом.

Замечание 2. Сброс внутреннего приоритета пакетов осуществляется в соответствии с картой преобразования «внутренний приоритет - внутренний приоритет» (IntP-to-IntP). При классификации потока внутренний приоритет берется от источника или устанавливается действиями, не связанными с цветом.

Работа с очередями и планирование: существует внутренний приоритет для исходящих пакетов, в соответствии с ним планируется распределение пакетов по

очередям с различным приоритетом и пакеты посылаются в соответствии с весовым приоритетом очереди и приоритетом сброса. Следующая схема описывает операции планирования.

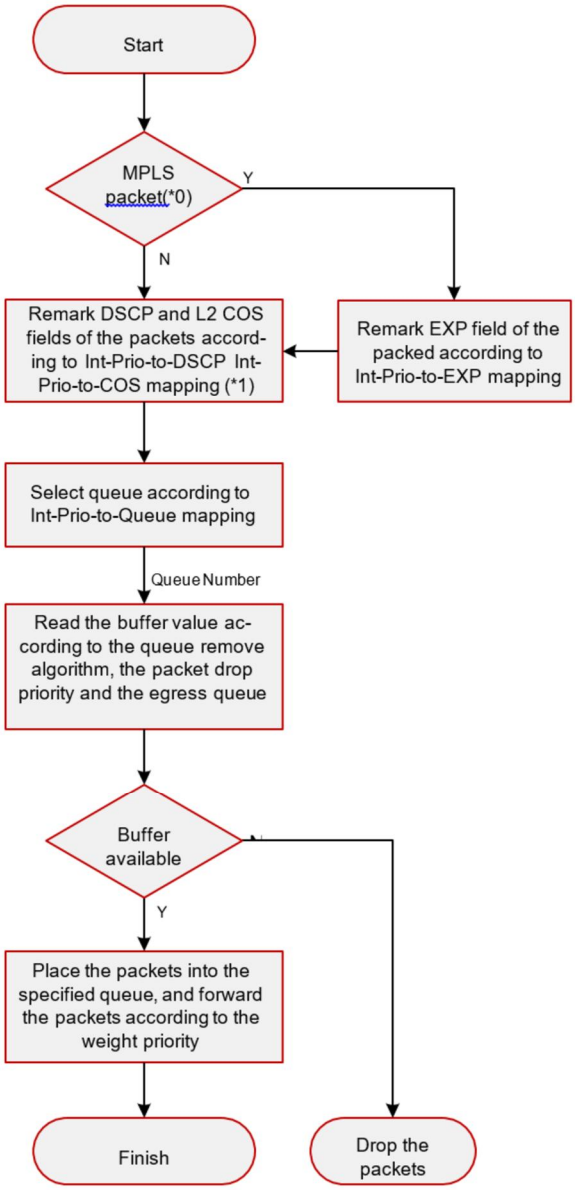


Рисунок 17.7 – Процессы планировки и управления очередями

4.1.2 Конфигурирование QoS

1. Конфигурирование карты классов (class map).

Устанавливает классификационные правила в соответствии с ACL, CoS, VLAN ID, приоритетом IPv4, DSCP и IPv6 FL для классификации потока данных. Различные классы потоков данных обрабатываются по разным политикам.

2. Конфигурирование карты политик (policy map).

После классификации потока данных может быть создана карта политик, для связи с картой классов, созданной ранее и входом в режим класса. Тогда различные политики (такие как ограничение полосы, понижение приоритета назначением нового значения DSCP) могут применяться для различных потоков данных. Также можно определить набор политик, которые могут применяться для нескольких классов в карте политик.

3. Применение QoS на порту или VLAN-интерфейсе.

Конфигурирование доверительного режима (trust mode) на порту или привязка политик к порту. Политики будут задействованы на порту только если они будут привязаны к нему. Политики так же могут быть привязаны к определенному VLAN. Не рекомендуется одновременно использовать карту политик на VLAN и на ее портах, в противном случае приоритет карты политик на порту будет выше.

4. Конфигурирование алгоритма управления очередями.

Конфигурирование алгоритма управления очередями, такого как sp, wdrr и других. Конфигурирование распределения QoS.

Конфигурирование распределения из CoS в DP, из DSCP в DSCP, из IntP в DSCP.

1. Конфигурирование карты классов.

Команда	Описание
Режим глобального конфигурирования	
class-map <class-map-name> no class-map <class-map-name>	Создание карты классов и вход в режим карты классов; команда «no class-map <class-map-name>» удаляет указанную карту классов.
match {access-group <acl-index-or-name> | ip dscp <dscp-list>| ip precedence <ip-precedencelist> | ipv6 access-group <acl-index- or-name> | ipv6 dscp <dscp-list>| ipv6 flowlabel <flowlabellist>|vlan <vlan-list> | cos <cos-list>} no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos}	Установка согласованных критериев (классификация потока данных по ACL, CoS, VLAN ID, приоритетом IPv4, IPv6 FL или DSCP, и т.д.) для карты классов; команда No удаляет определенный согласованный критерий.

2. Конфигурирование карты политик.

Команда	Описание
Режим глобального конфигурирования	
policy burst {1 | 2} <committed-burst-size>	Создание профиля ограничения всплесков траффика для последующей настройки policier.
policy-map <policy-map-name> no policy-map <policy-map-name>	Создание карты политик и вход в режим карты политик; команда NO удаляет определенную карту политик.
class <class-map-name> [insert-before <classmap-name>] no class <class-map-name>	После создания карты политик, ее можно связать с классом. Различные политики или новые значения DSCP могут быть применены к различным потокам данных в режиме классов; команда NO удаляет определенный класс.
set {ip dscp <new-dscp> | ip precedence	Присваивает новый внутренний приоритет классифицированному трафику; Команда NO отменяет назначение новой величины.

<newprecedence> | internal priority <new- inp> | drop precedence <new-dp>} no set {ip dscp | ip precedence | internal priority | drop precedence | internal-priority}	
policy <CIR_Kbits_per_second> burst- group <bucket_size_profile_ID> no policy	Конфигурация политики для классифицированного потока. Отдельные команды политик поддерживают три цвета. Анализирует рабочий режим виртуальной корзины, это может быть одна скорость – одна корзина, одна скорость – две корзины, две скорости – две корзины. Устанавливает соответствующие действия для различных цветов пакетов. Команда NO удаляет режим конфигурации.
accounting no accounting	Установка функции статистики для классифицированного трафика. После включения этой функции в режиме политики классов, добавляет статистику трафика по карте политики классов. В режиме одной корзины пакет может быть только зеленым или красным при применении политики. В выводимой информации будут два цвета (красный и зеленый) пакетов. В режиме двух корзин будут три цвета (зеленый, красный и желтый) пакетов.
Режим конфигурации карты политик классов	
drop no drop transmit no transmit	Сбрасывает или передает трафик в данном классе. Команда NO отменяет присвоенную функцию.

3. Применение QoS на порту или VLAN-интерфейсе.

Команда	Описание
Режим конфигурирования интерфейса	
mls qos trust dscp no mls qos trust dscp	Конфигурирование доверительного порта. Команда NO отменяет текущий режим доверительности на порту.
mls qos cos {<default-cos>} no mls qos cos	Конфигурация значения CoS по умолчанию на порту; команда NO восстанавливает значение по умолчанию.
service-policy input <policy-map-name> no service-policy input <policy-map-name>	Применяет карту политик к конкретному порту; Команда NO удаляет соответствующую карту политик, примененную на порту. Выходная карта политик пока не поддерживается.
Режим глобального конфигурирования	
service-policy input <policy-map-name> vlan <vlan-list>	Применяет карту политик к конкретному VLAN-интерфейсу. Команда NO удаляет соответствующую карту политик, примененную на VLAN-интерфейсе.

no service-policy input <policy-map-name> vlan <vlan-list>	

4. Конфигурирование алгоритма управления очередями.

Команда	Описание
Режим конфигурирования порта	
mls qos queue algorithm {sp | wrr | wdrr} no mls qos queue algorithm	Установка алгоритма управления очередями. По умолчанию алгоритм wdrr
Режим глобального конфигурирования	
mls qos queue {wrr | wdrr} weight <weight0..weight3> no mls qos queue weight	Устанавливает вес очередей wdrr для всех портов. По умолчанию веса очередей 1 2 3 4

5. Конфигурирование преобразования QoS.

Команда	Описание
Режим глобального конфигурирования	
mls qos map {cos-intp <intp1…intp8> | dscp-intp <in-dscp list> to <intp>} no mls qos map {cos-intp | dscp-intp}	Устанавливает приоритетную трансляцию для QoS. Команда NO восстанавливает значение трансляции по умолчанию

6. Очистка счетчиков данных в карте политик на определенном порту или VLAN’e.

Команда	Описание
Режим администратора	
clear mls qos statistics [interface <interface-name> | vlan <vlan-id>]	Очистка счетчиков данных в карте политик на определенном порту или VLAN’e. Если у команды нет параметров, очищаются счетчики у всех карт политик.

7. Просмотр конфигурации QoS.

Команда	Описание
Режим администратора	
show mls qos maps [cos-dp | dscp-dscp | dscpintp | dscp-dp | intp-dscp]	Показывает конфигурацию QoS трансляции
show class-map [<class-map-name>]	Показывает карту классов QoS
show policy-map [<policy-map-name>]	Показывает карту политик QoS.
show mls qos {interface [<interface-id>] [policy	Показывает конфигурацию QoS на порту.

| queuing] | vlan <vlan-id>}	

4.1.3 Пример QoS

Пример 1:

Необходимо включить функцию QoS, изменить веса выходных очередей на порту Ethernet 1/0/1 на 1:1:2:2:4:4:8:8, также установить на порту режим доверительного CoS без изменения значения DSCP и установить значение CoS по умолчанию равным 5.

Этапы конфигурирования описаны ниже:

```
rotek#config
rotek(config)# mls qos queue wrr weight 1 1 2 2 4 4 8 8
rotek(Config-If-Ethernet 1/0/1)#mls qos trust cos
rotek(Config-If-Ethernet1/0/1)#mls qos cos 5
```

Результат конфигурации:

Когда в общем режиме включен QoS, для выходных очередей полоса пропускания для каждого порта поделена в пропорции 1:1:2:2:4:4:8:8. Когда пакеты, имеющие параметр CoS, приходят через порт ethernet 1/0/1 им назначается внутренний приоритет в соответствии со значением CoS. Значения CoS от 1 до 7 соответствуют очередям 1,2,3,4,5,6,7,8 соответственно. Если входящий пакет не имеет установленного параметра CoS, он по умолчанию считается равным 5 и пакет помещается в очередь 6. Во всех проходящих пакетах значение DSCP не меняется.

Пример 2:

На порту Ethernet 1/0/2 необходимо установить полосу для пакетов из сегмента 192.168.1.0 в 10 Мбит/с с дополнительной полосой в 4 Мбит. Все пакеты, превышающие эту полосу, будут сброшены.

Этапы конфигурации показаны ниже:

```
rotek#config
rotek(config)#access-list 1 permit 192.168.1.0 0.0.0.255
rotek(config)#class-map c1
rotek(Config-ClassMap-c1)#match access-group 1
rotek(Config-ClassMap-c1)#exit
rotek(config)#policy burst 1 4000
rotek(config)#policy-map p1
rotek(Config-PolicyMap-p1)#class c1
rotek(Config-PolicyMap-p1-Class-c1)#policy 10000 burst-group 1
rotek(Config-PolicyMap-p1-Class-c1)#exit
rotek(Config-PolicyMap-p1)#exit
rotek(config)#interface ethernet 1/0/2
rotek(Config-If-Ethernet1/0/2)#service-policy input p1
```

Результат конфигурации:

Лист доступа с именем 1 настроен для выборки сегмента 192.168.1.0. Функция QoS включена глобально. Создана карта классов с именем c1, лист ACL 1 включен в карту классов. Создана группа burst 1 определяющая максимальный всплеск траффика, превышающего гарантированную полосу CIR. Создана другая карта политик с именем p1. Карта p1 ссылается на карту c1. Установлены соответствующие политики для ограничения полосы и дополнительных расширений. Эта карта политик применена на порту ethernet 1/0/2. После того, как вышеуказанные настройки сделаны, полоса для пакетов из сегмента 192.168.1.0, проходящих через порт Ethernet 1/0/2, установлена в 10 Мбит/с с дополнительным расширением в 4 Мбит. Все пакеты, превышающие данные установки в данном сегменте, будут отброшены.

Пример 3:

Как показано на рисунке, внутри отмеченной области, находится QoS домен, SwitchA классифицирует различный трафик и назначает различные приоритеты IP. Для примера, установим приоритет CoS для пакетов из сегмента 192.168.1.0 равным 5 на порту ethernet1/0/1 (установим внутренний приоритет равным 40 и по умолчанию трансляцию внутреннего приоритета в dcsp как 40-40, соответствующий IP приоритет равным 5). Порт, подключенный к SwitchB – транковый. На SwitchB порт Ethernet 1/0/1, подключенный к SwitchA настроен как доверительный dscp. Таким образом внутри области QoS пакеты с различными приоритетами будут распределяться в различные очереди и получать соответствующую полосу передачи.

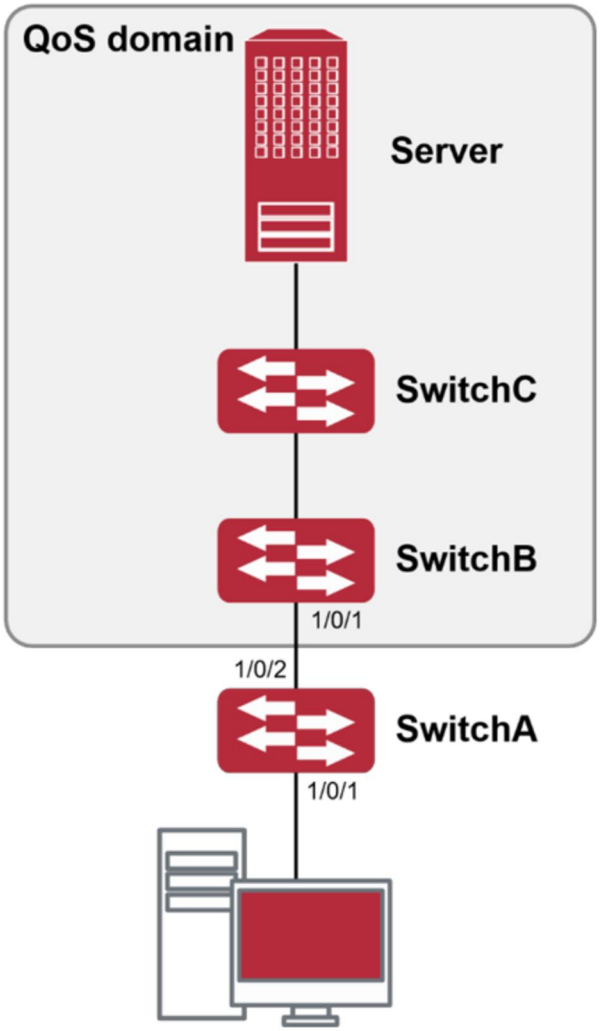


Рисунок 17.8 – Типовая топология QoS

Этапы конфигурации описаны ниже:

Конфигурация QoS на SwitchA:

```
rotek#config
rotek(config)#access-list 1 permit 192.168.1.0 0.0.0.255
rotek(config)#class-map c1
rotek(Config-ClassMap-c1)#match access-group 1
rotek(Config-ClassMap-c1)#exit rotek(config)#policy-map p1
rotek(Config-PolicyMap-p1)#class c1
rotek(Config-PolicyMap-p1-Class-c1)#set ip precedence 40
rotek(Config-PolicyMap-p1-Class-c1)#exit
rotek(Config-PolicyMap-p1)#exit
rotek(config)#interface ethernet 1/0/1
rotek(Config-If-Ethernet1/0/1)#service-policy input p1
```

Конфигурация QoS на SwitchB:

```
rotek#config
rotek(config)#interface ethernet 1/0/1
rotek(Config-If-Ethernet1/0/1)#mls qos trust cos
```

4.1.4 Устранение неисправностей QoS

- Доверительный режим cos и EXP может использоваться с другими доверительными режимами или картой политик.
- Доверительный режим dscp может использоваться с другими доверительными режимами или картой политик. Эта конфигурация применяется для пакетов IPv4 и IPv6.
- Доверительные режимы exp, dscp и cos могут быть сконфигурированы одновременно. Приоритеты по старшинству: EXP>DSCP>COS.
- Если сконфигурирован динамический VLAN (MAC VLAN/голосовой VLAN/VLAN подсети IP/VLAN-протокола), тогда значение COS для пакета равно значению COS для динамического VLAN.
- Карта политики (policy-map) может быть привязана только ко входящему направлению, выходящее направление не поддерживается.

В настоящее время не рекомендуется одновременно использовать карты политик (policy-map) на VLAN и на его порту.

5 МАРШРУТИЗАЦИЯ И ARP, ND

5.1 КОНФИГУРИРОВАНИЕ ФУНКЦИЙ 3-ГО УРОВНЯ

Коммутатор поддерживает только переадресацию на втором уровне, но имеет возможность настройки функций управления портом на третьем уровне для соединения всех видов протоколов управления на основе IP-протокола.

5.1.1 Интерфейс 3-го уровня

5.1.1.1 Общие сведения об интерфейсе управления 3-го уровня

В коммутаторах может быть создан интерфейс 3-го уровня. Он является не физическим интерфейсом, а виртуальным. Интерфейс 3-го уровня строится на интерфейсе VLAN. Интерфейс уровня 3 может содержать один или более интерфейсов уровня 2, принадлежащих одному и тому же VLAN, либо не содержать интерфейсов уровня 2. По крайней мере, один из интерфейсов уровня 2, содержащихся в интерфейсе уровня 3, должен быть включен (находиться в состоянии UP) – тогда будет включен и интерфейс уровня 3. В противном случае интерфейс уровня 3 будет выключен (будет находиться в состоянии DOWN). Коммутатор может использовать IP-адреса, установленные на интерфейсах 3-го уровня, для коммуникации с другими устройствами через IP-протокол. Коммутатор может пересылать IP-пакеты между разными интерфейсами 3-го уровня.

5.1.1.2 Настройка интерфейса 3-го уровня

Последовательность настройки интерфейса 3-го уровня:

1. Создание интерфейса 3-го уровня.
2. Настройка описания VLAN-интерфейса.

1. Создание интерфейса 3-го уровня.

Команда	Описание
Режим глобального конфигурирования	
interface vlan <vlan-id> no interface vlan <vlan-id>	Создание VLAN-интерфейса (VLAN-интерфейс – это интерфейс 3-го уровня); команда «no» удаляет VLAN-интерфейс, созданный на коммутаторе.

2. Настройка описания VLAN-интерфейса.

Команда	Описание
Режим конфигурирования VLAN-интерфейса	
description <text> no description	Настройка описания VLAN-интерфейса. Команда «no» уберет описание VLAN-интерфейса.

5.1.2 Настройка протокола IP

5.1.2.1 Введение в IPv4, IPv6

IPv4 – это текущая версия глобального универсального Интернет-протокола. Практика доказала, что IPv4 является простым, гибким, открытым, мощным, а также легким в реализации протоколом. Он обладает хорошей совместимостью с различными протоколами верхнего и нижнего уровней. Хотя IPv4 почти не менялся с момента его

появления в 1980-х годах, он продолжает распространяться по всему миру вместе с распространением Интернет. Однако по мере роста инфраструктуры Интернет и услуг, использующих Интернет-приложения, выявляются и некоторые недостатки протокола IPv4, связанные с масштабом и сложностью сегодняшнего Интернета.

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

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

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

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

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

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

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

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

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

Поддержка IPSec. IPSec обязателен в IPv6, в отличие от IPv4. IPv6 обеспечивает расширенный заголовок безопасности, который обеспечивает сервисы безопасности «из

конца в конец», такие как контроль доступа, конфиденциальность и целостность данных, следовательно, делает проще реализацию механизмов шифрования, проверки и виртуальных частных сетей (VPN).

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

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

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

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

5.1.2.2 Настройка IP протокола

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

5.1.2.2.1 Настройка адреса IPv4

1. Настройка IPv4-адрес интерфейса 3-го уровня.
2. Настройка шлюза по умолчанию.

1. Настройка IPv4-адрес интерфейса 3-го уровня.

Команда	Описание
Режим конфигурирования VLAN-интерфейса	
ip address <ip-address> <mask> [secondary] no ip address [<ip-address> <mask>]	Настройка IP-адреса VLAN-интерфейса; команда no ip address [<ip-address> <mask>] отменяет IP-адрес VLAN-интерфейса.

2. Настройка шлюза по умолчанию.

Команда	Описание
Глобальный режим конфигурирования	
ip route 0.0.0.0 0.0.0.0 <A.B.C.D> no ip route 0.0.0.0 0.0.0.0 <A.B.C.D>	Настройка статической маршрутизации. Команда no отменяет настройку.

5.1.3 ARP

5.1.3.1 Введение в ARP

ARP (Address Resolution Protocol – протокол определения адреса) в основном используется для определения Ethernet MAC-адреса по IP-адресу. Коммутатор поддерживает статическое добавление записей в ARP-таблицу.

5.1.3.2 Список задач конфигурации ARP

Список задач конфигурации ARP:

1. Настроить статический ARP

Команда	Описание
Режим VLAN-интерфейса	
arp <ip_address> <mac_address> {interface [ethernet] <portName>} no arp <ip_address>	Настраивает статическую запись ARP; команда no удаляет запись ARP указанного IP-адреса.

5.1.3.3 Поиск неисправностей ARP

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

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

5.2 НАСТРОЙКА ФУНКЦИИ ПРЕДОТВРАЩЕНИЯ ARP-СКАНИРОВАНИЯ

5.2.1 Введение в функцию предотвращения ARP-сканирования

ARP-сканирование – это обычный способ сетевой атаки. Для того, чтобы обнаружить все активные хосты в сегменте сети, источник атаки будет рассылать большое количество ARP-сообщений, что будет занимать большую часть пропускной способности сети. Возможна атака большим количеством трафика используя поддельные ARP-сообщения, что приведет к коллапсу сети из-за исчерпания пропускной способности. Обычно ARP-сканирование – это просто предпосылка к другой, более опасной атаке, такой, как автоматическое заражение вирусом или последующее сканирование портов, сканирование уязвимостей, нацеленное на хищение информации, атака искаженными сообщениями, DOS-атака и т.д.

Поскольку ARP-сканирование угрожает безопасности и стабильности сети, очень важно его предотвратить. Коммутатор обеспечивает полное решение для предотвращения ARP-сканирования: если в сегменте найден хост или порт с признаками ARP-сканирования, коммутатор отрежет источник атаки для обеспечения безопасности сети.

Есть два метода предотвращения ARP-сканирования: на основе порта и на основе IP. Метод на основе порта считает количество ARP-сообщений, полученных с порта за определенный период, если число превышает заданный порог, порт будет выключен. Метод на основе IP считает количество ARP-сообщений, полученных от IP-адреса в сегменте за определенный период, если число превышает заданный порог, любой трафик от этого IP будет заблокирован до тех пор, пока порт, связанный с IP-адресом, не будет погашен. Эти два метода могут быть включены одновременно. После того, как порт или IP-адрес были заблокированы, пользователь может восстановить их статус используя функцию автоматического восстановления.

Чтобы повысить эффективность, пользователи могут настроить доверенные порты и IP-адреса, ARP-сообщения от которых не будут проверяться коммутатором. Таким образом нагрузка на коммутатор может быть значительно снижена.

5.3 КОНФИГУРАЦИЯ ЗАЩИТЫ ОТ ПОДМЕНЫ ARP (ARP Spoofing)

5.3.1 Обзор

5.3.1.1 ARP (Address Resolution Protocol)

В общем, протокол ARP (RFC-826), в основном, отвечает за сопоставление IP-адреса с соответствующим 48-битному физическому адресу (MAC-адресу), например, IP-адрес 192.168.0.1, MAC-адрес сетевой карты 70:B3:D5:62:C0:63.

Весь процесс сопоставления состоит в том, что хост отправляет широковещательный (broadcast) пакет данных, включающий в себя информацию об IP-адресе хоста назначения (ARP-запрос), затем хост назначения отправляет исходному хосту пакет данных, включающий в себя информацию об IP-адресе и MAC-адресе. Таким образом, два хоста могут обмениваться информацией по MAC-адресу.

5.3.1.2 Подмена ARP

Чтобы уменьшить ARP-трафик в сети, если хост получит ARP-ответ, который он не запрашивал, он, в соответствии с протоколом ARP, так же добавит запись в свой ARP-кэш, что делает возможным подмену ARP (ARP spoofing). Если хакер хочет прослушать обмен данными между двумя хостами в одной сети (даже если они подключены через коммутаторы), он отправляет пакет ARP-ответа двум хостам по отдельности, это приводит к тому, что каждый из хостов считает MAC-адрес хакера адресом другого хоста. Таким образом, вместо прямого обмена, хосты обмениваются трафиком через хост хакера. Хакеры могут не только получать необходимую им информацию, но и модифицировать пакеты данных на свое усмотрение для последующей передачи. В связи с этим на компьютере хакера не нужно настраивать смешанный режим сетевой карты, т.к. пакеты данных поступают на компьютер хакера на физическом уровне, компьютер работает как ретранслятор.

5.3.1.3 Как предотвратить подмену ARP

Есть много видов атак, основанных на протоколе ARP. Большинство атак основаны на подмене ARP, так что очень важно предотвратить подмену ARP.

Механизм подмены ARP проникает в сеть, в первую очередь, путем подделки легального IP-адреса и последующей посылки большого количества поддельных ARP-пакетов коммутаторам, после чего коммутаторы заменяют правильные связки IP-MAC соответствующими связками из атакующих пакетов. Таким образом, коммутатор ошибочно отправляет пакеты атакующему хосту, и это действует на всей сети.

Основным методом предотвращения атак и подмены ARP на коммутаторах является отключение на коммутаторе функции автоматического обновления ARP. Злоумышленник не сможет изменить правильные связки IP-MAC на коммутаторе, тем самым предотвращается неправильная пересылка пакетов. В то же время это не прерывает функцию автоматического обучения ARP. Таким образом, это значительно предотвращает подмену ARP.

ND – протокол обнаружения соседей в IPv6, аналогичный протоколу ARP по принципу действия. Для предотвращения подмены ND используется механизм, аналогичный применяемому для ARP.

5.3.2 Конфигурация предотвращения подмены ARP

Последовательность настройки предотвращения подмены ARP:

1. Отключить функцию автоматического обновления ARP.
2. Отключить функцию автоматического обучения ARP.
3. Поменять динамические ARP на статические.

1. Отключить функцию автоматического обновления ARP.

Команда	Описание
Общий режим и Режим порта	
ip arp-security updateprotect no ip arp-security updateprotect	Отключить/включить функцию автоматического обновления ARP.

2. Отключить функцию автоматического обучения ARP, ND.

Команда	Описание
Общий режим и Режим интерфейса	
ip arp-security learnprotect no ip arp-security learnprotect	Отключить/включить функцию автоматического обучения ARP.

3. Поменять динамические ARP, ND на статические

Команда	Описание
Общий режим и Режим порта	
ip arp-security convert	Поменять динамические ARP на статические.

5.3.3 Пример предотвращения подмены ARP, ND

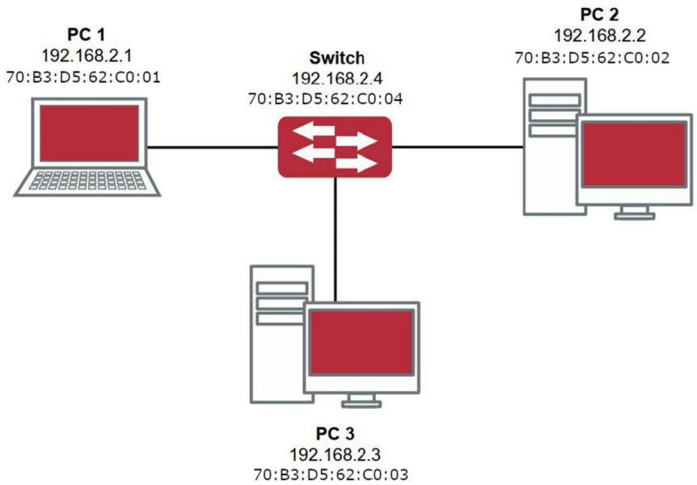


Рисунок 20.1 – Пример схемы подключения оборудования для проверки функции предотвращения подмены ARP

Описание оборудования

Оборудование	Конфигурация	Кол-во
Switch	IP:192.168.2.4;mac: 70-B3-D5-62-C0-04	1
PC 1	IP:192.168.2.1;mac: 70-B3-D5-62-C0-01	1
PC 2	IP:192.168.1.2;mac: 70-B3-D5-62-C0-02	1
PC 3	IP:192.168.2.3;mac: 70-B3-D5-62-C0-03	несколько

На диаграмме показана нормальная связь между PC 2 и PC 3. PC 1 хочет, чтобы коммутатор направлял ему пакеты, отправленные хостом PC 2. В первую очередь PC 1 отправляет пакет ARP-ответа на коммутатор в формате: 192.168.2.3, 70-B3-D5-62- C0-01, сопоставляя его MAC-адрес с IP-адресом хоста C, коммутатор обновляет ARP- список и начинает отправлять пакеты для 192.168.2.3 на MAC-адрес 70-B3-D5-62-C0-01 address (адрес хоста PC 1).

В дальнейшем хост PC 1 пересылает принятые пакеты хосту PC 3, меняя адрес источника и адрес назначения. Так как ARP-список своевременно обновляется, еще одной задачей для хоста A является непрерывная отправка ARP-ответов и обновление ARP-списка коммутатора.

Поэтому очень важно защитить ARP-список, настроить запрещение ARP-обучения в стабильной среде и затем изменить все динамические ARP-записи на статические. Выученные ARP не будут обновляться и будут защищены.

> *rotek#config rotek(config)#interface vlan 1*
> *rotek(Config-If-Vlan1)#arp 192.168.2.1 70-B3-D5-62-C0-01 interface eth 1/0/2*
> *rotek(Config-If-Vlan1)#interface vlan 2*
> *rotek(Config-If-Vlan2)#arp 192.168.1.2 70-B3-D5-62-C0-02 interface eth 1/0/2*
> *rotek(Config-If-Vlan2#interface vlan 3*
> *rotek(Config-If-Vlan3)#arp 192.168.2.3 70-B3-D5-62-C0-03 interface eth 1/0/2*
> *rotek(Config-If-Vlan3)#exit*
> *rotek(Config)#ip arp-security learnprotect*
> *rotek(Config)#*
> *rotek(config)#ip arp-security convert*

Если конфигурация внешнего оборудования меняется, это позволяет запретить ARP-обновления. Как только параметр ARP будетзафиксирован, он не может быть обновлен новым ARP-ответом, данные будут защищены от перехвата.

> *rotek#config*
> *rotek(config)#ip arp-security updateprotect*

5.4 НАСТРОЙКА DYNAMIC ARP INSPECTION (DAI)

5.4.1 Введение в ARP INSPECTION

Функция динамического контроля *ARP (Dynamic ARP Inspection)* - это функция безопасности, которая позволяет проверять пакеты ARP в сети. Через DAI администратор может перехватывать, записывать и отбрасывать пакеты ARP, которые имеют неверный MAC-адрес или IP-адрес. DAI позволяет проверить легитимность пакетов ARP в соответствии с легитимными IP и MAC-адресами, содержащимися в доверенной базе данных. Эта база может быть создана динамически, с помощью мониторинга DHCP. Если пакет ARP получен из доверенного для DAI порта, коммутатор пересылает его напрямую, без проверки. Если пакет ARP получен из порта, который не является доверенным, коммутатор передаст только легитимный пакет, нелегитимные пакеты коммутатор будет отбрасывать и фиксировать это действие в системном журнале.

5.4.2 Настройка Dynamic ARP inspection

1. Включить DAI на VLAN

2. Задать доверенный порт
3. Настроить допустимую скорость ARP с портов

1. Включить ARP inspection на VLAN

Команда	Описание
Режим глобальной конфигурации	
ip arp inspection vlan <vlan-id> no ip arp inspection vlan <vlan-id>	Включить ARP inspection на основе VLAN <vlan-id> Команда no отключает функцию

2. Задать доверенный порт

Команда	Описание
Режим конфигурации порта	
ip arp inspection trust no ip arp inspection trust	Настроить порт как доверенный порт для DAI Настроить порт как недоверенный порт для DAI (значение по умолчанию)

3. Настроить допустимую скорость ARP с портов

Команда	Описание
Режим конфигурации порта	
ip arp inspection limit-rate <rate> no ip arp inspection limit-rate <rate>	Настроить лимит ARP-сообщений в секунду для порта. События нарушения фиксируются в системном журнале. Удалить лимит ARP-сообщений (по умолчанию)

6 КОНФИГУРАЦИЯ DHCP

6.1 КОНФИГУРАЦИЯ DHCP

6.1.1 Введение DHCP

DHCP [RFC2131] (Dynamic Host Configuration Protocol –протокол динамической настройки хостов) – это протокол, который динамически назначает IP-адрес из пула адресов, так же устанавливает другие сетевые параметры, такие как шлюз по умолчанию, DNS-сервер и расположение в сети файла образа. DHCP – это расширенная версия BOOTP. Это основная технология, которая не только может обеспечить загрузочной информацией бездисковые рабочие станции, но также может освободить администраторов от ручного ведения IP-адресного пространства и упростить пользователям процесс настройки. Еще одно преимущество DHCP в том, что он может снизить требования к количеству IP-адресов, когда пользователь надолго покидает сеть, его IP может быть назначен другому.

DHCP является протоколом типа «клиент-сервер», DHCP-клиент запрашивает у DHCP-сервера сетевой адрес и параметры конфигурации, сервер предоставляет клиенту сетевой адрес и параметры конфигурации. Если клиент и сервер находятся в разных подсетях, необходимо использовать DHCP ретранслятор (relay) для передачи DHCP-пакетов между клиентом и сервером. Реализация DHCP представлена ниже:

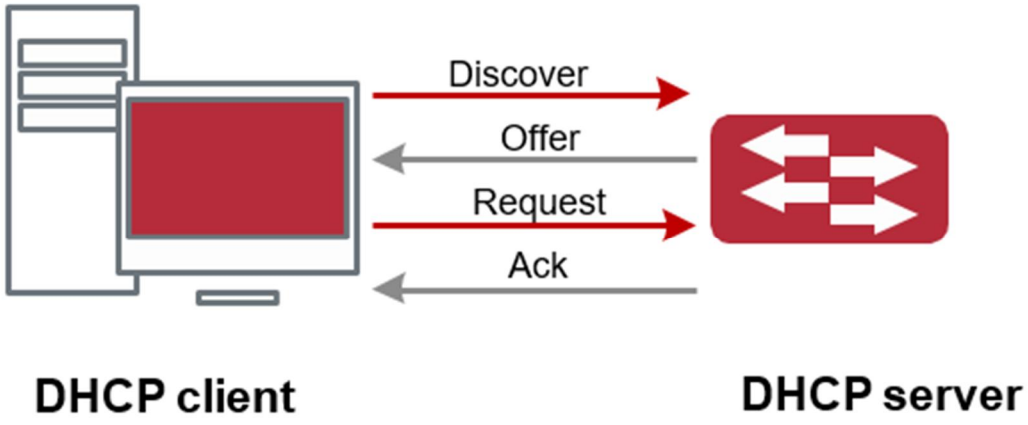


Рисунок 22.1 – Взаимодействия протокола DHCP

Разъяснение:

1. DHCP-клиент рассылает в локальную подсеть широковещательные пакты DHCPDISCOVER.
2. DHCP-сервер при получении пакета DHCPDISCOVER отправляет DHCP-клиенту пакет DHCPOFFER вместе с IP-адресами и другими сетевыми параметрами.
3. DHCP-клиент шлет широковещательный пакет DHCPREQUEST с информацией о DHCP-сервере, который он выбрал из DHCPOFFER-пакетов.
4. Выбранный клиентом DHCP-сервер отправляет пакет DHCPACK и клиент получает IP-адрес и другие параметры.

Эти четыре шага производят процесс динамической настройки хоста.

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

Коммутатор может работать и как DHCP-сервер, и как DHCP-ретранслятор. DHCP поддерживает не только динамическое назначение IP-адресов, но также ручную привязку адреса (например, указать определенный IP-адрес для определенного MAC-адреса или определенного ID устройства). Различия между динамическим и статическим назначением адресов: 1) динамически получаемый адрес может быть каждый раз разным; привязанный вручную адрес всегда будет одинаковый. 2) Время аренды IP-адреса, полученного динамически, одинаково для всего адресного пула, и оно ограничено. Время аренды IP-адреса, привязанного вручную, теоретически бесконечно. 3) Динамически выделяемые адреса не могут быть привязаны вручную. 4) Пул динамических адресов может наследовать параметры конфигурации сети пула динамических адресов, относящегося к сегменту.

6.1.2 Конфигурация DHCP-сервера

1. Включить/выключить сервис DHCP.
2. Настроить адресный пул DHCP.
    - Создать/удалить адресный пул DHCP.
    - Настроить параметры адресного пула DHCP.
    - Настроить параметры ручного адресного пула DHCP.

1. Включить/выключить сервис DHCP.

Команда	Описание
Общий режим	
service dhcp no service dhcp	Включить/выключить сервис DHCP.
Режим конфигурирования порта	
ip dhcp disbale no ip dhcp disable	Отключение не порте DHCP-обслуживания, команда no отменяет отключение.

2. Настроить адресный пул DHCP.

2.1 Создать/удалить адресный пул DHCP.

Команда	Описание
Общий режим	
ip dhcp pool <name> no ip dhcp pool <name>	Настроить адресный пул DHCP. Команда no отменяет пул адресов DHCP.

2.2 Настроить параметры адресного пула DHCP.

Команда	Описание
Режим адресного пула DHCP	
network-address <network-number> [mask | prefixlength] no network-address	Настройка области адресов, которые могут быть выделены адресному пулу. Команда no

	отменяет выделение адресного пула.
default-router [<addresSwitchA>[<addresSwitchB>[…<address8>]]] no default-router	Настройка шлюза по умолчанию для DHCP-клиентов. Команда no отменяет шлюз по умолчанию.
dns-server [<addresSwitchA>[<addresSwitchB>[…<address8>]]] no dns-server	Настройка DNS-сервера для DHCP-клиентов. Команда no отменяет настройку DNS-сервера.
domain-name <domain> no domain-name	Настройка доменного имени для DHCP-клиентов. Команда no отменяет доменное имя.
netbios-name-server [<addresSwitchA>[<addresSwitchB>[…<address8>]]] no netbios-name-server	Настройка адреса WINS-сервера. Команда no отменяет настройку.
netbios-node-type {b-node|h-node|m- node|pnode|<type-number>} no netbios-node-type	Настройка типа узла для DHCP-клиентов. Команда no отменяет тип узла.
bootfile <filename> no bootfile	Настройка загрузочного файла для DHCP-клиентов. Команда no отменяет загрузочный файл.
next-server [<addresSwitchA>[<addresSwitchB>[…<address8>]]] no next-server [<addresSwitchA>[<addresSwitchB>[…<address8>]]]	Настройка адреса сервера, размещающего загрузочный файл. Команда no отменяет удаляет адрес сервера.
option <code> {ascii <string> | hex <hex> | ipaddress <ipaddress>} no option <code>	Настройка сетевого параметра, определенного кодом опции. Команда no удаляет сетевой параметр.
lease {days [hours][minutes] | infinite} no lease	Настройка времени аренды адресов пула. Команда no удаляет настройку времени аренды.
max-lease-time {[<days>] [<hours>] [<minutes>] | infinite} no max-lease-time	Настройка максимального времени аренды адресов в адресном пуле, команда no восстанавливает настройки по умолчанию.
Общий режим	
ip dhcp excluded-address <low-address> [<highaddress>] no ip dhcp excluded-address <low-address> [<highaddress>]	Исключение из адресного пула адресов, которые не предназначены для динамического выделения.

2.3 Настроить параметры ручного адресного пула DHCP.

Команда	Описание
Режим адресного пула DHCP	

hardware-address <hardware-address> [{Ethernet | IEEE802|<type-number>}] no hardware-address	Задать/удалить аппаратный адрес, при ручном назначении адреса.
host <address> [<mask> | <prefix-length>] no host	Задать/удалить IP-адрес, который будет назначен заданному клиенту.
client-identifier <unique-identifier> no client-identifier	Задать/удалить уникальный ID пользователя.

6.1.3 Примеры конфигурации DHCP

Сценарий 1:

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

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

В расположении A машине с MAC-адресом 70-B3-D5-62-C0-AB назначен фиксированный IP-адрес 10.16.1.210 и имя хоста «management».

```
rotek(config)#service dhcp
rotek(config)#interface vlan 1
rotek(Config-Vlan-1)#ip address 10.16.1.2 255.255.0.0
rotek(Config-Vlan-1)#exit
rotek(config)#ip dhcp pool A
rotek(dhcp-A-config)#network 10.16.1.0 24
rotek(dhcp-A-config)#lease 3
rotek(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201
rotek(dhcp-A-config)#dns-server 10.16.1.202
rotek(dhcp-A-config)#netbios-name-server 10.16.1.209
rotek(dhcp-A-config)#netbios-node-type H-node
rotek(dhcp-A-config)#exit
rotek(config)#ip dhcp excluded-address 10.16.1.200 10.16.1.201
rotek(config)#ip dhcp pool B
rotek(dhcp-B-config)#network 10.16.2.0 24
rotek(dhcp-B-config)#lease 1
rotek(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201
rotek(dhcp-B-config)#dns-server 10.16.2.202
rotek(dhcp-B-config)#option 72 ip 10.16.2.209
rotek(dhcp-config)#exit
rotek(config)#ip dhcp excluded-address 10.16.2.200 10.16.2.201
rotek(config)#ip dhcp pool A1
```

rotek(dhcp-A1-config)#host 10.16.1.210
rotek(dhcp-A1-config)#hardware-address 70:B3:D5:62:C0:AB
rotek(dhcp-A1-config)#exit

Руководство по использованию: Когда DHCP/BOOTP-клиент подключается к VLAN1 порту коммутатора, клиент может получить адрес только из сети 10.16.1.0/24 вместо 10.16.2.0/24. Это потому, что широковещательный пакет от клиента будет запрашивать IP-адрес в том же сегменте VLAN-интерфейса, а IP-адрес VLAN-интерфейса - 10.16.1.2/24, поэтому адрес, назначаемый клиенту, будет принадлежать сети 10.16.1.0/24.

Если DHCP/BOOTP-клиент хочет получить адрес в сети 10.16.2.0/24, шлюз, пересылающий широковещательные пакеты клиента, должен принадлежать сети 10.16.2.0/24. Чтобы клиент получил адрес из пула 10.16.2.0/24, должна быть обеспечена связность между клиентским шлюзом и коммутатором.

6.1.4 Поиск неисправностей DHCP

Если DHCP-клиенты не получают IP-адреса и другие параметры сети, после проверки кабелей и клиентского оборудования, следует выполнить следующее:

- Проверьте, запущен ли DHCP-сервер, запустите его, если он не запущен.
- Если DHCP клиент и DHCP сервер находятся не в одной сети и не имеют прямой связности на втором уровне – проверьте, настроена ли на промежуточном маршрутизаторе/коммутаторе, отвечающем за пересылку пакетов, функция DHCP-relay. Если на промежуточном маршрутизаторе/коммутаторе нет функции DHCP-ретранслятора, рекомендуется заменить его или обновить ПО (если обновленная версия ПО поддерживает необходимый функционал).
- Проверьте DHCP-сервер на предмет наличия адресного пула в том же сегменте, что и VLAN коммутатора, если такой пул не существует, его необходимо добавить.
- Адресный пул может быть либо динамическим (команда «network-address»), либо статическим (команда «host»). Например, если к пулу применены команды «network-address» и «host», только одна из них вступит в силу. Кроме того, в ручной привязке только одна привязка IP-MAC может быть настроена в каждом пуле. Если необходимо несколько привязок, нужно создать отдельный адресный пул для каждой из них. Новая конфигурация в пуле с уже имеющейся привязкой перезапишет старую.

6.2 КОНФИГУРАЦИЯ ОПЦИИ 82 DHCP

6.2.1 Введение в опцию 82 DHCP

Опция 82 DHCP это опция информации ретранслирующего агента (Relay Agent). Опция 82 используется для того, чтобы проинформировать DHCP-сервер о том, от какого DHCP-ретранслятора и через какой его порт был получен запрос. Опция 82 DHCP направлена на укрепление безопасности серверов DHCP и улучшения политики конфигурации IP-адресов. Ретранслирующий агент добавляет опцию 82 (включающую физический порт доступа клиента, идентификатор устройства доступа и другую информацию) в DHCP-запрос, полученный от клиента, затем пересылает его DHCP-серверу. Когда DHCP-сервер, который поддерживает функцию опции 82, получает сообщение, он выделяет клиенту IP-адрес и другие параметры в соответствии с преднастроенными политиками и информацией в опции 82. В то же время DHCP-сервер может идентифицировать все возможные атаки DHCP-сообщениями в соответствии с информацией в опции 82 и защитить от них. DHCP-ретранслирующий агент снимет опцию 82 с ответного сообщения и передаст его определенному порту устройства доступа, в соответствии с информацией о физическом порте в опции. Применение опции 82 DHCP прозрачно для клиента.

6.2.1.1 Структура сообщения опции 82 DHCP

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

Code	Length	Agent Information Field			
82	N	Sub Option 1	Sub Option 2	Sub Option 3	Sub Option M

Code: представляет порядковый номер опции информации ретранслирующего агента, опция 82 называется так потому, что RFC3046 определяет ее как 82.

Len: количество байт в поле информации агента, не включая два байта в сегменте Code и сегменте Len.

Опция 82 может иметь несколько суб-опций, требуется как минимум одна субопция. RFC3046 определяет следующие две суб-опции, формат которых показан ниже:

SubOpt	Length	Sub-option Value				
1	N	s 1	s 2	s 3		s M
2	N	i 1	i 2	i 3		i M

SubOpt: порядковый номер суб-опции, порядковый номер суб-опции Circuit-ID – 1, порядковый номер суб-опции Remote ID – 2.

Len: количество байт в суб-опции, не включая два байта в сегменте SubOpt и сегменте Len.

6.2.1.2 Механизм работы опции 82

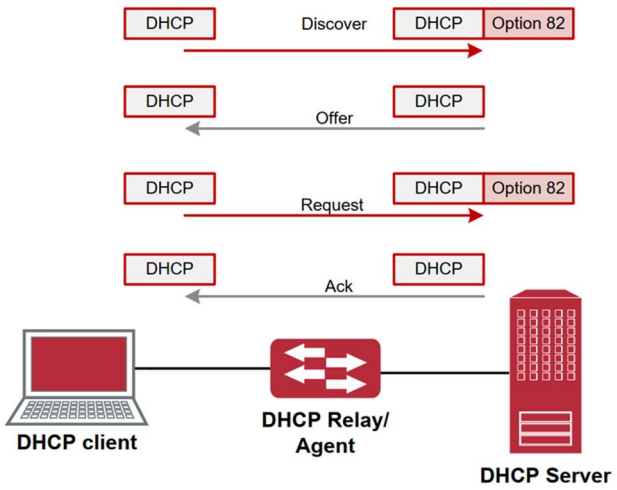


Рисунок 23.1 – Диаграмма потоков опции 82 DHCP

Если DHCP-ретранслирующий агент поддерживает опцию 82, DHCP-клиент должен пройти следующие четыре шага, чтобы получить IP-адрес от DHCP-сервера: discover, offer, select и acknowledge. Протокол DHCP следует приведенной ниже процедуре:

1. DHCP-клиент при инициализации посылает широковещательное сообщение запроса. Это сообщение не имеет опции 82.
2. DHCP-ретранслирующий агент добавит опцию 82 к сообщению запроса, которое он получит, затем перешлет это сообщение DHCP-серверу. По умолчанию суб-опция 1 опции 82 (Circuit ID) это информация об интерфейсе, к которому подключен DHCP-клиент (VLAN и физической порт), но пользователь может настроить Circuit ID по своему усмотрению. Суб-опция 2 опции 82 (Remote ID) это MAC-адрес устройства DHCP-ретранслятора.

3. После получения DHCP-запроса DHCP-сервер выделит клиенту IP-адрес и другую информацию, в соответствии с преднастроенными политиками и информацией в опции 82. Затем он направит DHCP-ретранслирующему агенту ответное сообщение с DHCP конфигурацией и опцией 82.
4. DHCP-ретранслирующий агент очистит ответное сообщение от опции 82 и направит его клиенту.

6.2.2 Конфигурирование опции 82 DHCP

1. Включить опцию 82 DHCP-ретранслирующего агента.
2. Настроить атрибуты интерфейса опции 82 DHCP.
3. Включить опцию 82 DHCP-сервера.
4. Настроить формат по умолчанию опции 82 DHCP-ретранслирующего агента.
5. Настроить разделитель.
6. Настроить метод создания опции 82.

1. Включить опцию 82 DHCP-ретранслирующего агента.

Команда	Описание
Общий режим	
ip dhcp relay information option no ip dhcp relay information option	Включает функции опции 82 на ретранслирующем агенте коммутатора. Команда no выключает функцию.

2. Настроить атрибуты интерфейса опции 82 DHCP.

Команда	Описание
Режим конфигурации интерфейса	
ip dhcp relay information policy {drop | keep | replace} no ip dhcp relay information policy	Устанавливает политики ретрансляции сообщения, которое уже содержит опцию 82. Режим drop означает, что сообщение, содержащее опцию 82, будет отброшено без какой-либо обработки. Режим keep означает, что система оставит оригинальную опцию 82 и передаст сообщение серверу. Режим replace означает, что система заменит существующую опцию 82 своей и передаст сообщение серверу. Команда no установит политику в режим по умолчанию – replace.
Ip dhcp relay information option subscriberid {standard | <circuit- id>} no ip dhcp relay information option subscriber-id	Устанавливает формат суб-опции 1 опции 82 (Circuit ID), standard означает стандартные названия VLAN и физического порта, например, «Vlan2+Ethernet1/0//12», <circuit-id> это содержание circuit-id, заданного пользователем (строка не более 64 символов). Команда no установит стандартный формат.
Общий режим	

ip dhcp relay information option remote-id {standard | <remote- id>} no ip dhcp relay information option remoteid	Устанавливает формат суб-опции 1 опции 82 (Remote ID). Команда no установит стандартный формат.

3. Включить опцию 82 DHCP-сервера.

Команда	Описание
Общий режим	
ip dhcp server relay information enable no ip dhcp server relay information enable	Позволяет DHCP-серверу коммутатора идентифицировать опцию 82. Команда no отключает эту функцию.

4. Настроить формат по умолчанию опции 82 DHCP-ретранслирующего агента.

Команда	Описание
Общий режим	
ip dhcp relay information option subscriberid format {hex | acsii | vs-hp}	Устанавливает формат subscriber-id опции 82 ретранслирующего агента.
ip dhcp relay information option remote-id format {default | vs-hp}	Устанавливает формат remote-id опции 82 ретранслирующего агента.

5. Настроить разделитель.

Команда	Описание
Общий режим	
ip dhcp relay information option delimiter [colon | dot | slash | space] no ip dhcp relay information option delimiter	Настраивает разделитель каждого параметра субопций в опции 82 в глобальном режиме. Команда no восстанавливает разделитель по умолчанию – slash.

6. Настроить метод создания опции 82.

Команда	Описание
Общий режим	
ip dhcp relay information option self-defined remote-id {hostname | mac | string WORD} no ip dhcp relay information option self- defined remote-id	Устанавливает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции remote- id.
ip dhcp relay information option selfdefined remote-id format [ascii | hex]	Устанавливает пользовательский формат remote-id для опции 82.

ip dhcp relay information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD} no ip dhcp relay information option self- defined subscriber-id	Устанавливает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции circuit -id.
ip dhcp relay information option selfdefined subscriber-id format [ascii | hex]	Устанавливает пользовательский формат circuit -id для опции 82.

6.2.3 Примеры применения опции 82 DHCP

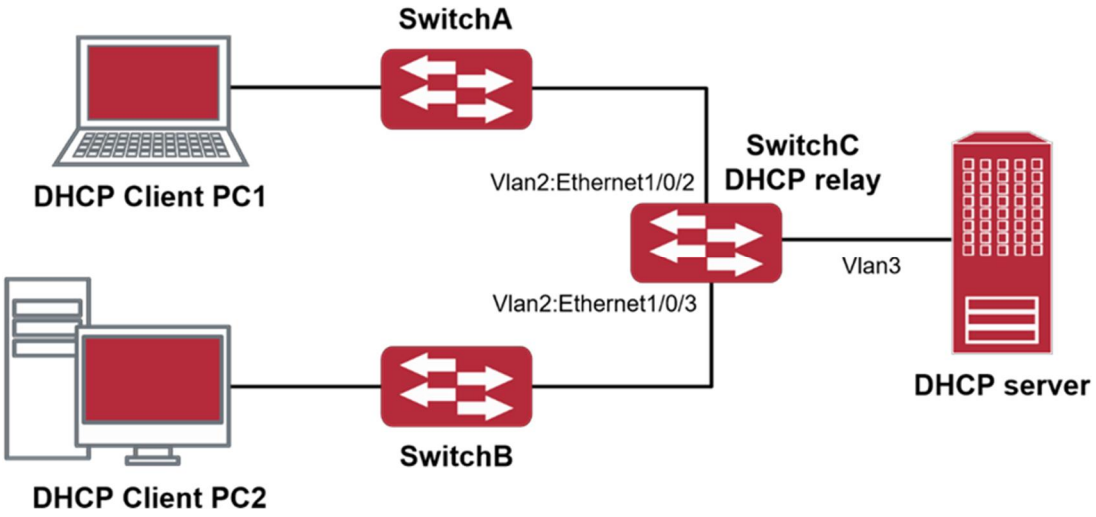


Рисунок 23.2 – Типовой пример применения опции 82 DHCP

В данной схеме оба коммутатора второго уровня (A и B) подключены к коммутатору третьего уровня (C), который передает DHCP-запросы от клиентов серверу. Если опция 82 выключена, DHCP-сервер не сможет распознать, из какой подсети клиент, и все клиенты, подключенные к SwitchA и SwitchB, будут получать адреса из общего адресного пула DHCP-сервера. После включения опции 82, т.к. коммутатор C добавляет к запросу информацию о порте, сервер сможет распознать, в какой сети находится клиент (SwitchA или SwitchB) и, таким образом, сможет выделять разное адресное пространство двум подсетям, чтобы упростить управление сетью.

Конфигурация SwitchC (MAC-адрес 08:B6:C3:00:00:01):

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

Linux ISC DHCP-сервер поддерживает опцию 82, его конфигурационный файл

/etc/dhcpd.conf:

```
ddns-update-style interim; ignore client-updates;
class "Switch3Vlan2ClasSwitchA»{
```

```
match if option agent.circuit-id = "Vlan2+Ethernet1/0/2» and option agent.remote-
id=08:B6:C3:00:00:01;
}
class "Switch3Vlan2ClasSwitchB»{
match if option agent.circuit-id = "Vlan2+Ethernet1/0/3» and option agent.remote-
id=08:B6:C3:00:00:01;
}
subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name "example.com";
option domain-name-servers 192.168.10.3; authoritative;
pool {
range 192.168.102.21 192.168.102.50;
default-lease-time 86400; #24 Hours
max-lease-time 172800; #48 Hours
allow members of "Switch3Vlan2ClasSwitchA";
}
pool {
range 192.168.102.51 192.168.102.80;
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch3Vlan2ClasSwitchB";
}
}
```

Теперь DHCP-сервер будет выделять адреса для узлов с коммутатора 2 из диапазона 192.168.102.21 ~ 192.168.102.50, а для коммутатора 1 из диапазона 192.168.102.51 ~ 192.168.102.80.

6.2.4 Поиск неисправностей опции 82 DHCP

Опция 82 DHCP реализована как подфункция модуля DHCP-ретранслятора. Прежде, чем ее использовать, необходимо убедиться, что DHCP-ретранслирующий агент настроен правильно.

- Опция 82 требует взаимодействия DHCP-ретранслятора и DHCP-сервера. DHCP-сервер должен установить политику выделения адресов основываясь на сетевой топологии DHCP-ретранслятора, но, даже если ретранслятор работает нормально, выделение адресов может не получиться. Если в сети больше одного ретранслятора, уделите внимание политике передачи DHCP-запросов.
- При реализации функции опции 82 DHCP-ретранслятора, подробная информация о процессе работы функции опции 82 DHCP-ретранслятора может быть получена командой «debug ip dhcp relay packet». Эта информация может помочь в поиске неисправностей.
- При реализации функции опции 82 DHCP-севера, подробная информация о процессе работы функции опции 82 DHCP-сервера может быть получена командой «debug ip dhcp server packet». Эта информация может помочь в поиске неисправностей.

6.3 КОНФИГУРАЦИЯ DHCP SNOOPING

6.3.1 Введение в DHCP Snooping

С помощью DHCP Snooping коммутатор контролирует процесс присвоения IP-адресов по протоколу DHCP. Это предотвращает появление нелегальных DHCP-серверов и DHCP-атаки путем настройки доверенных и недоверенных портов. DHCP-сообщение с доверенных портов передается без проверки.

При типичной конфигурации доверенные порты используются для подключения DHCP-сервера или DHCP-ретранслятора, а к недоверенным портам подключаются клиенты. С недоверенных портов коммутатор будет пересылать только DHCP-запросы, но не ответы. Если с недоверенного порта получено сообщение DHCP-ответа, коммутатор поднимет тревогу и предпримет определенные действия с портом, согласно настройкам, например, выключение или создание «black hole».

Если включена привязка DHCP Snooping Binding, коммутатор сохранит в соответствующей таблице связующую информацию о каждом DHCP-клиенте с недоверенного порта (включая MAC-адрес, IP-адрес, аренду IP, номера VLAN и порта). Имея такую информацию DHCP Snooping, можно комбинировать с другими модулями, такими, как dot1x и ARP, или самостоятельно реализовать контроль доступа пользователей.

Основной функционал:

Защита от поддельного DHCP-сервера: если коммутатор перехватывает ответ DHCP-сервера (включая DHCPOFFER, DHCPACK и DHCPNAK), он поднимет тревогу и предпримет определенные действия, согласно настройкам (выключение порта или создание «black hole»).

Защита от перегрузки DHCP: Чтобы избежать большого количества сообщений DHCP, атакующих процессор, пользователь может ограничить скорость получения DHCP-пакетов на доверенных и недоверенных портах.

Запись данных привязки DHCP (dhcp snooping binding): DHCP snooping при пересылке DHCP-пакетов будет записывать данные (ip + mac). Можно так же загрузить эти данные на сервер в целях восстановления утерянной информации. Данные привязки, в основном, используются для настройки динамических пользовательских портов dot1x. За подробной информацией о dot1x обратитесь, пожалуйста, к главе «Настройка dot1x».

Добавление связующего ARP: можно добавить статическую связку ARP в соответствии с динамическими данными, чтобы предотвратить ARP-мошенничество.

Добавление доверенных пользователей: можно добавить записи в список доверенных пользователей в соответствии с параметрами связующих данных; эти пользователи получат доступ ко всем ресурсам без dot1x-аутентификации.

Автоматическое восстановление: через некоторое время после выключения порта или создания «black hole», нужно автоматически убрать блокировку порта или MAC-адреса и отправить при этом информацию на сервер через syslog.

Функция журнала: Когда коммутатор обнаруживает ненормальные пакеты, он должен отправить информацию на сервер журнала через syslog.

Шифрование приватных сообщений: связь между коммутатором и внутренней системой управления безопасностью сети TrustView происходит через приватные сообщения. Пользователи могут шифровать эти сообщения в версии 2.

Функция добавление опции 82: различные sub-опции 82 добавляются в DHCP-сообщение в соответствии со статусом аутентификации пользователя.

6.3.2 Последовательность конфигурации DHCP Snooping

1. Включить DHCP Snooping.
2. Включить функцию привязки DHCP Snooping.
3. Включить функцию привязки ARP DHCP Snooping.
4. Включить функцию опции 82 DHCP Snooping.
5. Установить версию приватных пакетов.
6. Установить зашифрованный ключ DES для приватных пакетов.
7. Установить адрес DHCP-сервера.

8. Настроить доверенные порты.
9. Включить функцию привязки DHCP Snooping DOT1X.
10. Включить функцию привязки DHCP Snooping USER.
11. Добавить записи в статический список.
12. Установить действия защиты.
13. Включить функцию записи в журнал событий о действиях защиты.
14. Установить ограничение скорости передачи DHCP-сообщений.
15. Включить отладку.
16. Настроить атрибуты опции 82 DHCP Snooping.

1. Включить DHCP Snooping.

Команда	Описание
Глобальный режим	
ip dhcp snooping enable no ip dhcp snooping enable	Включить/выключить DHCP Snooping.

2. Включить функцию привязки DHCP Snooping.

Команда	Описание
Глобальный режим	
ip dhcp snooping binding enable no ip dhcp snooping binding enable	Включить/выключить функцию привязки DHCP Snooping.

3. Включить функцию привязки ARP DHCP Snooping.

Команда	Описание
Глобальный режим	
ip dhcp snooping binding arp no ip dhcp snooping binding arp	Включить/выключить функцию привязки ARP DHCP Snooping.

4. Включить функцию опции 82 DHCP Snooping.

Команда	Описание
Глобальный режим	
ip dhcp snooping information enable no ip dhcp snooping information enable	Включить/выключить функцию опции 82 DHCP Snooping.

5. Установить версию приватных пакетов.

Команда	Описание
Глобальный режим	
ip user private packet version two no ip user private packet version two	Настроить/удалить версию приватных пакетов.

6. Установить зашифрованный ключ DES для приватных пакетов.

Команда	Описание
Глобальный режим	
enable trustview key 0/7 <password> no enable trustview key	Настроить/удалить зашифрованный ключ DES для приватных пакетов.

7. Установить адрес DHCP-сервера.

Команда	Описание
Глобальный режим	
ip user helper-address A.B.C.D [port <udpport>] source <ipAddr> (secondary|) no ip user helper-address (secondary|)	Настроить/удалить адрес DHCP-сервера.

8. Настроить доверенные порты.

Команда	Описание
Режим порта	
ip dhcp snooping trust {vlan <vlan-list>} no ip dhcp snooping trust {vlan <vlanlist>}	Сделать порт доверенным. Команда no отменяет настройку.

9. Включить функцию привязки DHCP Snooping DOT1X.

Команда	Описание
Режим порта	
ip dhcp snooping binding dot1x no ip dhcp snooping binding dot1x	Включить/выключить функцию привязки DHCP Snooping DOT1X.

10. Включить функцию привязки DHCP Snooping USER.

Команда	Описание
Режим порта	

ip dhcp snooping binding user-control no ip dhcp snooping binding usercontrol	Включить/выключить функцию привязки DHCP Snooping USER.

11. Добавить записи в статический список.

Команда	Описание
Глобальный режим	
ip dhcp snooping binding user <mac> address <ipAddr> vlan <vid> interface (ethernet|) <ifname> no ip dhcp snooping binding user <mac> interface (ethernet|) <ifname>	Добавить/удалить записи в статический список.

12. Установить действия защиты.

Команда	Описание
Режим порта	
ip dhcp snooping action {shutdown|blackhole} [recovery <second>] no ip dhcp snooping action	Установить/отменить автоматические защитные действия на портах.

13. Включить функцию записи в журнал событий о действиях защиты.

Команда	Описание
Глобальный режим	
ip dhcp snooping blocked record enable no ip dhcp snooping blocked record enable	Включить/выключить функцию записи в журнал событий о действиях защиты.

14. Установить ограничение скорости передачи DHCP-сообщений.

Команда	Описание
Глобальный режим	
ip dhcp snooping limit-rate <pps> no ip dhcp snooping limit-rate	Установить ограничение скорости передачи DHCP-сообщений.

15. Настроить атрибуты опции 82 DHCP Snooping.

Команда	Описание
Глобальный режим	

ip dhcp snooping information option subscriber-id format {hex | acsii | vs-hp | vs-huawei | vs-cisco}	Устанавливает формат subscriber-id опции 82 DHCP snooping.
ip dhcp snooping information option remote- id {<remote-id> | cpu-mac | standard | vs-cisco | vs- huawei} no ip dhcp snooping information option remote-id	Устанавливает содержание суб-опции remote-id опции 82. Команда no возвращает стандартный формат.
ip dhcp snooping information option allow-untrusted [replay] no ip dhcp snooping information option allow-untrusted	Разрешить передачу DHCP-запросов с добавленной опцией 82, полученные с недоверенных портов, replace - поле опции 82 будет добавлено заново, после чего запросу будет передан серверу. Если не включено, все недоверенные порты будут отбрасывать DHCP-пакеты с опцией 82.
ip dhcp snooping information option delimiter [colon | dot | slash | space | none] no ip dhcp snooping information option delimiter	Устанавливает разделитель для параметров суб-опций опции 82. Команда no устанавливает разделитель по умолчанию – slash.
ip dhcp snooping information option self-defined remote-id {template <template> | hostname | mac | string WORD} no ip dhcp snooping information option selfdefined remote-id	Задает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции remoteid.
ip dhcp snooping information option self-defined remote-id format [ascii | hex]	Пользовательский формат remote-id для опции 82.
ip dhcp snooping information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac) | string WORD} no ip dhcp snooping information option type self-defined subscriber-id	Задает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции circuteid.
ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]	Пользовательский формат circuit-id для опции 82.
ip dhcp snooping information option reply keep no ip dhcp snooping information option reply keep	Сохранять опцию 82 при ответах и не удалять её. Команда no отключает сохранение опции 82 в ответах.

ip dhcp snooping information option subscriber-id format (ascii | hex | vs-cisco | vs-hp | vs-huawei)p dhcp snooping information option subscriber-id format (ascii | hex | vs-cisco | vs-hp | vs-huawei

6.3.3 Типовое применение DHCP Snooping

Как показано на рисунке, устройство Mac-AA – обычный пользователь, подключенный к недоверенному порту 1/0/1 коммутатора, получает IP-настройки через DHCP, IP-адрес клиента 1.1.1.5. DHCP-сервер и шлюз подключены к доверенным портам коммутатора, 1/0/11 и 1/0/12 соответственно. Злоумышленник Mac-BB, подключенный к недоверенному порту 1/0/1 коммутатора, пытается подделать DHCP-сервер (посылая пакеты DHCPACK). Функция DHCP Snooping на коммутаторе эффективно обнаружит и блокирует такой тип сетевой атаки.

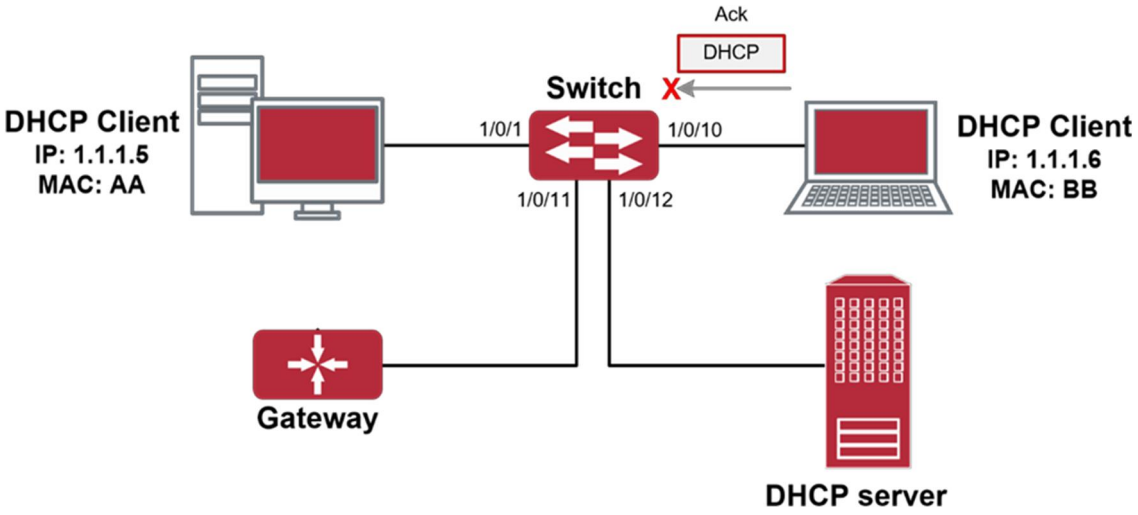


Рисунок 24.1 – Типовое применение

Последовательность настройки:

```
rotek# rotek#config
rotek(config)#ip dhcp snooping enable
rotek(config)#interface ethernet 1/0/11
rotek(Config-If-Ethernet1/0/11)#ip dhcp snooping trust
rotek(Config-If-Ethernet1/0/11)#exit
rotek(config)#interface ethernet 1/0/12
rotek(Config-If-Ethernet1/0/12)#ip dhcp snooping trust
rotek(Config-If-Ethernet1/0/12)#exit
rotek(config)#interface ethernet 1/0/1-10
rotek(Config-Port-Range)#ip dhcp snooping action shutdown
rotek(Config-Port-Range)#
```

6.3.4 Устранение неисправностей DHCP Snooping

6.3.4.1 Наблюдение и отладочная информация

Для получения отладочной информации может быть использована команда «debug ip dhcp snooping».

6.3.4.2 Устранение неисправностей

Если возникает проблема с использованием функции DHCP Snooping, пожалуйста, проверьте следующее:

- Включена ли функция DHCP Snooping глобально;
- Если порт не реагирует на ложный DHCP-пакет, проверьте, настроен ли этот порт как недоверенный.

7 Безопасность

7.1 TACACS+

7.1.1 Общие сведения о TACACS+

TACACS+ представляет собой похожий на RADIUS сеансовый протокол контроля доступа. Протокол TACACS+ использует три независимые функции: Аутентификация, Авторизация и Аккаунтинг (учёт) (AAA). В отличие от RADIUS протокол TACACS+ использует TCP и шифрование передаваемых данных для обеспечения безопасности.

На данном коммутаторе TACACS+ может быть использован при авторизации и аутентификации пользователей для доступа к коммутатору по telnet или ssh.

7.1.2 Конфигурация TACACS+

1. Задать ключ сервера TACACS+
2. Настроить тайм-аут аутентификации TACACS+
3. Настроить параметры сервера TACACS+
4. Настроить IP-адрес TACACS+ NAS

1. Задать ключ сервера TACACS+

Команда	Описание
Глобальный режим	
tacacs-server key {0 | 7} <string> *no tacacs-server key*	Задать глобальный ключ сервера TACACS+. Команда no удаляет этот ключ.

2. Настроить тайм-аут аутентификации TACACS+

Команда	Описание
Глобальный режим	
tacacs-server timeout <seconds> *no tacacs-server timeout*	Задать глобальное время ожидания ответа от TACACS+ сервера в секундах. Команда no возвращает значение по умолчанию - 3 секунды.

3. Настроить параметры сервера TACACS+

Команда	Описание
Глобальный режим	
tacacs-server authentication host <ipaddress> [port <port-number>] [timeout <seconds>] [key {0 | 7} <string>] [primary]	Сконфигурировать параметры обращения к серверу TACACS+: <ipaddress> - IP-адрес сервера;[port <port-number>] - порт назначения (по умолчанию 49); [timeout <seconds>] - время ожидания ответа от сервера;key {0 | 7} <string>] - ключ сервера; primary - данный сервер будет использоваться в приоритетном порядке. Если параметры [timeout <seconds>] и key {0 | 7} <string>] не

no tacacs-server authentication host <ip-address>	заданы, будут использоваться параметры, заданные глобально. Команда **no** удаляет заданный сервер с адресом <ip-address>.

4. Настроить IP-адрес TACACS+ NAS

Команда	Описание
Глобальный режим	
tacacs-server nas-ipv4 <ip-address> *no tacacs-server nas-ipv4*	Задать IP-адрес <ip-address> источника пакетов TACACS+, отправляемых коммутатором. Команда no устанавливает в качестве источника адрес IP-интерфейса, с которого были отправлены пакеты (по умолчанию).

7.1.3 Пример типичной конфигурации TACACS+

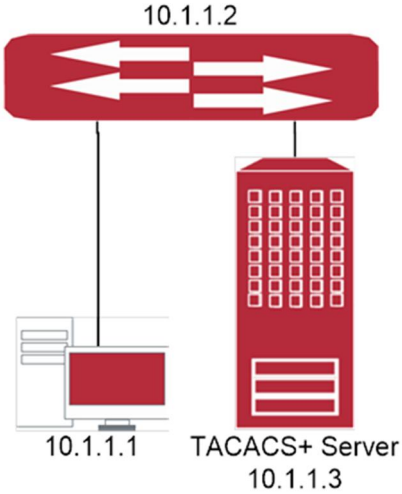


Рисунок 25.1 – Пример схемы подключений для конфигурации TACACS+

Компьютер подключается к коммутатору, IP-адрес которого 10.1.1.2 и который соединен с сервером аутентификации TACACS+. IP-адрес сервера - 10.1.1.3, порт аутентификации по умолчанию – 49.

Установите аутентификацию telnet log on коммутатора как локальную tacacs с помощью сервера аутентификации TACACS + для обеспечения аутентификации пользователей telnet.

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#tacacs-server authentication host 10.1.1.3
Switch(config)#tacacs-server key test
Switch(config)#authentication line vty login tacacs
```

7.1.4 Устранение проблем при конфигурации TACACS+

Убедитесь, что:

- IP-связность коммутатора с сервером TACACS+ присутствует;
- Ключ аутентификации на коммутаторе совпадает с ключом на TACACS+ сервере;

- Подключение осуществляется к правильному TACACS+ серверу.

7.2 RADIUS

7.2.1 Общие сведения о RADIUS

7.2.1.1 Общее описание AAA и RADIUS

AAA - сокращение от Authentication, Authorization and Accounting (Аутентификация, Авторизация, учёт) и используется при предоставлении доступа в сеть, к управлению оборудованием и управления этим доступом. RADIUS - это один из сетевых клиент-серверных протоколов, используемый для централизованного управления авторизацией, аутентификацией и учетом при запросе доступа пользователей к различным сетевым службам. Клиент RADIUS обычно используется на сетевом устройстве для реализации AAA совместно с протоколом 802.1x. Сервер RADIUS хранит базу данных для AAA и связывается с клиентом RADIUS через протокол RADIUS, который является наиболее распространенным протоколом в рамках AAA.

7.2.1.2 Структура сообщения для RADIUS

Протокол RADIUS использует UDP для доставки пакетов протокола. Формат пакета показан ниже.

0 7	15	31
Code	Identifier	Length
Authenticator		
Attributes		

Поле Code (1 октет): тип пакета RADIUS. Доступное значение для поля кода показано ниже:

1 Access-Request

2 Access-Accept

3 Access-Reject

4 Accounting-Request

5 Accounting-Response

11 Access-Challenge

Поле Identifier (1 октет): Идентификатор для пакетов запроса и ответа.

Поле Length (2 октета): Длина всего пакета RADIUS, включая поле Code, Identifier, Length, Authenticator и Attributes.

Поле Authenticator (16 октетов): используется для проверки пакетов, полученных от сервера RADIUS. Его также можно использовать для переноса зашифрованных паролей. Это поле подразделяется на два вида: Request Authenticator и Response Authenticator.

Поле Attributes: используется для переноса подробной информации о AAA. Значение атрибута формируется полями Type (Тип), Length (Длина) и Value (Значение).

- Поле Type (1 октет) – тип значения атрибута, который показан ниже:

Значение	Тип значения	Значение	Тип значения
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State

Значение	Тип значения	Значение	Тип значения
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-Id	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-Id	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

- Поле Length (1 октет) – длина в октетах атрибута, включая поля Type, Length и Value.
- поле Value – значение атрибута, содержимое и формат которого определяются типом и длиной атрибута.

7.2.2 Конфигурация RADIUS

1. Включить функцию аутентификации и учета
2. Настроить ключ сервера RADIUS
3. Настроить параметры сервера RADIUS
4. Настроить параметры сервиса RADIUS
5. Настроить адреса RADIUS NAS

1. Включить функцию аутентификации и учета

Команда	Описание

Глобальный режим	
aaa enable no aaa enable	Включить функцию аутентификации AAA. Команда no отключает эту функцию.
aaa-accounting enable no aaa-accounting enable	Включить функцию учета AAA. Команда no отключает эту функцию.
aaa-accounting update {enable|disable}	Включить или выключить (по умолчанию) периодическую отправку данных об онлайн-пользователях.

2. Настроить ключ сервера RADIUS

Команда	Описание
Глобальный режим	
radius-server key {0 | 7} <string> no radius-server key	Задать глобальный ключ RADIUS-сервера. Команда no удаляет заданный ключ.

3. Настроить параметры RADIUS сервера

Команда	Описание
Глобальный режим	
radius-server authentication host {<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary] [access-mode {dot1x | telnet}] no radius-server authentication host {<ipv4-address> | <ipv6-address>}	Настроить параметры RADIUS-сервера <ipv4-address> | <ipv6-address> для аутентификации. Если параметр [key {0 | 7} <string>] не будет задан, то будет использован параметр, заданный глобально. Команда no удаляет заданный сервер.
radius-server accounting host {<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary] no radius-server accounting host {<ipv4-address> | <ipv6-address>}	Настроить параметры RADIUS-сервера <ipv4-address> | <ipv6-address> для учета. Если параметр [key {0 | 7} <string>] не будет задан, то будет использован параметр, заданный глобально. Команда no удаляет заданный сервер.

4. Настроить параметры сервиса RADIUS

Команда	Описание
Глобальный режим	
radius-server retransmit <retries> no radius-server retransmit	Задать число попыток <retries> повторной отправки пакетов на RADIUS-сервер. Команда no восстанавливает значение по умолчанию - 3 попытки.
radius-server timeout <seconds> no radius-server timeout	Задать время ожидания ответа от сервера перед повторной отправкой пакета, в секундах. Команда no восстанавливает значение по умолчанию - 3 секунды.

5. Настроить адреса RADIUS NAS

Команда	Описание
Глобальный режим	
radius nas-ipv4 <ip-address> no radius nas-ipv4	Задать IPv4-адрес <ip-address> источника пакетов RADIUS, отправляемых коммутатором. Команда no устанавливает в качестве источника адрес IP-интерфейса, с которого были отправлены пакеты (по умолчанию)

7.2.3 Примеры типовой настройки RADIUS

7.2.3.1 Пример настройки RADIUS при использовании IPv4

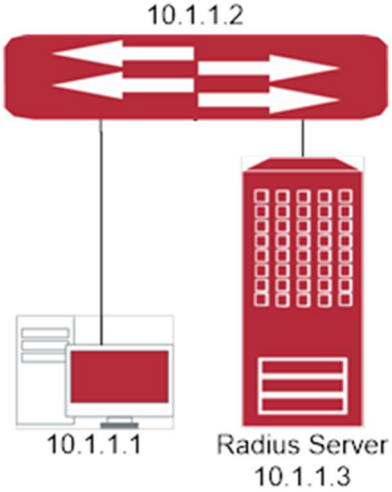


Рисунок 26.1 – Пример схемы подключений для конфигурации RADIUS

Компьютер подключается к коммутатору, IP-адрес которого 10.1.1.2 и подключен к серверу аутентификации RADIUS без Ethernet1/0/2. IP-адрес сервера - 10.1.1.3, порт аутентификации по умолчанию - 1812, порт учета - 1813.

Порядок настройки:

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

7.2.3.2 Пример настройки RADIUS при использовании IPv6

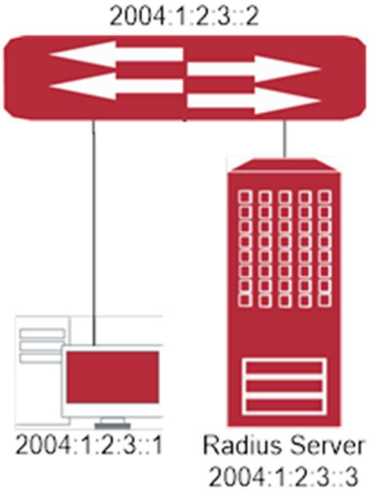


Рисунок 26.2

Компьютер подключается к коммутатору, IP-адрес которого - 2004:1:2:3:: 2 и подключен к серверу аутентификации RADIUS без Ethernet1/0/2. IP-адрес сервера - 2004:1:2:3:: 3, порт аутентификации по умолчанию - 1812, порт учета по умолчанию - 1813.

Порядок настройки:

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

7.2.4 Устранение проблем при конфигурации RADIUS

Убедитесь, что:

- IP-связность коммутатора с сервером RADIUS присутствует;
- ключ аутентификации на коммутаторе совпадает с ключом на RADIUS сервере;
- подключение осуществляется к правильному RADIUS серверу.
- Подробная отладочная информация может быть отображена после применения команды debug aaa.

7.3 PPPoE Intermediate Agent

7.3.1 Общие сведения о PPPoE Intermediate Agent

Протокол *PPPoE (Point to Point Protocol over Ethernet)* - протокол канального уровня передачи **PPP кадров** через **Ethernet**. **PPPoE** — это туннелирующий протокол, который позволяет инкапсулировать IP или другие протоколы через соединения **Ethernet**, устанавливая соединение «точка-точка», которое используется для транспортировки **IP-пакетов**. Такое соединение может быть установлено с **BRAS**, предоставляя пользователю широкополосный доступ и использующее аутентификацию.

PPPoE Intermediate Agent предоставляет возможность инкапсулировать в пакеты **PPPoE** данные о местоположении пользователя, что обеспечивает дополнительные возможности для проверки подлинности.

Существует 2 этапа в работе **PPPoE:** этап обнаружения и этап сеанса.

Этап обнаружения используется для получения MAC-адреса удаленного сервера для установления соединения «**точка-точка**» и идентификатора сеанса с сервером, а этап сеанса использует этот идентификатор сеанса для связи. **PPPoE Intermediate Agent** относится только к стадии обнаружения.

Этап обнаружения состоит из четырех шагов:

1. Клиент отправляет пакет **PADI (PPPoE Active Discovery Initiation)**. На первом шаге клиент использует широковещательный адрес как адрес назначения и широковещательный **PADI** (инициация активного обнаружения **PPPoE**) пакет для обнаружения концентратора доступа;
2. Сервер отправляет в ответ **PADO (PPPoE Active Discovery Offer).** Как только пользовательская машина отослала **PADI-пакет**, сервер отвечает, посылая **PADO-пакет**, используя **MAC-адреса**, пришедшие с **PADI. PADO-пакет** содержит **MAC-адреса** сервера, его имя и имя сервиса;
3. Клиент выбирает сервер, отсылая **PADR (PPPoE Active Discovery Request);**
4. Подтверждая полученный PADR-пакет, сервер посылает **PADS (PPPoE Active Discovery Session-confirmation)**, содержащий идентификатор сессии - **Session ID.**

PPPoE Intermediate Agent перехватывает **PADI** и **PADR** пакеты, добавляя дополнительные данные, идентифицирующие местоположение пользователя, например **MAC** коммутатора, порт коммутатора, **VLAN** пользователя. PPPoE Intermediate Agent также включает в себя функцию доверенного порта, который позволяет заблокировать прием нежелательных **PADO** и **PADS** пакетов с недоверенных портов.

7.3.2 Конфигурация PPPoE Intermediate Agent

1. Настроить PPPoE Intermediate Agent глобально;
2. Настроить PPPoE Intermediate Agent на интерфейсе.

1. Настроить PPPoE Intermediate Agent глобально:

Команда	Описание
В режиме глобальной конфигурации	
pppoe intermediate-agent no pppoe intermediate-agent	Включить фунцию PPPoE Intermediate Agent, команда no отключает эту функцию
pppoe intermediate-agent type tr-101 circuit-id access-node-id <string> no pppoe intermediate-agent type tr-101 circuit-id access-node-id	Настроить идентификатор узла доступа <string> с circuit-id tr-101 Команда no удаляет этот идентификатор. Формат circuit-id по-умолчанию: access-node-id +” eth “+ Slot ID + delimiter + Port Index + delimiter + Vlan ID. Пример тега: “abcd eth 01/003:0003”
pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp | sv | pv | spv} delimiter <WORD> [delimiter <WORD>]	Настроить добавляемые поля circuit-id формата tr-101. sp - слот и порт, sv - слот и vlan, pv - порт и vlan, spv - слот и порт и vlan. В случае использования spv может быть указано 2 различных разделителя delimiter друг за другом. Команда no возвращает формат по-умолчанию - spv. Формат circuit-id по-умолчанию: access-node-id +” eth

no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter	“+ Slot ID + delimiter + Port Index + delimiter + Vlan ID. Пример тега: “abcd eth 01/003:0003”
pppoe intermediate-agent type self-defined circuit-id {vlan| port|id (switch-id (mac | hostname)| remote-mac) | string WORD} no pppoe intermediate-agent type self-defined circuit-id	Задать собственный формат circuit-id. Команда no удаляет эту конфигурацию.
pppoe intermediate-agent type self-defined remoteid {mac | vlan-mac |hostname| string WORD} no pppoe intermediate-agent type self-defined remote-id	Задать собственный формат remote-id. Команда no удаляет эту конфигурацию.
pppoe intermediate-agent delimiter <WORD> no pppoe intermediate-agent delimiter	Задать разделитель (#|.|,|;|:|/|space). Команда no возвращает разделитель по-умолчанию - ‘\’
pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii) no pppoe intermediate-agent format (circuit-id | remote-id)	Задать формат представления circuit-id или remote-id. Команда no удаляет эту конфигурацию.

2. Настроить PPPoE Intermediate Agent на интерфейсе:

Команда	Описание
В режиме конфигурации интерфейса	
pppoe intermediate-agent no pppoe intermediate-agent	Включить фунцию PPPoE Intermediate Agent, команда no отключает эту функцию
pppoe intermediate-agent vendor-tag strip no pppoe intermediate-agent vendor-tag strip	Включить функцию снятия тега вендора на порту. Команда no отключает эту функцию.
pppoe intermediate-agent trust no pppoe intermediate-agent trust	Выбрать порт в качестве доверенного. Команда no выбирает порт в качестве недоверенного.
pppoe intermediate-agent circuit-id <string> no pppoe intermediate-agent circuit-id	Задать строку circuit-id, для добавления на порту. Команда no удаляет эту конфигурацию.
pppoe intermediate-agent remote-id <string> no pppoe intermediate-agent remote-id	Задать строку remote-id

7.3.3 Пример конфигурации PPPoE Intermediate Agent

PPPoE клиент и сервер подключены к одной **L2 Ethernet** сети. На коммутаторе, к которому подключен клиент, активирована функция **PPPoE Intermediate Agent**.

Пример конфигурации 1:

```
Switch(config)#pppoe intermediate-agent
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust vendor-
tag strip
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-
node-id abcd
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id
aaaa
Switch (config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id
xyz
```

В результате **circuit-id** для клиента в порту eth1/0/2 будет выглядеть как ”**abcd eth 01/002:0001**”, **remote-id** - MAC коммутатора ”**0a0b0c0d0e0f**”.
Для клиента в порту eth1/0/3 будет добавляться **circuit-id** ”**aaaa**”, **remote-id** ”**xyz**”.

Пример конфигурации 2:

```
Switch(config)#pppoe intermediate-agent
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent
Switch(config-if-ethernet1/0/3)#exit
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-
node-id abcd
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id
identifier-string efgh option spv delimiter # delimiter /
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent circuit-id
bbbb
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id xyz
```

В результате **circuit-id** для клиента в порту eth1/0/2 будет выглядеть как ”**bbbb**”, **remote-id** - MAC коммутатора ”**0a0b0c0d0e0f**”.
Для клиента в порту eth1/0/3 будет добавляться **circuit-id** ”**efgh eth 01#003/1234, remote-id** ”**xyz**”.

8 ЗЕРКАЛИРОВАНИЕ ТРАФИКА

8.1 Зеркалирование трафика (SPAN)

8.1.1 Общие сведения о зеркалировании трафика

Функция зеркалирования трафика позволяет дублировать трафик, отправляемый или принимаемый портом или CPU коммутатора в другой порт. К порту назначения дублированного трафика может быть подключен анализатор трафика SPAN (Switch Port Analyzer) для диагностики проблем в сети.

На данном коммутаторе также существует возможность дублировать входящий в порт трафик на основе разрешающих правил ACL.

8.1.2 Конфигурация SPAN

1. Задать порт (CPU) источника трафика
2. Задать порт назначения зеркала
3. Задать скорость дискретизации
4. Выбрать порт-источник трафика с использованием ACL

1. Задать порт (CPU) источника трафика

Команда	Описание
Глобальный режим	
monitor session <session> source {interface <interface-list> | cpu} {rx| tx| both}	Задать интерфейс или CPU в качестве источника трафика зеркала для сессии <session>. {rx| tx| both} указывают направление трафика.
no monitor session <session> source {interface <interface-list> | cpu}	Команда no удаляет источник трафика для сессии <session>.

2. Задать порт назначения зеркала

Команда	Описание
Глобальный режим	
monitor session <session> destination interface <interface-number>	Задать интерфейс назначения трафика зеркала для сессии <session>.
no monitor session <session> destination interface <interface-number>	Команда no удаляет интерфейс назначения для сессии <session>.

3. Задать скорость дискретизации

Команда	Описание
Глобальный режим	
monitor session <session> sample rate <num>	Задать скорость дискретизации <0-65535> для зеркала <session>.

no monitor session <session> sample rate	Команда no отменяет дискретизацию - каждый пакет из источника попадет в зеркало.

4. Выбрать порт-источник трафика с использованием ACL

Команда	Описание
Глобальный режим	
monitor session <session> source {interface <interface-list>} access-group <num> {rx} no monitor session <session> source {interface <interface-list>} access-group <num>	Задать интерфейс в качестве источника трафика зеркала для сессии <session>. access-group <num> rx применяет ACL на входящее направление трафика в интерфейсе источника зеркала. Команда no удаляет источник трафика для сессии <session>.

8.1.3 Пример конфигурации SPAN

В порт 1/0/1 необходимо отправлять следующий трафик:

1. трафик поступающий на порт 1/0/7 (ingress);
2. трафик уходящий с порта 1/0/9 (egress);
3. трафик в CPU всех направлений;
4. трафик TCP с адресом источника 1.2.3.4/24, адресом назначения 5.6.7.8/24 входящий (ingress) в порт 1/0/5.

Конфигурация коммутатора будет выглядеть следующим образом:

```
rotek(config)#monitor session 1 destination interface ethernet 1/0/1
rotek(config)#monitor session 1 source interface ethernet 1/0/7 rx
rotek(config)#monitor session 1 source interface ethernet 1/0/9 tx
rotek(config)#monitor session 1 source cpu
rotek(config)#access-list 120 permit tcp 1.2.3.4 0.0.0.255 5.6.7.8 0.0.0.255
rotek(config)#monitor session 1 source interface ethernet 1/0/15 access-list 120 rx
```

8.1.4 Решение проблем при зеркалировании трафика

- Убедитесь, что пропускная способность интерфейса назначения удовлетворяет суммарному количеству трафика всех источников, учитывая возможные кратковременные всплески трафика;
- для одной сессии возможен выбор только одного интерфейса назначения трафика

9 Конфигурация NTP

9.1 NTP

9.1.1 Общие сведенья о NTP

NTP (Network Time Protocol) - протокол сетевого времени, используемый с целью синхронизации времени среди распределенных серверов и клиентов. Благодаря используемым алгоритмам способен достичь точности до 10мс. События, состояния, функции передачи и действия определены в RFC-1305. Время на коммутаторе может быть синхронизировано с внешним сервером, также коммутатор может выполнять роль эталона времени в качестве NTP сервера.

9.1.2 Конфигурация NTP

1. Включить функцию NTP;
2. Настроить NTP-клиент;
3. Просмотр информации и отладка;

1.Включить функцию NTP.

Команда	Описание
Глобальный режим	
ntp enable ntp disable	Включить функцию NTP. Выключить функцию NTP.

2.Настроить NTP-клиент.

Команда	Описание
Глобальный режим	
ntp server {<ip-address> | <ipv6-address>} [version <version_no>] [key <key-id>] no ntp server {<ip-address> | <ipv6-address>}	Задать IP адрес и ключ сервера, команда no удаляет эту конфигурацию.
clock timezone WORD {add | subtract} <0-23> [<0-59>] no clock timezone WORD	Задать смещение часового пояса относительно UTC. subtract - отрицательное смещение, add - положительное смещение. Команда no удаляет настроенное смещение.

3.Просмотр информации и отладка.

Команда	Описание
Режим администратора	
show ntp status	Отобразить информацию о статусе и конфигурации NTP.

show ntp session [<ip-address> |<ipv6-address>]	Отобразить информацию о сессиях NTP.
debug ntp packets [send | receive] no debug ntp packets [send | receive]	Выводить отладочную информацию о локальных настройках времени. Команда no отменяет вывод отладочной информации.

9.1.3 Пример конфигурации NTP

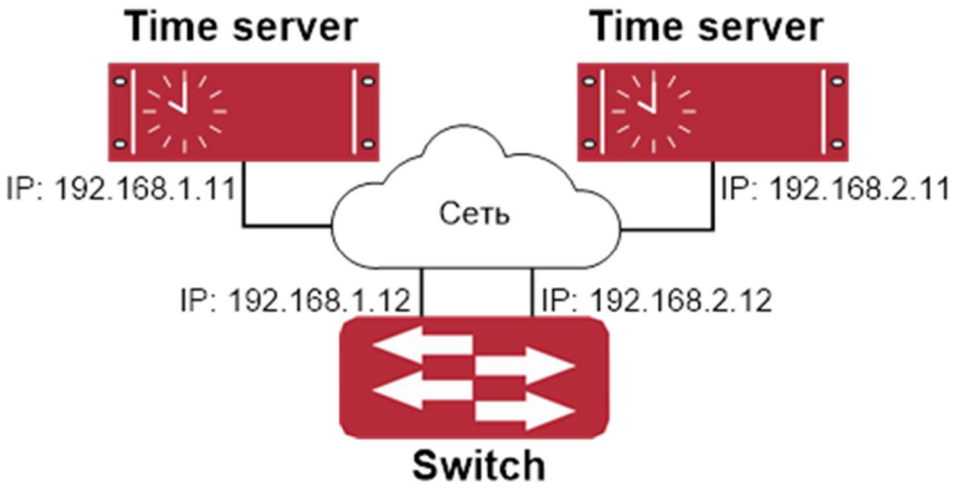


Figure 1 Рисунок 28.1 – Пример схемы для конфигурирования функции NTP

Рисунок 28.1 – Пример схемы для конфигурирования функции NTP

Необходимо синхронизировать локальное время на коммутаторе Switch. В сети расположены два сервера времени: один находится в активном режиме и используется, другой находится в режиме ожидания (используется в качестве резервного).

Процедура конфигурирования:

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

9.1.4 Устранение неработоспособности функции NTP

В процессе конфигурирования, при возникновении ошибки, система может выдать отладочную информацию.

Функция NTP по умолчанию отключена. Для отображения текущей конфигурации можно использовать команду show. Если конфигурация правильная, используйте команду debug для отдельных статусов, настроек и событий. Также может использоваться команда show для отображения текущей информации NTP.

9.2 Летнее время

9.2.1 Общие сведения о летнем времени

Летнее и зимнее время - смещение времени на 1 час вперед весной и на 1 час назад осенью для экономии электроэнергии. В настоящее время большая часть стран мира используют переход на летнее время и обратно. Федеральное законодательство РФ не предусматривает ежегодного перехода на «летнее» и «зимнее» время. Текущее время в разных регионах РФ, в завсимости от расположения, может отличаться.

9.2.2 Конфигурация летнего времени

1. Включить и настроить переход на летнее время.
2. Включить и настроить переход на летнее время.

Команда	Описание
Глобальный режим	
clock summer-time <word> recurring <HH:MM> {<week> <day> <month>|<MM.DD>} <HH:MM> {<week> <day> <month>|<MM.DD>} [<offset>] no clock summer-time	Задать повторяющееся время начала и окончания летнего времени, а также его смещение <offset> Команда no удаляет эту конфигурацию.

9.2.3 Пример конфигурации функции летнего времени

Пример 1:

Требования к конфигурации следующие: Летнее время с 23:00 в первую субботу апреля до 00:00 в последнее воскресенье октября год за годом, смещение часов на 2 часа (120 минут), а летнее время называется time_travel.

Процедура конфигурирования:

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

9.2.4 Устранение неработоспособности функции летнего времени

- Проверить, работает ли командный режим в глобальном режиме.
- Проверить правильность системных часов.

10 НАСТРОЙКА POE

Power over Ethernet (PoE) - технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными через стандартную витую пару в сети Ethernet. Основные настройки PoE на коммутаторах приведены ниже.

10.1 Приоритезация портов PoE

Если необходимая мощность для всех подключенных устройств превышает бюджет коммутатора, некоторые порты PoE будут отключены. Для такого случаев можно указать приоритеты питания по портам - Low / High / Critical.
В первую очередь питание подается на порты с уровнем Critical, затем на High, и, в последнюю очередь, на Low (по умолчанию все порты Low). При нехватке питания PoE на портах с наименьшим приоритетом отключается. Если приоритеты равны, то отключается на порте со старшим номером.

10.2 Повышенный пусковой ток

Некоторым устройствам для запуска требуются повышенный пусковой ток. По умолчанию, если пусковой ток превысит допустимое по мощности значение, то система защиты коммутатора автоматически отключит PoE на порте (как и в случае с power inline max).

Команда	Описание
В режиме глобальной конфигурации	
`power inline max <Вт>`	Установить ограничение максимальной мощности коммутатора
power inline police enable	Включить приоритезацию портов
power inline high-inrush enable	Включение режима повышенного пускового тока
show power inline	Вывод информации о состоаянии PoE
В режиме конфигурации порта	
`power inline max <мВт>`	Установить ограничение выделяемой мощности порта
power inline priority {low | high | critical}	Установить приоритет порта

11 ОБЩАЯ ИНФОРМАЦИЯ

11.1 Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь Вам эффективнее настраивать и эксплуатировать наше оборудование при её использовании, поэтому мы хотели бы услышать Ваши замечания. Мы всегда рады обратной связи, в особенности:

- информации об ошибках в содержании, непонятных или противоречащих местах в тексте;
- предложениям по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на http://labinsys.ru/.

11.2 Техническая поддержка

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