Операционная система
VISP
(Vector Intelligent Service Platform)

Руководство администратора

Приведенные в настоящем руководстве администратора названия и программные продукты могут содержать в себе зарегистрированные товарные знаки своих владельцев.

Настоящее руководство администратора содержит всю необходимую информацию для корректного использования операционной системы VISP (Vector Intelligent Service Platform) (далее по тексту – ОС) производства компании ООО «Ви Лаб».

Настоящее руководство предназначено для специалистов, отвечающих за администрирование системы.

Операционная система VISP является неотъемлемой частью коммутаторов марки Vector Switch.

Данное руководство администратора предназначено для ознакомления пользователя с техническими характеристиками и функциональными возможностями операционной системы VISP.

Руководство администратора обеспечивает полную информативность по структуре интерфейса программного обеспечения, описывает все реализованные функции программы и взаимодействие его с оборудованием.

Оглавление

1 ВВЕДЕНИЕ 8

1.1 Назначение руководства администратора 8

1.2 Начало работы с программным обеспечением VISP 8

1.3 Уровень подготовки пользователей 8

2 ОБЛАСТЬ ПРИМЕНЕНИЯ 9

3 ТРЕБОВАНИЕ К ВСПОМОГАТЕЛЬНОМУ ОБОРУДОВАНИЮ 9

3.1 Требования к коммутатору 9

3.2 Требования к персональному компьютеру 9

4 ПОДГОТОВКА К РАБОТЕ С ОС VISP 9

5 ОПИСАНИЕ РАБОТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ VISP 10

5.1 Знакомство с командами CLI 10

5.2 Введение в режимы CLI 14

5.3 Введение в Синтаксис команд 17

5.4 Горячие клавиши командной строки 19

5.5 История команд 21

5.6 Таблица команд (Описание) 21

6 УПРАВЛЕНИЕ СИСТЕМОЙ 22

6.1 Команды глобального управления 22

6.2 Управление системой 22

6.3 Управление пользователями 24

6.4 Управление системным временем 25

6.5 Управление системным журналом 26

7 ВИРТУАЛЬНЫЙ IP-ИНТЕРФЕЙС 27

7.1 IP-интерфейс 27

7.2 Управление статической маршрутизацией 28

7.3 ARP (Address Resolution Protocol)/ Протокол разрешения адресов 29

7.4 Пример настройки 30

8 КОНФИГУРАЦИЯ ПОРТОВ 36

8.1 Общая конфигурация портов 36

8.2 Конфигурация ограничения скорости порта 36

8.3 Конфигурация управления потоком порта 37

8.4 Показать статус порта 37

9 ТАБЛИЦА MAC-АДРЕСОВ 37

9.1 Определение таблицы пересылки MAC-адресов для коммутаторов 37

9.2 Принцип изучения MAC-адресов 38

9.3 Настройка таблицы MAC-адресов 39

9.4 Пример настройки 40

10 НАСТРОЙКИ БЕЗОПАСНОСТИ 42
10.1 Настройка зеркалирования 42
10.2 Настройка подавления шторма 44
10.3 Пример настройки параметров безопасности 46
11 LLDP (LINK LAYER DISCOVERY PROTOCOL)/ ПРОТОКОЛ ОБНАРУЖЕНИЯ КАНАЛЬНОГО УРОВНЯ 48
11.1 Конфигурация LLDP 49
11.2 Просмотр LLDP 50
11.3 Пример настройки 51
12 VLAN (VIRTUAL LOCAL AREA NETWORK)/ ВИРТУАЛЬНАЯ ЛОКАЛЬНАЯ СЕТЬ 54
12.1 Введение в VLAN 55
12.2 Конфигурация VLAN 61
12.3 Пример настройки VLAN 63
13 КАЧЕСТВО ОБСЛУЖИВАНИЯ 68
13.1 Введение в QoS 68
13.2 Настройка QoS 69
13.3 Просмотр конфигурации 71
13.4 Пример базовой конфигурации QoS 71
14 АГРЕГАЦИЯ КАНАЛОВ 74
14.1 Обзор 74
14.2 Ручное агрегирование каналов 75
14.3 Статическая агрегация каналов 75
14.4 Список команд агрегации каналов 76
14.5 Пример Настройки 77
15 IGMP SNOOPING/ОТСЛЕЖИВАНИЕ IGMP 80
15.1 Введение в IGMP SNOOPING 80
15.2 MVR (Multicast VLAN Registration)/ Регистрация многоадресной сети VLAN 86
15.3 Настройка IGMP SNOOPING 87
15.4 Пример настройки IGMP SNOOPING 90
16 DHCP SNOOPING/ ОТСЛЕЖИВАНИЕ DHCP 92
16.1 Введение в DHCP SNOOPING 92
16.2 Настройка DHCP SNOOPING 93
16.3 DHCP option82 94
16.4 Пример настройки 94
17 DHCP RELAY/ АГЕНТ РЕТРАНСЛЯЦИИ DHCP 96
17.1 Введение в DHCP Relay 96
17.2 Конфигурация DHCP Relay 97
17.3 Пример настройки 99
18 DHCP-сервер 101

18.1 Введение в DHCP-сервер 101
18.2 Пример настройки 103

19 STP (SPANNING TREE PROTOCOL)/ ПРОТОКОЛ КАНАЛЬНЫЙ 105
19.1 Обзор Spanning Tree Protocol/ 105
19.2 Роли портов в Spanning Tree 109
19.3 Конфигурация Spanning Tree 111
19.4 Пример настройки Spanning Tree 113

20 ERPS (ETHERNET RING PROTECTION SWITCHING)/ КОММУТАЦИЯ КОЛЬЦЕВОЙ ЗАЩИТЫ ETHERNET 116
20.1 Обзор ERPS 116
20.2 Введение в ERPS 116
20.3 Поддержка Multi-Ring Intersection and Cutting 121
20.4 Конфигурация ERPS (Ethernet Ring Protection Switching)/ Коммутация кольцевой защиты Ethernet 121
20.5 Пример настройки ERPS 122

21 ACL (ACCESS CONTROL LIS)/ СПИСОК УПРАВЛЕНИЯ ДОСТУПОМ 130
21.1 Обзор ACL 130
21.2 Введение в технологию ACL 130
21.3 Конфигурация ACL 132
21.4 Пример настройки 133

22 Защита IP-источника/ IP Source Guard 135
22.1 Обзор защиты IP-источника 135
22.2 Настройка IPSG 136

23 SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)/ СЕТЕВОЙ ПРОТОКОЛ УПРАВЛЕНИЯ 137
23.1 Обзор SNMP 137
23.2 Введение в технологию SNMP 137
23.3 Настройка SNMP 139

24 СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ 141
24.1 Введение в технологию 141
24.2 Настройка статической маршрутизации 142
24.3 Пример настройки статической маршрутизации 142

25 RIP (ROUTING INFORMATION PROTOCOL)/ ПРОТОКОЛ МАРШРУТИЗАЦИИ ИНФОРМАЦИИ 144
25.1 Обзор RIP 144
25.2 Принцип работы 144
25.3 Настройка RIP 146
25.4 Пример настройки 147

26 OSPF (OPEN SHORTEST PATH FIRST)/ ПРОТОКОЛ ВНУТРЕННЕГО ШЛЮЗА 151
26.1 Обзор OSPF 151
26.2 Терминология и понятия 151

26.3 Конфигурация OSPF 153
26.4 Пример настройки 155

27 POE (POWER OVER ETHERNET)/ ПИТАНИЕ ЧЕРЕЗ ETHERNET 158

27.1 Введение в PoE 158
27.2 Конфигурация POE 160
27.3 Пример настройки 160

28 RMON (REMOTE MONITORING)/ УДАЛЁННЫЙ МОНИТОРИНГ 163

28.1 Общая конфигурация RMON 163
28.2 Просмотр RMON 164

29 IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)/ ПРОТОКОЛ УПРАВЛЕНИЯ ИНТЕРНЕТ-ГРУППАМИ 164

29.1 Введение в IGMP 164
29.2 Настройка IGMP 172

30 PIM (PROTOCOL INDEPENDENT MULTICAST)/ МНОГОАДРЕСНАЯ РАССЫЛКА 173

30.1 Введение в PIM 173
30.2 Введение в PIM-SM 173
30.3 Механизм протокола PIM-SM 174
30.4 Принципы работы 177
30.5 Настройка PIM 181
30.6 Пример настройки 184

31 VRRP (VIRTUAL ROUTER REDUNDANCY PROTOCOL)/ ПРОТОКОЛ РЕЗЕРВИРОВАНИЯ ВИРТУАЛЬНОГО МАРШРУТИЗАТОРА 190

31.1 Введение в VRRP 190
31.2 Настройка VRRP 193
31.3 Пример настройки 194

32 BGP (BORDER GATEWAY PROTOCOL)/ ПРОТОКОЛ ПОГРАНИЧНОГО ШЛЮЗА 198

32.1 Обзор BGP 198
32.2 Настройка BGP 199
32.3 Пример настройки 200

33 DOT1X/ ПРОТОКОЛ УПРАВЛЕНИЯ ДОСТУПОМ К СЕТИ НА ОСНОВЕ ПОРТОВ 202

33.1 Обзор Dot1x 202
33.2 Конфигурация dot1x 203
33.3 Пример настройки 204

34 НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ 205

34.1 Восстановление ПО коммутатора через встроенный загрузчик 205

35 Информирование о лицензиях 207

35.1 SNMP 207
35.2 PIMD 208

1 ВВЕДЕНИЕ

1.1 Назначение руководства администратора

Настоящее руководство администратора представляет полную информацию о характеристиках и функция операционной системы VISP.

Операционная система VISP является частью коммутатора серии Vector Switch и работает только при его наличии. Интерфейс операционной системы открывается на персональном компьютере пользователя через IP-адрес коммутатора.

В настоящем руководстве администратора предоставлена вся необходимая для специалиста или рабочего информация, оснащённая графическими указателями и подробными описаниями каждой функции программного обеспечения.

1.2 Начало работы с программным обеспечением VISP

Перед началом работы убедитесь в наличии коммутатора марки Vector Switch совместимого с операционной системой VISP и персонального компьютера с предустановленным веб-браузером.

Ознакомьтесь с настоящим руководством администратора и при возникновении вопросов воспользуйтесь содержанием, собранным для удобства навигации по разделам руководства. Убедитесь, что проблема не описана в одном из них.

При возникновении проблем, не описанных в настоящем руководстве пользователя, необходимо обратиться в сервисный центр компании, любым удобным для пользователя способом:

- по электронной почте: **support@vi-lab.tech;**
- на сайте: **https://vi-lab.tech**;
- по телефону: **+7 (495) 127-01-64.**

1.3 Уровень подготовки пользователей

Специалист, осуществляющий работу с операционной системой VISP, должен обладать знаниями и умениями эксплуатации коммутаторов и их операционной системы, а также обладать углублёнными знаниями работы с командной строкой.

2 ОБЛАСТЬ ПРИМЕНЕНИЯ

Операционная система VISP производства компании ООО «Ви Лаб» обеспечивает доступ для функций и аппаратной части коммутаторов марки Vector Switch.

Операционная система VISP – это комплекс программ, предназначенных для управления ресурсами коммутатора и организации сетевого взаимодействия.

Система представляет собой пакет функций маршрутизации, коммутации, межсетевого взаимодействия и обмена данными, интегрированный в многозадачную операционную систему. Встроенные возможности безопасности обеспечивают контроль доступа к сети, интегрированный с проверкой целостности конечной точки, контролем доступа, простым и интуитивно понятным интерфейсом конфигурации и мониторинга.

3 ТРЕБОВАНИЕ К ВСПОМОГАТЕЛЬНОМУ ОБОРУДОВАНИЮ

3.1 Требования к коммутатору

Операционная система VISP производства компании ООО «Ви Лаб» совместимо только с коммутаторами марки Vector Switch и не предназначено для работы с другими коммутаторами.

3.2 Требования к персональному компьютеру

Специальных требований к персональному компьютеру не предъявляется.

Перед началом работы, убедитесь, что на персональному компьютере установлен веб-браузер.

4 ПОДГОТОВКА К РАБОТЕ С ОС VISP

1. Перед началом работы с операционной системой VISP производства ООО «Ви Лаб», убедитесь в наличии:

– Коммутатора марки Vector Switch с предустановленной операционной системой;

– Персонального компьютера с установленным веб-браузером.

2. Установите коммутатор на предназначенное для него место.

3. Определите персональный компьютер, с которого будет осуществляться подключение к операционной системе VISP и убедитесь, что на нём предустановлен веб-браузер.

4. Подключитесь к операционной системе VISP через IP-адрес. По умолчанию на коммутаторах адрес 192.168.1.240 255.255.255.0, по этому адресу пользователь может подключиться, использовав адрес для своего персонального компьютера, находящегося в той же сети.

5 ОПИСАНИЕ РАБОТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ VISP

5.1 Знакомство с командами CLI

CLI (Command Line Interface) - интерфейс командной строки.

В этой главе подробно описаны команды CLI. Она в основном включает в себя следующие темы:

- Вход в CLI коммутатора;
- Командные режимы CLI;
- Синтаксис команд CLI;
- Горячие клавиши;
- История команд.

5.1.1 Команды CLI для доступа к коммутатору

Команды CLI предоставляет пользовательский интерфейс для управления коммутатором. Пользователи могут получить доступ к интерфейсу командной строки коммутатора через два типа терминалов: Консольный порт (Console port) и Telnet.

5.1.2 Доступ к CLI через Консольный порт

Порядок настройки:

Шаг 1. Подключите рабочую станцию (терминал или компьютер, на котором установлено программное обеспечение эмуляции терминала) к Консольному порту на коммутаторе. Как показано на следующем рисунке 1.

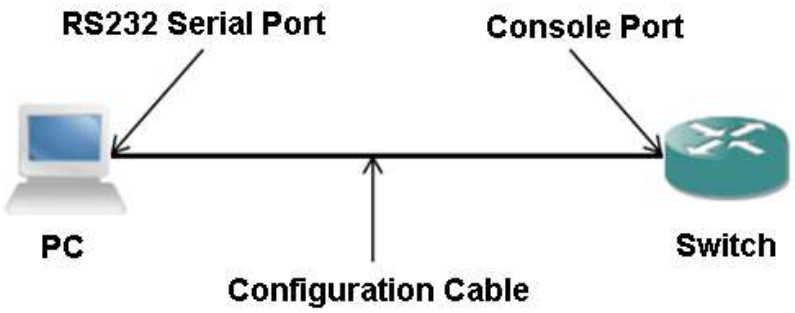

Рисунок 1 – Подключение рабочей станции

Шаг 2. Настройте рабочую станцию следующим образом (Рисунок 2):
Baud rate: 115200
Data bits: 8
Parity: None
Stop bit: 1
Flow control: off

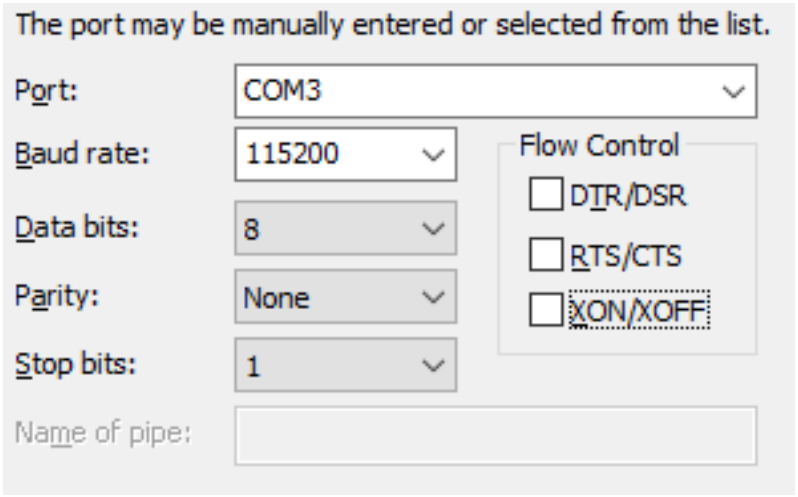

Рисунок 2 – Настройка рабочей станции

Шаг 3. Включите коммутатор. После установки соединения появится пригласительная строка «SWITCH>».

Далее необходимо ввести команду «**enable**» и пароль «**admin**». После успешного входа отобразится строка «SWITCH#». Как показано на следующем рисунке 3.

```
********************************************************************************
*    Welcome to use our product of VA2200-48P-6X.                              *
*    Copyright (c) 2024 Vector Technologies, LLC..                             *
*    ALL RIGHTS RESERVED.                                                      *
*    No decompiling or reverse-engineering without the owner's permission.     *
********************************************************************************

Access via Console use vty[0] succeed

Please press Enter to continue.
```

Рисунок 3 – Включение коммутатора

5.1.3 Доступ к CLI через Telnet

Доступ к коммутатору осуществляется через Ethernet порт. IP-адрес коммутатора по умолчанию — 192.168.1.240.

Порядок настройки:

Шаг 1. Подключите Ethernet порт PC к порту коммутатора с помощью Ethernet кабеля. Как показано на следующем рисунке 4.

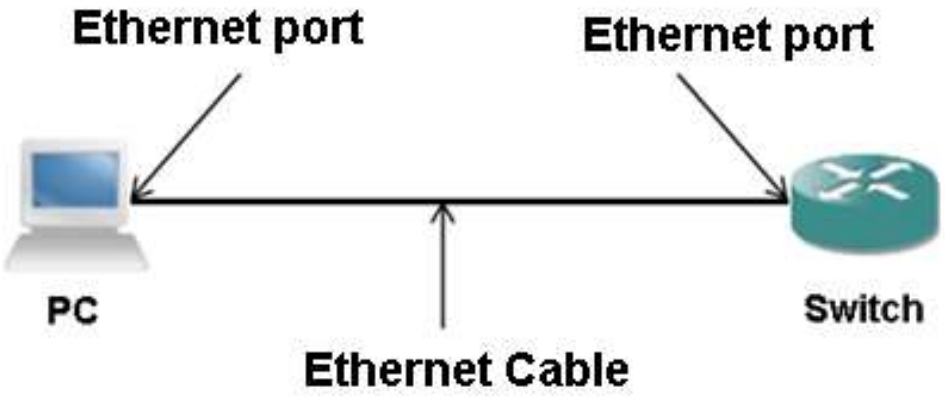

Рисунок 4 – Подключение Ethernet порт PC к порту коммутатора

Шаг 2. Настройте IP-адрес для Ethernet порта PC. IP-адрес должен находиться в диапазоне 192.168.1.0/24 (например, IP-адрес 192.168.1.100). Вы можете проверить, есть ли соединение между PC и коммутатором, с помощью команды Ping.

Шаг 3. Запустите утилиту telnet (можно использовать встроенную утилину telnet операционной системы компьютера) и подключитесь к IP-адресу коммутатора (введите “telnet 192.168.1.240”). Как показано на следующем рисунке 5.

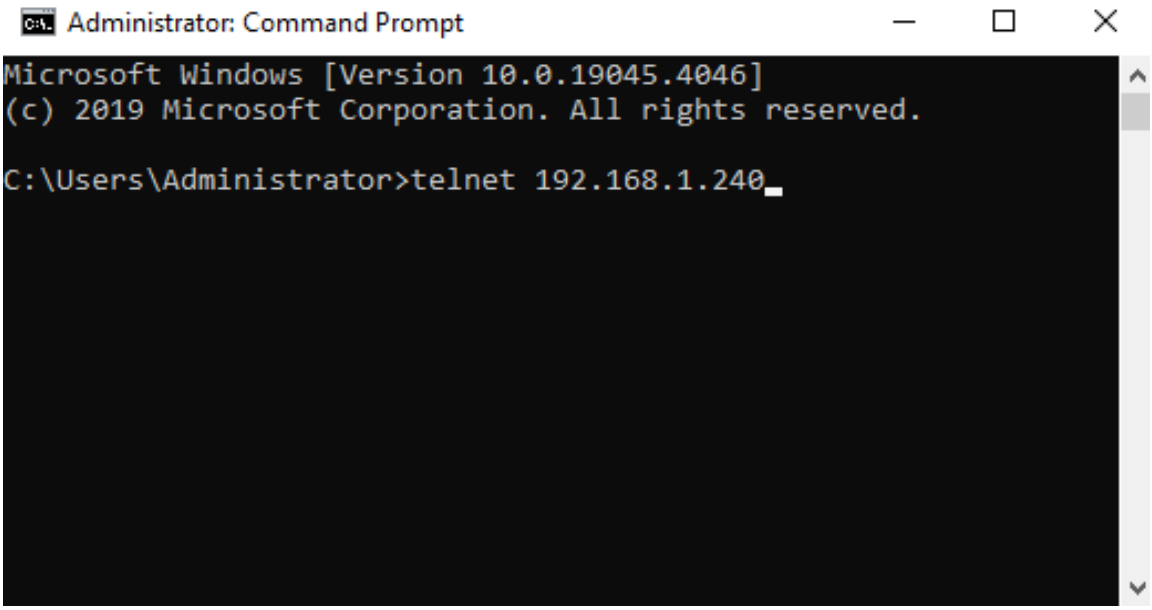

Рисунок 5 – Подключение к коммутатору по IP

Шаг 4. После подключения к коммутатору по telnet вы можете войти в рабочий интерфейс CLI, используя имя пользователя и пароль. Имя пользователя и пароль по умолчанию — **admin** и **admin**.

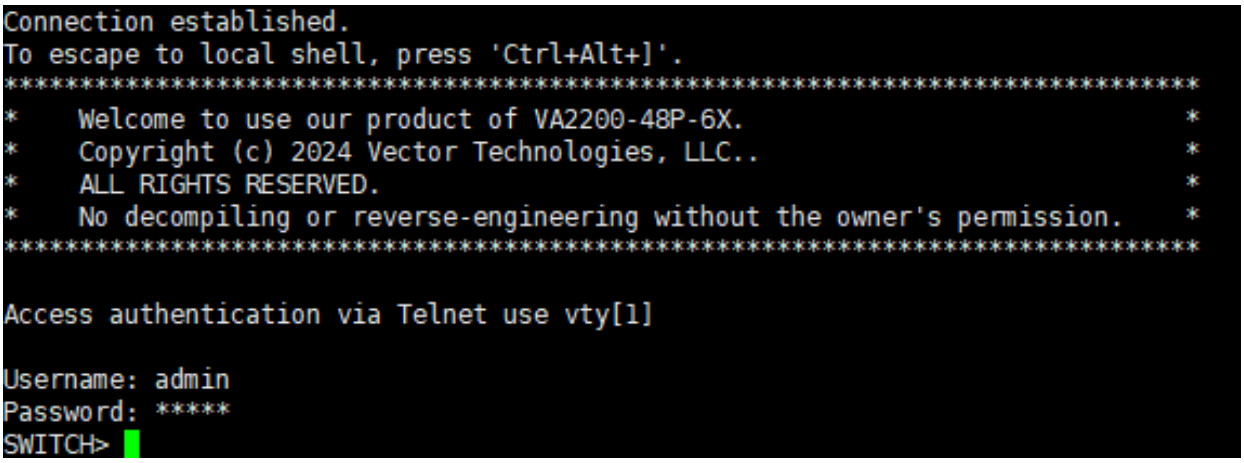

Рисунок 6 – Вход в рабочий интерфейс

Примечание - IP-адрес порта коммутатора создается на основе интерфейсов VLAN уровня 3. Прежде чем получить доступ к коммутатору, необходимо установить IP-адрес интерфейса VLAN. IP-адрес по умолчанию для VLAN 1 — 192.168.1.240. IP-адрес интерфейсов VLAN можно настроить через консольный порт.

5.2 Введение в режимы CLI

5.2.1 Функции режима CLI

Существует две основные функции режима CLI. Такие как:

1. Удобство классификации пользователей.

Предотвращение несанкционированного использования CLI неавторизованными пользователями.

Обычные пользователи могут просматривать только некоторые рабочие состояния и использовать только команды просмотра информации о коммутаторе.

Пользователи с правами на внесение изменений могут не только просматривать рабочее состояние, но и настраивать коммутатор, изменяя его поведение.

2. Удобство настройки.

Существует множество настроек коммутатора. Если все настройки вынести в один режим, это будет очень неудобно для пользователей. Поэтому в CLI установлено несколько режимов, группирующих похожие команды в один режим, чтобы облегчить понимание и использование пользователем. Например, команды, связанные с VLAN, помещаются в режим настройки VLAN, а команды, связанные с интерфейсом, помещаются в режим настройки интерфейса.

5.2.2 Идентификация режима CLI

Приветственная строка CLI является идентификатором режима CLI, благодаря ней, пользователи могут узнать текущий режим.

Приветственная строка CLI состоит из двух частей: одна часть идентифицирует хост, а другая часть определяет режим.

Хост-часть приветственной строки CLI использует имя хоста системы, которое можно настроить и по умолчанию оно равно SWITCH.

Часть строки, отвечающая за режим CLI, не настраивается. Каждому режиму соответствует своя строка, причем некоторые строки режима являются фиксированными, а другие — переменными. Например, строка режима для режима конфигурации фиксирована, а строка режима для режима конфигурации интерфейса является переменной.

Например:

Приветственная строка CLI “SWITCH#” указывает на привилегированный режим, где “SWITCH” идентифицирует имя хоста, а “#” идентифицирует режим.

Приветственная строка CLI “SWITCH(config)#” указывает на режим конфигурации, где “SWITCH” идентифицирует имя хоста, а “(config)#” идентифицирует режим.

Приветственная строка CLI “SWITCH(Vlan-interface1)#” указывает режим настройки интерфейса VLAN, в частности настройку VLAN 1, где “SWITCH” идентифицирует имя хоста, а “(Vlan-interface1)#” идентифицирует режим виртуального интерфейса VLAN 1.

5.2.3 Классификация режимов CLI

Режимы CLI обычно делятся на три категории: обычный режим, режим глобальной конфигурации и под режим конфигурации, а подрежим конфигурации состоит из множества различных режимов CLI.

Привилегированный режим при входе в систему через Telnet или консоль после ввода “enable”. Введите команду “**configure**” в привилегированном режиме, чтобы войти в режим глобальной конфигурации. В режиме глобальной конфигурации можно вводить различные команды для входа в различные подрежимы конфигурации.

Таблица 1 - Список режимов CLI

Режим	Описание	Prompt	Команда для входа в режим
Привилигированный режим	Помимо предоставления команд для просмотра информации о состоянии коммутатора, он также предоставляет такие команды, как отладка и настройка.	SWITCH#	Введите “enable” в режиме «>» или первый режим через telnet.
Режим глобальной конфигурации	Предоставляет универсальные команды, которые невозможно реализовать в подрежиме конфигурации,	SWITCH(config)#	Введите команду “configure” в режме «#»

	например настройку команд статической маршрутизации.		
Режим настройки порта	Предоставляет команды настройки портов.	SWITCH(config-eth1/0/1)#	Введите “interface <PORTTYPE> <INTERFACE> ” в режиме «config».
Режим конфигурации виртуального интерфейса	Предоставляет команды настройки для виртуальных интерфейсов VLAN.	SWITCH(Vlan-interface1)#	Введите “interface vlan-interface <index>” в режиме «config».
Режим VLAN	Предоставляет команды настройки для VLAN.	SWITCH(Vlan2)#	Введите “vlan <vlan-id>” в режиме «config».
Режим пула адресов	Предоставляет команды настройки для пула адресов DHCP.	SWITCH(ip-pool-aaa)#	Введите “ip dhcp server ip-pool <POOLNAME> ” в режиме «config».
Режим ACL	Предоставляет команды настройки для ACL.	SWITCH(acl-basic-2000)#	Введите “acl number <index> name <NAME>” в режиме «config».
Режим агрегации	Предоставляет команды настройки для интерфейсов агрегации.	SWITCH(config-lag1)#	Введите “interface lag <index>” в режиме «config».
Режим OSPF	Предоставляет команды настройки для OSPF.	SWITCH(ospf-router)#	Введите “router ospf” в режиме «config».
Режим RIP	Предоставляет команды настройки для RIP.	SWITCH(rip-router)#	Введите “router rip” в режиме «config».

5.3 Введение в Синтаксис команд

5.3.1 Состав команды

Команды CLI состоят из ключевых слов и параметров. Первое слово должно быть ключевым словом, а последующие слова могут быть либо ключевыми словами, либо параметрами, которые могут появляться поочерёдно.

Команда должна иметь ключевые слова и может не иметь параметров. Например, команда “**save**” состоит всего из одного ключевого слова без параметров. Команда «show running-config» состоит из двух ключевых слов и а ней нет параметров; команда “vlan <vlan-id>” состоит из одного ключевого слова и одного параметра; команда “ acl number <index> name <NAME>” имеет два ключевых слова и два параметра, при этом ключевые слова и параметры появляются поочередно.

5.3.2 Правила Синтаксиса команд

При описании команд в данном руководстве используются следующие правила:

1. Ключевые слова представлены непосредственно словами.

Например: show running.

2. Параметры заключены в <>.

Например: vlan <vlan-id>

3. Если параметр не необязательный, за ним следует <cr> (Enter).

4. Если несколько ключевых слов или параметров требуют выбора одного, они заключаются в круглые скобки (), и разделены |.

Например, для команды с несколькими обязательными ключевыми словами: "qos queue-scheduler (wrr | hq-wrr)", где либо "wrr", либо "hq-wrr" должен быть выбран. Для команд с несколькими обязательными параметрами: "no arp {aging-time | <ip-address>}".

5. Параметры описываются одним или несколькими словами, разделенными знаком “-“, причем каждое слово пишется строчными буквами.

Например, такие параметры, как <vlan-id>, <if-name>, <router-id>, <count>, и др.

5.3.3 Сокращение команд

Пользователи могут сокращать ключевые слова команд при вводе команд в интерфейсе CLI. CLI поддерживает автоматическое дополнение:

если входные данные соответствуют уникальному префиксу ключевого слова, они автоматически дополняются этим ключевым словом при выполнении команды, либо по нажатию клавиши “TAB”. Эта функция значительно упрощает использование CLI, позволяя пользователям вводить меньше символов для выполнения команды. Например, команду "show running" можно сократить до "sh ru".

5.3.4 Справка по синтаксису

CLI предоставляет справку по синтаксису, поддерживающую справку для каждого уровня команды и параметра, описанную следующим образом:

1. Ввод вопросительного знака “**?**” в определенном режиме CLI позволяет вывести список всех доступных команд в этом режиме вместе с их описаниями.

Например:

" SWITCH(config)#?".

2. Ввод первой части команды, затем пробела и затем "?" выведет список всех ключевых слов или параметров следующего уровня вместе с их описаниями.

Например:

" SWITCH(config)#show ?".

3. Ввод неполного ключевого слова, а затем "?" выведет список всех ключевых слов, соответствующих входному префиксу, вместе с их описаниями.

Например:

"Switch#show r?".

4. Введя начальную часть команды, за которой следует пробел, а затем нажав клавишу Tab, вы увидите список всех ключевых слов следующего уровня. Если следующий уровень является параметром, он не будет указан.

5. Ввод неполного ключевого слова и последующее нажатие клавиши Tab приведет к автозаполнению, если только одно ключевое слово соответствует входному префиксу, в противном случае на терминале будут перечислены все соответствующие ключевые слова.

5.3.5 Сообщение об ошибке в командной строке

Если введенная команда не проходит проверку синтаксиса, на терминале отобразится сообщение об ошибке. Распространенные сообщения об ошибках показаны в таблице ниже.

Таблица 2 – Распространённые ошибки

Сообщение об ошибке	Причина ошибки
Invalid input или Unknown command или Incorrect string	Нет соответствующих ключевых слов. Ввод параметров неверен. Введено слишком много ключевых слов или параметров.
Command incomplete	Введена неполная команда. Ключевое слово или параметр не введено.
Ambiguous command	Введено неполное ключевое слово. Несколько ключевых слов соответствуют входному префиксу.

5.4 Горячие клавиши командной строки

5.4.1 Сочетания клавиш редактирования строк

Команда CLI поддерживает функцию сочетания клавиш редактирования строк, которая облегчает ввод и редактирование команд CLI. Пользователи могут использовать сочетания клавиш для редактирования строк, чтобы ускорить ввод команд при вводе или редактировании команд. В следующей таблице перечислены все варианты редактирования строк и их реализованные функции:

Таблица 3 – Варианты редактирования строк

Сочетания клавиш	Функция
Ctrl+p or ↑ key	Предыдущая команда
Ctrl+n or ↓ key	Следующая команда
Ctrl+u	Удалить всю строку
Ctrl+a	Вернуть курсор в начало строки
Ctrl+f or → key	Переместите курсор на один символ вправо
Ctrl+b or ← key	Переместите курсор на один символ влево
Ctrl+d	Удалить символ, на котором находится курсор
Ctrl+h	Удалить символ перед курсором
Ctrl+k	Удалить все символы до и после курсора
Ctrl+w	Удалить все символы перед курсором
Ctrl+e	Переместить курсор в конец строки
Ctrl+c	Прервать, не выполнять команду. В режиме глобальной конфигурации или подрежиме конфигурации интерфейс командной строки возвращается в привилегированный режим. В обычном или привилегированном режиме режим CLI остается неизменным, но CLI начинает новую строку.
Ctrl+z	То же самое с функцией клавиши пробела.
Tab	Используйте эту клавишу при вводе неполных ключевых слов. Если ключевое слово соответствует входному префиксу, оно автоматически полностью заполнится. А если входному префиксу соответствует несколько ключевых слов, перечислятся все соответствующие ключевые слова. А если совпадения ключевых слов нет, этот ключ не ответит.

5.5 История команд

CLI поддерживает функцию записи истории, которая может запоминать последние введеные команды пользователя и сохранять самые последние введенные пользователем команды. Вы можете использовать “**show history**” для отображения уже введенных команд или использовать клавиши Ctrl+p, Ctrl+n или ↑, ↓ для выбора команд из истории.

5.6 Таблица команд (Описание)

В следующих главах каждая команда будет объяснена в виде таблицы, описание ее параметров приведено ниже:

Таблица 4 – Параметры таблицы описания команд

Описание	1.	“*”означает, что команда есть в текущем режиме и во всех режимах выше.
	2.	“√”означает, что эта команда существует только в выбранном режиме.
	3.	“#” - привилигированный режим
	4.	“(config)#” - режим глобальной конфигурации
	5.	“{ x | y | ... }” означает, что необходимо выбрать один из двух или более элементов.
	6.	“[x | y | ...]” означает, что можно выбрать один из двух или более элементов.
	7.	*курсивом* выделены параметры команды (части команды, которые необходимо заменить фактическими значениями).
	8.	**Жирным** шрифтом обозначены ключевые слова команды (части команды, которые остаются неизменными и должны быть введены).

6 УПРАВЛЕНИЕ СИСТЕМОЙ

В этой главе представлено подробное описание команд CLI:

– Команды глобального управления;
– Управление системой;
– Управление пользователями;
– Управление системным временем;
– Управление системным журналом.

6.1 Команды глобального управления

Команды глобального управления обеспечивают операции управления каталогами, справочную информацию и историю выполнения.

6.1.1 Список команд глобального управления

Таблица 5 – Список команд глобального управления

Команды	Описание	Режим
configure	В режим глобальной конфигурации.	“#”
exit	Вернуться в предыдущий режим	*
show history	Отображение информации об истории ввода (максимум 20 командных исторических операций).	*
clear	Очистить содержимое экрана	*
list	Просмотр списка доступных команд в текущем режиме, включая ключевые команды и параметры команд.	*
home	Выйти из пользовательского режима	*

6.2 Управление системой

6.2.1 Конфигурация системных функций

Таблица 6 - Конфигурация системных функций

Команды	Описание	Режим
save	Сохранить текущую конфигурацию на Flash	“(config)#”
factory-defaults	Восстановить заводские настройки и перезагрузить коммутатор	“(config)#”
reboot	Перезагрузить систему	“#”
show running-config	Показать текущую конфигурацию	“#”
show startup-config	Показать конфигурацию запуска	“#”

hostname HOSTNAME	Настроить имя хоста (имя системы), можно использовать цифры, буквы и символы - _ .	“(config)#”
show current	Показать текущую конфигурацию текущего режима	*
cfg download ftp ip <ip-address> user <user-name> password <pswd> filename <filename>	Импорт файлов конфигурации через FTP	“(config)#”
download tftp ip <ip-address> filename <filename>	Импорт файлов конфигурации с помощью инструмента TFTP	“(config)#”
cfg upload ftp ip <ip-address> user <user-name> password <pswd> filename <filename>	Экспорт файлов конфигурации через FTP	“(config)#”
upload tftp ip <ip-address> filename <filename>	Экспорт файлов конфигурации через TFTP	“(config)#”

6.2.2 Информация о системе

Таблица 7 – Информация о системе

Команды	Описание	Режим
show version	Показать полную информацию об устройстве	“#”
show memory-usage	Показать % использованной памяти	“#”
show cpu-usage	Показать загрузку CPU	“#”
show mem-cpu-usage detail	Показать подробную информацию об использовании памяти и CPU	“#”

6.2.3 Обновление системы

Таблица 8 – Обновление системы

Команды	Описание	Режим
upgrade master ftp ip <ip-address> user <user-name> password <pswd> filename <filename>	Обновление через FTP	“(config)#”
upgrade master tftp ip <ip-address> filename <filename>	Обновление с помощью TFTP	“(config)#”
upgrade master local <file-name>	Обновление через локальный файл	“(config)#”
upload ftp ip <ip-address> user <user-name> password <pswd> filename <filename>	Загрузка файлов через FTP	“(config)#”

upload master tftp ip <ip-address>filename <filename>	Загрузка файлов с помощью TFTP	“(config)#”
download ftp ip <ip-address> user <user-name> password <pswd> filename <filename>	Скачивание файлов через FTP	“(config)#”
download master tftp ip <ip-address>filename <filename>	Скачивание файлов через TFTP	“(config)#”
show filelist	Показать список локальных файлов	“(config)#”
show upgrade master status	Показать статус обновления	“#”

6.2.4 Конфигурация входа

Таблица 9 – Конфигурация входа

Команды	Описание	Режим
[no] local-user <user-name> service-type {http | ssh | telnet}	Установить/отменить права доступа пользователей	“(config)#”
local-user authentication-mode web {none | password}	Настройка методов аутентификации веб-пользователей	“(config)#”
local-user authentication-mode vty {none | password}	Настройка методов аутентификации пользователя telnet	“(config)#”
[no] local-user exec-timeout web <1-60>	Установка времени ожидания веб-пользователя	“(config)#”
[no] local-user exec-timeout vty <1-60>	Установка времени ожидания пользователя Telnet	“(config)#”

6.2.5 Системные инструменты

Таблица 10 – Системные инструменты

Команды	Описание	Режим
ping <ip-address>	Пинг IP-адреса	“#”
telnet <ip-address>	Удаленное подключение к устройству с помощью telnet	“(config)#”

6.3 Управление пользователями

6.3.1 Уровень привилегий пользователя

По умолчанию в системе имеется учетная запись суперадминистратора, и можно добавить до 4 пользователей. Учетная запись суперадминистратора не может быть удалена, но ее пароли и имя могут быть изменены.

Таблица 11 – Описание параметра

Параметр	Описание
NAME	Имя, строковый формат, допустимые символы A–Z, a–z, 0–9, _ длиной 1-32 символа.
PASSWORD	Пароль: любой печатный символ ASCII длиной от 1-16 символа.
administrator|normal	Настройка уровня пользователя, поддерживает 2 уровня: 1. administrator: со всеми разрешениями и неограниченной конфигурацией. 2. normal: только чтение, могут только просматривать конфигурацию, не могут изменять или удалять конфигурации. **Примечание**: при создании нового пользователя без установки уровня по умолчанию используется уровень administrator.
enable|disable	Настройка статуса пользователя enable: разрешить вход disable: отключить вход в систему; **Примечание:** при создании нового пользователя без установки статуса пользователя по умолчанию включается.

6.3.2 Список команд управления пользователями

Таблица 12 – Список команд управления пользователями

Команды	Описание	Режим
[no] ssh	Вкл/выкл SSH	“(config)#”
local-user <user-name> level {administrator | normal}	Создать/изменить конфигурацию пользователя	“(config)#”
no local-user <user-name>	Удалить пользователя	“(config)#”
local-user <user-name> level {administrator | normal}	Изменить уровень пользователя	“(config)#”
[no] local-user <user-name> service-type {http | ssh | telnet}	Установить/отменить права доступа пользователя	“(config)#”
local-user authentication-mode web {none | password}	Настроить метод аутентификации веб-пользователя	“(config)#”
local-user authentication-mode vty {none | password}	Настроить метод аутентификации пользователя Telnet	“(config)#”
[no]local-user exec-timeout web <1-60>	Установить временя ожидания веб-пользователя	“(config)#”
[no]local-user exec-timeout vty <1-60>	Установить время ожидания пользователя Telnet	“(config)#”
show local-user information	Показать текущую информацию о пользователях	“#”
show local-user authentication-mode	Показать режим аутентификации	“#”
show local-user exec-timeout	Показать текущее время ожидания пользователя	“#”

6.4 Управление системным временем

6.4.1 Список команд управления системным временем

Таблица 13 - Список команд управления системным временем

Команды	Описание	Режим
set-clock <date> <time>	Установить системное временя	“(config)#”
show clock	Показать системное время	“#”

6.5 Управление системным журналом

Модуль системного журнала является важной частью коммутатора, который используется для записи рабочего состояния, ненормального поведения и поведения пользователя в системе. Он помогает администраторам своевременно понимать и контролировать рабочее состояние системы.

Модуль системного журнала контролирует всю информацию журнала из работающих модулей системы, собирает, классифицирует, хранит и отображает информацию журнала для вывода.

Существует два способа хранения журналов:

– Сохранение в памяти;

– сохранение на сервере.

6.5.1 Описание уровней системного журнала

Таблица 14 – Описание уровней системного журнала

Параметр	Описание
<0-7>	Уровень журнала по умолчанию — 7. Чем меньше число, тем выше уровень. Описание каждого уровня ниже: 0 – Аварийная ситуация (Система не работоспособна) 1 – Тревога (Необходимо срочное вмешательство) 2 – Критический (Критические события) 3 – Ошибка (Сообщения о ошибках) 4 – Предупреждение (Всевозможные предупреждения) 5 – Уведомление (Различные важные уведомления) 6 – Информация (Информационные сообшения) 7 – Отладка (Отладочые сообщения)

6.5.2 Список команд управления системным журналом

Таблица 15 – Список команд управления системным журналом

Команды	Описание	Режим
show logging message	показать сообщение журнала	“#”
logging enable	включить ведение журнала	“(config)#”
logging disable	ведение журнала отключено	“(config)#”
logging console level <0-7>	Установить уровень журнала для вывода на консольный порт	“(config)#”
logging buffered level <0-7>	Установить уровень журнала для вывода в буфер	“(config)#”
logging host A.B.C.D level <0-7>	Установить уровень журнала для вывода на удаленный сервер	“(config)#”
logging syslog-port (default | port) (514|<1024-65534>)	Установить порт удаленного сервера системного журнала Порт по умолчанию — 514. Порт можно изменить на 1024 - 65534.	“(config)#”
no logging host	Запретить удаленные серверы системного журнала	“(config)#”
show logging config	Показать конфигурацию системного журнала	“#”
clear logging message	Очистить системные журналы	“(config)#”

7 ВИРТУАЛЬНЫЙ IP-ИНТЕРФЕЙС

В этой главе представлено подробное описание команд CLI:

- Конфигурация виртуального IP-интерфейса;
- конфигурация таблицы маршрутизации;
- таблица ARP.

7.1 IP-интерфейс

В коммутаторе каждый интерфейс уровня 3 привязан к VLAN, поэтому интерфейсы уровня 3 также называются IP-интерфейсами VLAN. Создание и удаление IP-интерфейсов VLAN выполняется вручную. Хотя коммутатор может поддерживать до 4094 сетей VLAN, он может установить **не более 8 IP-интерфейсов VLAN**. L3 интерфейсы могут быть созданы на основе требований пользователя и удалены пользователем вручную.

На IP-интерфейсах VLAN пользователи могут настроить IP-адрес и указать маску подсети. Прежде чем настраивать IP-адрес, пользователям необходимо создать VLAN и добавить в него соответствующие порты. По

умолчанию коммутатор имеет IP-интерфейс для VLAN1, на этом интерфейсе настроен IP-адрес **192.168.1.240/24.** Пользователь также может изменить IP-адрес интерфейса VLAN1.

7.1.1 Конфигурация виртуального интерфейса

Таблица 16 – Конфигурация виртуального интерфейса

Команды	Описание	Режим
[no] interface vlan-interface <vlan-id>	Удалить/создать виртуальный интерфейс	“(config)#”
interface vlan-interface IPIFNAME	Войти в режим настройки интерфейса уровня 3	“(config)#”
ip address <ip-address> <ip-mask>	Добавить/изменить IP-адрес	“(Vlan-interface1)#”
no ip address <ip-address> <ip-mask>	Удалить IP-адрес	“(Vlan-interface1)#”
ip address <ip-address> <ip-mask> secondary	Добавить дополнительный IP-адрес	“(Vlan-interface1)#”
[no] ip address dhcp-alloc	Отключить/включить DHCP-клиент	“(Vlan-interface1)#”
[no] ip dhcp client identifier (string | hex) <1-63><1-126>	Отменить/настроить опцию 61	“(Vlan-interface1)#”
ip dhcp client debug (all | none)	Включить отладочную информацию DHCP	“(config)#”
show interface vlan-interface all	Показать информацию о конфигурации для всех интерфейсов уровня 3	“#”
show ip dhcp client	Показать информацию о состоянии DHCP-клиентов	“#”

7.2 Управление статической маршрутизацией

Статическая маршрутизация — это информация о маршрутизации, настроенная вручную пользователем. Если топология или состояние канала сети были изменены, администраторам необходимо вручную изменить информацию о статической маршрутизации в таблице маршрутизации. Информация о статической маршрутизации по умолчанию является конфиденциальной и не будет передаваться другим маршрутизаторам. Конечно, администраторы также могут настроить распространение

информации о маршрутизации. Статическая маршрутизация обычно подходит для относительно простых сетевых сред, где сетевые администраторы могут легко понять топологию сети и установить правильную информацию о маршрутах.

7.2.1 Настройка статической маршрутизации

Таблица 17 – Настройка статической маршрутизации

Команды	Описание	Режим
[no] ip route-static <ip-address> <ip-mask> (<next-hop-address> | reject | blackhole) [des]	Удалить/добавить запись маршрутизации	“(config)#”
clear ip route-static (all | static | reject | blackhole)	Удалить таблицу маршрутизации в зависимости от типа	“(config)#”

7.2.2 Показать информацию о маршрутизации

Таблица 18- Отображение информации о маршрутизации

Команды	Описание	Режим
show ip routing-table (all | static | direct | reject | blackhole)	Отобразить таблицы маршрутизации в зависимости от типа	“#”
show ip routing-table <ip-address> <ip-mask>	Отобразить таблицы маршрутизации на основе сегмента сети	“#”

7.3 ARP (Address Resolution Protocol)/ Протокол разрешения адресов

7.3.1 Конфигурация ARP

Таблица 19 – Конфигурация ARP

Команды	Описание	Режим
arp static <ip-address> <mac-address> vlan <vlan-id> interfaces <interface-type> <interface-number>	Добавить ARP	“(config)#”
no arp <ip-address>	Удалить ARP	“(config)#”
clear arp (all | dynamic | static | vlan <vlan-id>)	Удалить таблицу ARP согласно указанному типу	“(config)#”
[no] arp aging-time <aging-time>	Восстановить/установить время устаревания ARP	“(config)#”

arp auto renew (disable | enable)	Отключить/включить автоматическое продление ARP	“(config)#”
gratuitous-arp-sending enable interval <timer>	Включить функцию Gratuitous ARP	“(config)#”
gratuitous-arp-sending disable	Отключить отправку Gratuitous ARP	“(config)#”
gratuitous-arp-learning (enable | disable)	Включить/отключить изучение Gratuitous ARP	“(config)#”

7.3.2 Показ ARP

Таблица 20 – Показ ARP

Команды	Описание	Режим
show arp (all | dynamic | static)	Показать таблицу ARP в зависимости от типа	“#”
show arp vlan <vlan-id >	Показать таблицу ARP на основе VLAN	“#”
show arp ip-address <ip-address>	Показать таблицу ARP на основе IP-адреса	“#”
show arp aging-time	Показать время устаревания ARP	“#”
show arp auto renew	Показать функцию автоматического продления ARP	“#”

7.4 Пример настройки

1. Сетевые требования

— Настройте функцию статической маршрутизации, чтобы получить связь между хостами.

— Топология сети:

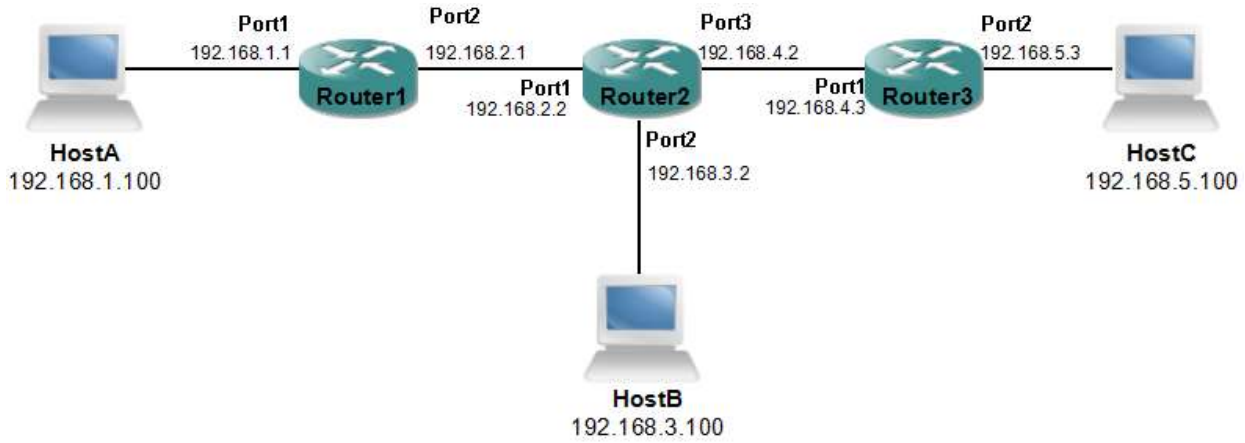

Рисунок 7 – Топология сети

2. План конфигурации

— Настроить виртуальные интерфейсы для Router1, Router2 и Router3.

— Настроить статическую маршрутизацию

3. Шаги конфигурации

（1）Настройка адреса виртуальных интерфейсов.

```
# Настройка Router1
Router1(config)# vlan 2
Router1(config)# interface ethernet 1/0/2
Router1(config-eth1/0/2)# switchport access vlan 2
Router1(config-eth1/0/2)# interface vlan-interface 1
Router1(Vlan-interface1)# ip address 192.168.1.1 255.255.255.0
Router1(Vlan-interface1)# interface vlan-interface 2
Router1(Vlan-interface2)# ip address 192.168.2.1 255.255.255.0
# Настройка Router2
Router2(config)# vlan 2-3
Router2(config)# interface ethernet 1/0/2
Router2(config-eth1/0/2)# switchport access vlan 2
Router2(config-eth1/0/2)# interface ethernet 1/0/3
Router2(config-eth1/0/3)# switchport access vlan 3
Router2(config-eth1/0/3)# interface vlan-interface 1
Router2(Vlan-interface1)# ip address 192.168.2.2 255.255.255.0
Router2(Vlan-interface1)# interface vlan-interface 2
Router2(Vlan-interface2)# ip address 192.168.3.2 255.255.255.0
Router2(Vlan-interface2)# interface vlan-interface 3
Router2(Vlan-interface3)# ip address 192.168.4.2 255.255.255.0
# Настройка Router3
Router3(config)# vlan 2
Router3(config)# interface ethernet 1/0/2
Router3(config-eth1/0/2)# switchport access vlan 2
Router3(config-eth1/0/2)# interface vlan-interface 1
Router3(Vlan-interface1)# ip address 192.168.4.3 255.255.255.0
Router3(Vlan-interface1)# interface vlan-interface 2
Router3(Vlan-interface2)# ip address 192.168.5.3 255.255.255.0
```

（2）Настройка статической маршрутизации.

```
# Настройка Router1
Router1(config)# ip route-static 192.168.3.0 255.255.255.0 192.168.2.2
Router1(config)# ip route-static 192.168.4.0 255.255.255.0 192.168.2.2
Router1(config)# ip route-static 192.168.5.0 255.255.255.0 192.168.2.2
# Настройка Router2
Router2(config)# ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
Router2(config)# ip route-static 192.168.5.0 255.255.255.0 192.168.4.3
# Настройка Router3
```

Router3(config)# ip route-static 192.168.1.0 255.255.255.0 192.168.2.2
Router3(config)# ip route-static 192.168.2.0 255.255.255.0 192.168.2.2
Router3(config)# ip route-static 192.168.3.0 255.255.255.0 192.168.2.2

4. Проверка конфигурации

Просмотр настроек всех виртуальных интерфейсов на Router1, Router2 и Router3.

Просмотр настроек виртуальных интерфейсов на Router1.

Router1(config)# show interface vlan-interface all

Vlan-interface 1
Hardware Address : 00:00:00:00:11:00
Mtu : 1500
Current state :UP
Protocol :Static
Internet Address : 192.168.1.1/255.255.255.0
Input: 2458bytes 40packets 0drops 40multecasts
Output: 0bytes 0packets 0drops
Dhcp-Relay enable: Disable
Dhcp-Relay giaddr:
Dhcp-Relay Option82: Disable
Dhcp-Relay Option82 Action: Keep
Dhcp-Relay Option82 Circuit-ID:
Dhcp-Relay Option82 Remote-ID:
Ospf Config
Ospf Mtu Ignore : Disable
Ospf Cost : 10
Ospf Priority : 1

Vlan-interface 2
Hardware Address : 00:00:00:00:11:00
Mtu : 1500
Current state :UP
Protocol :Static
Internet Address : 192.168.2.1/255.255.255.0
Input: 252bytes 4packets 0drops 4multecasts
Output: 0bytes 0packets 0drops
Dhcp-Relay enable: Disable
Dhcp-Relay giaddr:
Dhcp-Relay Option82: Disable
Dhcp-Relay Option82 Action: Keep
Dhcp-Relay Option82 Circuit-ID:
Dhcp-Relay Option82 Remote-ID:
Ospf Config

Ospf Mtu Ignore : Disable
Ospf Cost : 10
Ospf Priority : 1
Просмотр настроек виртуальных интерфейсов на Router2.
Router2(config)# show interface vlan-interface all

Vlan-interface 1
Hardware Address : 00:00:00:00:00:77
Mtu : 1500
Current state :UP
Protocol :Static
Internet Address : 192.168.2.2/255.255.255.0
Input: 966bytes 17packets 0drops 14multecasts
Output: 0bytes 0packets 0drops
Dhcp-Relay enable: Disable
Dhcp-Relay giaddr:
Dhcp-Relay Option82: Disable
Dhcp-Relay Option82 Action: Keep
Dhcp-Relay Option82 Circuit-ID:
Dhcp-Relay Option82 Remote-ID:
Ospf Config
Ospf Mtu Ignore : Disable
Ospf Cost : 10
Ospf Priority : 1

Vlan-interface 2
Hardware Address : 00:00:00:00:00:77
Mtu : 1500
Current state :UP
Protocol :Static
Internet Address : 192.168.3.2/255.255.255.0
Input: 0bytes 0packets 0drops 0multecasts
Output: 0bytes 0packets 0drops
Dhcp-Relay enable: Disable
Dhcp-Relay giaddr:
Dhcp-Relay Option82: Disable
Dhcp-Relay Option82 Action: Keep
Dhcp-Relay Option82 Circuit-ID:
Dhcp-Relay Option82 Remote-ID:
Ospf Config
Ospf Mtu Ignore : Disable
Ospf Cost : 10
Ospf Priority : 1

Vlan-interface 3

Hardware Address : 00:00:00:00:00:77
Mtu : 1500
Current state :UP
Protocol :Static
Internet Address : 192.168.4.2/255.255.255.0
Input: 0bytes 0packets 0drops 0multecasts
Output: 0bytes 0packets 0drops
Dhcp-Relay enable: Disable
Dhcp-Relay giaddr:
Dhcp-Relay Option82: Disable
Dhcp-Relay Option82 Action: Keep
Dhcp-Relay Option82 Circuit-ID:
Dhcp-Relay Option82 Remote-ID:
Ospf Config
Ospf Mtu Ignore : Disable
Ospf Cost : 10
Ospf Priority : 1
Просмотр настроек виртуальных интерфейсов на Router3.
Router3(config)# show interface vlan-interface all

Vlan-interface 1
Hardware Address : C8:C5:0E:01:33:01
Mtu : 1500
Current state :UP
Protocol :Static
Internet Address : 192.168.4.3/255.255.255.0
Input: 0bytes 0packets 0drops 0multecasts
Output: 0bytes 0packets 0drops
Dhcp-Relay enable: Disable
Dhcp-Relay giaddr:
Dhcp-Relay Option82: Disable
Dhcp-Relay Option82 Action: Keep
Dhcp-Relay Option82 Circuit-ID:
Dhcp-Relay Option82 Remote-ID:
Ospf Config
Ospf Mtu Ignore : Disable
Ospf Cost : 10
Ospf Priority : 1

Vlan-interface 2
Hardware Address : C8:C5:0E:01:33:01
Mtu : 1500
Current state :UP
Protocol :Static
Internet Address : 192.168.5.3/255.255.255.0

Input: 0bytes 0packets 0drops 0multecasts
Output: 0bytes 0packets 0drops
Dhcp-Relay enable: Disable
Dhcp-Relay giaddr:
Dhcp-Relay Option82: Disable
Dhcp-Relay Option82 Action: Keep
Dhcp-Relay Option82 Circuit-ID:
Dhcp-Relay Option82 Remote-ID:
Ospf Config
Ospf Mtu Ignore : Disable
Ospf Cost : 10
Ospf Priority : 1

Просмотр настроек статической маршрутизации.

Просмотр настроек статической маршрутизации на Router1.
Router1(config)# show ip routing-table all
Total Entry: 5

Destination/MaskProtoNextHopInterfaceDes
192.168.1.0/24 Direct 192.168.1.1Vlanif1
192.168.2.0/24 Direct 192.168.2.1Vlanif2
192.168.3.0/24 Static 192.168.2.2Vlanif2
192.168.4.0/24 Static 192.168.2.2Vlanif2
192.168.5.0/24 Static 192.168.2.2Vlanif2
Просмотр настроек статической маршрутизации на Router2.
Router2(config)# show ip routing-table all
Total Entry: 5

Destination/MaskProtoNextHopInterfaceDes
192.168.1.0/24 Static 192.168.2.1Vlanif1
192.168.2.0/24Direct 192.168.2.2Vlanif1
192.168.3.0/24Direct 192.168.3.2Vlanif2
192.168.4.0/24Direct 192.168.4.2Vlanif3
192.168.5.0/24Static 192.168.4.3Vlanif3
Просмотр настроек статической маршрутизации на Router3.
Router3(config)# show ip routing-table all
Total Entry: 5

Destination/ MaskProtoNextHopInterfaceDes
192.168.1.0/24 Static 192.168.4.2Vlanif1
192.168.2.0/24 Static 192.168.4.2Vlanif1
192.168.3.0/24 Static 192.168.4.2Vlanif1
192.168.4.0/24 Direct 192.168.4.3Vlanif1
192.168.5.0/24 Direct 192.168.5.3Vlanif2

8 КОНФИГУРАЦИЯ ПОРТОВ

В этой главе описывается настройка портов:

– Общая конфигурация портов;
– настройка ограничения скорости порта;
– настройка управления потоком портов;
– просмотр информации о порте.

8.1 Общая конфигурация портов

Администратор контролирует доступ пользователей в соответствии с конфигурацией порта коммутатора. Если пользователям за портом не разрешен доступ к сети, порт можно выключить.

Таблица 21 – Команды для конфигурации портов

Команды	Описание	Режим
shutdown	Отключить порт	“(config-eth)”
no shutdown	Включить порт	“(config-eth)”
description <WORD>	Настроить описание порта	“(config-eth)”
[no] jumboframe <1536-9216>	Запретить/настроить JUMBO-кадры	“(config-eth)”
mdi (across | auto | normal)	Конфигурация MDI Crossline	“(config-eth)”
[no] port-isolate	Отключить/включить изоляцию портов	“(config-eth)”
speed (10 | 100 | 1000 | AUTO)	Настроить скорость порта	“(config-eth)”
duplex (auto | full | half)	Настроить duplex порта	“(config-eth)”

8.2 Конфигурация ограничения скорости порта

Таблица 22 - Ограничения скорости порта

Команды	Описание	Режим
[no] rate-limit (ingress | egress) <target-rate>	Запретить/настроить ограничение скорости порта	“(config-eth)”

8.3 Конфигурация управления потоком порта

Таблица 23 - Управления потоком порта

Команды	Описание	Режим
[no] flow-control	Отключить/включить управление потоком порта	“(config-eth)”

8.4 Показать статус порта

Таблица 24 - Статус порта

Команды	Описание	Режим
show interface statistics <PORTTYPE> <INTERFACE>	Отобразить статистику порта	“#”
clear interface statistics <PORTTYPE> <INTERFACE>	Очистить статистику порта	“(config)#”
show interface switchport <PORTTYPE> <INTERFACE>	Отобразить настройки порта	“#”

9 ТАБЛИЦА MAC-АДРЕСОВ

В этой главе представлено подробное описание команд CLI:

- Определение таблицы пересылки MAC-адресов для коммутаторов;
- принцип изучения MAC-адресов;
- список команд таблицы пересылки MAC-адресов.

9.1 Определение таблицы пересылки MAC-адресов для коммутаторов

Основная функция коммутатора Ethernet — пересылка пакетов на канальном уровне сети передачи данных, что включает в себя направление пакетов на соответствующие порты на основе MAC-адресов назначения. Таблица пересылки MAC-адресов представляет собой таблицу пересылки уровня 2, которая содержит соответствующие взаимосвязи между MAC-адресами и портами. Это фундаментальный компонент коммутаторов Ethernet, обеспечивающий быструю пересылку пакетов уровня 2. Каждая запись в таблице пересылки MAC-адресов содержит следующую информацию:

– MAC адрес назначения;
– Идентификатор VLAN, которому принадлежит порт;
– Номер порта для пересылки на устройство.

Коммутаторы Ethernet используют информацию из записей таблицы MAC-адресов для выполнения пересылки пакетов следующими двумя способами:

– **Режим Unicast:** когда таблица MAC-адресов содержит запись, соответствующую MAC-адресу назначения пакета, коммутатор напрямую отправляет пакет из порта, связанного с этой записью таблицы.

– **Режим Broadcast:** когда коммутатор получает пакет с адресом назначения все “F” (broadcast адрес) или когда в таблице MAC-адресов нет соответствующей записи для MAC-адреса назначения, коммутатор пересылает пакет на все порты, кроме принимающего порта, используя broadcast режим.

9.2 Принцип изучения MAC-адресов

Процесс самообучения таблицы MAC-адресов выглядит следующим образом: когда компьютер A на порт_1 хочет связаться с компьютером B на порт_2, A отправляет информацию на коммутатор. После получения информации коммутатор сначала записывает MAC-адрес A, соответствующий порту отправки 1, в таблицу MAC. Затем он проверяет, присутствует ли MAC-адрес получателя B в таблице. Если MAC-адрес B находится в таблице MAC-адресов, коммутатор пересылает информацию на Port 2, связанный с B. Если MAC-адрес B отсутствует в таблице, коммутатор передает информацию на все порты. Когда B получает информацию, он отвечает коммутатору, который затем пересылает ответ A. Во время этого процесса ответа коммутатор записывает MAC-адрес B в таблицу MAC, обеспечивая двустороннюю связь.

Аналогичным образом коммутаторы узнают MAC-адреса от отправителя. По истечении времени устаревания (по умолчанию равно 5 минут), если нет обмена информацией с MAC-адресом компьютера, подключенного к порту, коммутатор удаляет MAC-адрес этого компьютера из

таблицы MAC-адресов, связанной с этим портом. Это обеспечивает емкость и актуальность адресной таблицы.

9.3 Настройка таблицы MAC-адресов

9.3.1 Общая конфигурация

Таблица 25 – Общая конфигурация

Команды	Описание	Режим
mac-address static <mac-address> vlan <vlan-id> interface <interface-type> <interface-number>	Настроить привязку MAC	“(config)#”
mac-address blackhole <mac-address> vlan <vlan-id>	Настроить фильтрацию MAC-адресов	“(config)#”
mac-address aging-time <10-1000000>	Настроить время устаревания	“(config)#”
mac-address aging-time no-aging	Восстановить время устаревания по умолчанию	“(config)#”
mac-address num-limit <max-count> interface <interface-type> <interface-number>	Настроить максимальное количество изучения MAC	“(config)#”
no mac-address (dynamic | static) <mac-address> interface <interface-type> <interface-number> vlan <vlan-id>	Удалить привязку MAC	“(config)#”
no mac-address (dynamic | static) interface <interface-type interface-number>	Удалить MAC по порту	“(config)#”
no mac-address (blackhole | dynamic | static | <mac-address>) vlan <vlan-id>	Удалить MAC по VLAN	“(config)#”
no mac-address all	Удалить все MAC адреса	“(config)#”

9.3.2 Показать таблицу переадресации MAC-адресов

Таблица 26 – Переадресация MAC-адресов

Команда	Описание	Режим
show mac-address <mac-address> vlan <vlan-id>	Просмотреть запись таблицы MAC	“#”
show mac-address all	Посмотреть все MAC-адреса	“#”
show mac-address (blackhole | dynamic | static)	Просмотреть MAC по типу	“#”
show mac-address interface <interface-type> <interface-number>	Просмотреть MAC по порту	“#”
show mac-address vlan <vlan-id>	Просмотреть MAC по VLAN	“#”
show mac-address aging-time	Отобразить времени устаревания	“#”
show mac-address num-limit	Отобразить максимальное количество изучения MAC	“#”

9.4 Пример настройки

1. Требования к сети

— Настроить HostA, HostB, HostC и сервер как статические записи таблицы MAC-адресов.

— Если коммутатор получает исходный MAC-адрес, который статически привязан, пересылает его в соответствии с портом и отбрасывает несовместимый с портом.

— Если адрес назначения отправленного сообщения соответствует статическому привязанному MAC-адресу, оно будет перенаправлено на соответствующий порт. Если оно несовместимо, оно будет направлено на broadcast адрес.

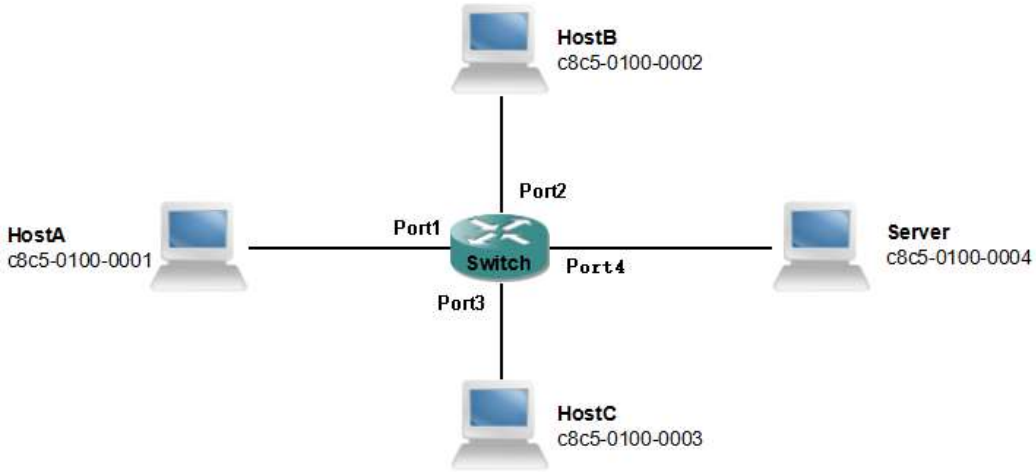

Рисунок 8 – Требования к сети

2. План конфигурации

— Добавить статическую топологию привязки MAC к соответствующему порту.

3. Шаги настройки

Добавить статическую запись mac на коммутатор

SWITCH(config)# mac-address static c8:c5:01:00:00:01 vlan 1 interface ethernet 1/0/1

SWITCH(config)# mac-address static c8:c5:01:00:00:02 vlan 1 interface ethernet 1/0/2

SWITCH(config)# mac-address static c8:c5:01:00:00:03 vlan 1 interface ethernet 1/0/3

SWITCH(config)# mac-address static c8:c5:01:00:00:04 vlan 1 interface ethernet 1/0/4

4. Проверка конфигурации

Просмотр статических mac-адресов на коммутаторе

SWITCH(config)# show mac-address static

```
 VID|MAC Address|Type|   Ports
--------+--------------+--------------+--------------+--------------+-----
    1| C8:C5:01:00:00:01|    Static| eth1/0/1
    1| C8:C5:01:00:00:02|    Static| eth1/0/2
    1 |C8:C5:01:00:00:03|    Static| eth1/0/3
1 | C8:C5:01:00:00:04|    Static| eth1/0/4
```

10 НАСТРОЙКИ БЕЗОПАСНОСТИ

В этой главе представлено подробное описание команд CLI:

– Настройка зеркалирования;

– Настройка подавления широковещательного шторма (broadcast storm)/неизвестного юникаст трафика (unknown unicast)/мультикаст сообщений (multicast message).

10.1 Настройка зеркалирования

Зеркалирование портов (Port mirroring) — очень полезная функция для просмотра данных, полученных и отправленных одним или несколькими портами. Порт, поддерживающий зеркалирование, может прослушивать входящие и исходящие данные от других портов. Зеркальный порт может одновременно прослушивать несколько портов. В этом разделе представлена настройка зеркалирования:

– Настройка порта назначения и порта источника для зеркалирования;

– Просмотр конфигурации зеркалирования.

10.1.1 Настройка порта назначения и порта источника для зеркалирования

При настройке прослушиваемого порта администратору необходимо войти в глобальный режим, чтобы установить исходный порт. Например, для зеркалирования входящего и исходящего трафика Порта 2 на Порт 1 конфигурация будет следующей:

SWITCH (config)# monitor session 1 monitor-port interface ethernet 1/0/1

SWITCH (config)# monitor session 1 mirror-port interface ethernet 1/0/2 both

В этот момент Порт 1 определяется как порт назначения, а Порт 2 — как порт источник.

Синтаксис команды для установки порта как источник:

monitor session <session-number> monitor-port interface <interface-type> <interface-number>

monitor session <session-number> mirror-port interface <interface-type> <interface-number> (both | ingress | egress)

В этот момент Порт 1 настроен как порт назначения, Порт 2 настроен как порт источник, а параметры (both | ingress | egress) указывают направление для порта источника: 'ingress' относится к пакетам, полученным на порту; 'egress' относится к пакетам, отправленным с порта; 'both' включают все пакеты, отправленные и полученные портом источником.

Также, в режиме глобальной конфигурации администраторы могут отменить мониторинг указанной группы зеркалирования с помощью следующей команды:

SWITCH (config)# no monitor session <session-number>

Необходимо отметить следующие моменты:

— Порт не может быть одновременно установлен как порт назначения зеркалирования и как порт источник зеркалирования.

— Порт назначения может быть только один, а портов источников может быть несколько.

Таблица 27 – Команды портов

Команды	Описание	Режим
monitor session <session-number> monitor-port interface <interface-type> <interface-number>	Установить порт источник мониторинга	“(config)#”
no monitor session <session-number> mirror-port interface <interface-type> <interface-number>	Удалить порт источник мониторинга	“(config)#”
monitor session <session-number> mirror-port interface <interface-type> <interface-number> (both | ingress | egress)	Установить порт назначения мониторинга	“(config)#”
no monitor session <session-number>	Удалить сессию мониторинга	“(config)#”

10.1.2 Просмотр конфигурации зеркалирования

Администраторы могут просмотреть настроенные конфигурации зеркалирования с помощью следующих команд:

Таблица 28 - конфигурации зеркалирования

Команды	Описание	Режим
show monitor session <session-number>	Показать конфигурацию сессии мониторинга	“#”
show monitor all	Показать количество всех групп мониторинга	“#”

10.2 Настройка подавления шторма

Функция подавления шторма на коммутаторах имеет решающее значение для предотвращения перегрузки сети. Все порты коммутатора поддерживают подавление широковещательных, многоадресных и неизвестных одноадресных пакетов.

В этом разделе представлено подробное описание конфигурации подавления шторма, касательно следующих тем:

— Конфигурация по умолчанию

— Конфигурация подавления широковещательной рассылки

— Конфигурация подавления многоадресной рассылки

— Конфигурация функции подавления

— Просмотр конфигурацию широковещательного шторма

10.2.1 Конфигурация по умолчанию

Коммутатор поддерживает отдельные настройки для широковещательной, многоадресной и одноадресной передачи на каждом порту, причем каждая настройка имеет собственное индивидуальное ограничение скорости. По умолчанию на портах включено подавление широковещательных пакетов со степенью подавления 64 КБ. Для неизвестных одноадресных и многоадресных пакетов по умолчанию нет подавления.

10.2.2 Настройка подавления широковещательной рассылки и ограничение скорости

Следующая команда настраивает подавление широковещательной рассылки для этого порта:

Таблица 29 – Настройка подавления широковещательные рассылки

Команды	Описание	Режим
broadcast-suppression (kbps|pps) <suppression>	Настроить подавление широковещательной рассылки	“(config-eth)”
no broadcast-suppression	Отменить подавление широковещательной рассылки	“(config-eth)”

6.2.3 Подавление многоадресной рассылки и настройка ограничения скорости

Следующая команда настраивает подавление многоадресной рассылки для этого порта.

Таблица 30 – Команды настраивания подавления многоадресной рассылки

Команды	Описание	Режим
multicast-suppression (kbps|pps) <suppression>	Настроить подавление многоадресной рассылки	“(config-eth)”
no multicast-suppression	Отменить подавление многоадресной рассылки	“(config-eth)”

6.2.4 Конфигурация подавления неизвестной одноадресной рассылки и ограничения скорости

Следующая команда настраивает подавление неизвестной одноадресной рассылки для этого порта:

Таблица 31 - Настройки подавления неизвестной одноадресной рассылки

Команды	Описание	Режим
unicast-suppression (kbps|pps) <suppression>	Настроить подавление неизвестной одноадресной рассылки	“(config-eth)”
no unicast-suppression	Отменить подавление неизвестной одноадресной рассылки	“(config-eth)”

6.2.5 Просмотр конфигурацию широковещательного шторма

Следующая команда отображает конфигурацию подавления шторма в глобальном режиме или режиме интерфейса:

Таблица 32 – Просмотр конфигурации порта

Команды	Описание	Режим
show interface switchport <PORTTYPE> <INTERFACE>	Показать конфигурацию порта	“#”

10.3 Пример настройки параметров безопасности

10.3.1 Пример настройки зеркалирования портов

1. Требования к сети

— Порт назначения 1 отслеживает исходящий трафик порта 2.

— Порт назначения 2 отслеживает входящий трафик порта 3.

— Порт назначения 3 контролирует двунаправленный трафик порта 4.

2. План настройки

— Настроить порт назначения 1 для мониторинга исходящего трафика порта 2.

— Настроить порт назначения 2 для мониторинга входящего трафика порта 3.

— Настроить порт назначения 3 для мониторинга двунаправленного трафика порта 4.

3. Шаги настройки

（1）Настройка порта назначения для мониторинга каждого порта источника

#Настройка коммутатора

SWITCH# configure

SWITCH(config)# monitor session 1 monitor-port interface ethernet 1/0/1

SWITCH(config)# monitor session 1 mirror-port interface ethernet 1/0/2 outbound

SWITCH(config)# monitor session 1 mirror-port interface ethernet 1/0/3 inbound

SWITCH(config)# monitor session 1 mirror-port interface ethernet 1/0/4 both

4. Проверка конфигурации

#Просмотр настроек зеркалирования

SWITCH(config)# show monitor session 1

monitor-session 1: eth1/0/1

---

port-mirror:

Mirror-port Direction Monitor-session

---

eth1/0/2 outbound Monitor-session 1

```
eth1/0/3        inbound      Monitor-session 1
eth1/0/4        both         Monitor-session 1
```

10.3.2 Пример настройки ограничения скорости порта

1. Требования к сети

— Ограничить исходящую скорость порта 1.

— Ограничить входящую скорость порта 1.

— Ограничить двунаправленную скорость порта 3.

2. План настройки

— Настроить ограничения исходящей скорости порта 1.

— Настроить ограничение входящей скорости порта 2.

— Настроить ограничение двунаправленной скорости порта 3.

3. Шаги настройки

（1）Настроить ограничение скорости порта

```
#Настройка коммутатора
SWITCH# configure
SWITCH(config)# interface ethernet 1/0/1
SWITCH(config-eth1/0/1)# rate-limit egress 500
SWITCH(config-eth1/0/1)# interface ethernet 1/0/2
SWITCH(config-eth1/0/2)# rate-limit ingress 500
SWITCH(config-eth1/0/2)# interface ethernet 1/0/3
SWITCH(config-eth1/0/3)# rate-limit ingress 2000
SWITCH(config-eth1/0/3)# rate-limit egress 2000
```

4. Проверка конфигурации

```
SWITCH (config)# show interface switchport ethernet 1/0/1
  Port                        : eth1/0/1
-----------------------------------------------------
Port Mode                     : Access
Port Pvid                     : 1
Description                   : Eth1/0/1
Link State                    : Unlink
Speed/Duplex                  : Auto-Negotiation
Priority                      : 0
```

Flow Control : Disabled
PHY : Open
MDIX : AUTO
Isolate : Disabled
Jumboframe : 1536
Ratelimit ingress : 0
Ratelimit egress : 448
Broadcast suppression : disable
Multicast suppression : disable
Unicast suppression : disable
Mac limit : 0
---

11 LLDP (LINK LAYER DISCOVERY PROTOCOL)/ ПРОТОКОЛ ОБНАРУЖЕНИЯ КАНАЛЬНОГО УРОВНЯ

LLDP (Link Layer Discovery Protocol) – протокол обнаружения канального уровня предоставляет стандартизированный метод обнаружения устройств на канальном уровне. Он организует основные параметры, адреса управления, идентификаторы устройств, идентификаторы интерфейсов и другую информацию о локальном устройстве в различные TLV (Type/Length/Value) - тип/длина/значение, и инкапсулирует их в LLDPDU (Link Layer Discovery Protocol Data Units) - блоки данных протокола обнаружения канального уровня, для публикации до соседних устройств подключеных напрямую.

Получив эту информацию, соседи сохраняют ее в стандартизированном формате базы управляющей информации (MIB - Management Information Base), чтобы системы управления сетью могли запрашивать и оценивать состояние связи канала.

В этом разделе основное внимание уделяется настройке LLDP, касательно тем:

– Конфигурация LLDP;

– Просмотр LLDP.

11.1 Конфигурация LLDP

Существует четыре режима работы порта LLDP:

Tx&Rx: отправляет и получает пакеты LLDP.

Tx: отправляет пакеты LLDP, но не получает их.

Rx: получает пакеты LLDP, но не отправляет их.

Disabel: пакеты LLDP не отправляются и не принимаются.

При изменении режима работы порта LLDP порт инициализирует механизм состояния протокола. Чтобы частые изменения режима работы порта не приводили к непрерывным операциям инициализации, вы можете настроить задержку инициализации порта. Эта задержка позволяет пройти некоторому времени перед выполнением операций инициализации при изменении режима работы порта.

11.1.1 Общая конфигурация LLDP

Таблица 33 - Настройка LLDP в глобальном режиме

Команды	Описание	Режим
[no] lldp enable	Отключить/включить LLDP глобально	“(config)#”
[no] lldp trap enable	Отключить/включить trap LLDP глобально	“(config)#”

Примечание - когда порт LLDP настроен по умолчанию, порт исполняет глобальные настройки LLDP.

Настройки LLDP для указанных портов можно настроить в глобальном или интерфейсном режиме.

11.1.2 Конфигурация таймера LLDP

Таблица 34 - Настройка параметров LLDP в режиме глобальной конфигурации

Команды	Описание	Режим
[no] lldp timer reinit-delay <1-10>	Время задержки восстановления/инициализации конфигурации	“(config)#”
[no] lldp message-transmission tx-interval <5-32768>	Восстановить/настроить интервал отправки сообщений LLDP	“(config)#”

[no] lldp message-transmission hold-multiplier <2-10>	Восстановить/настроить время удержания соседнего устройства LLDP	“(config)#”
[no] lldp tx-delay <1-8192>	Восстановить/настроить время задержки до соседних устройств LLDP для отправки сообщений	“(config)#”
[no] lldp fast-count <3-10>	Настроить количество быстрых передач сообщений LLDP	“(config)#”

11.1.3 Конфигурация интерфейса LLDP

Таблица 35 - Настройка параметров LLDP в режиме интерфейса

Команды	Описание	Режим
[no] lldp enable	Отключить/включить LLDP	“(config-eth)”
lldp work-mode (disable | rx | tx | txrx)	Настроить режим работы LLDP	“(config-eth)”
[no] lldp tlv-select basic-tlv (all | management-address | port-description | system-capability | system-description | system-name)	Отменить/настроить базовый TLV для публикации интерфейса	“(config-eth)”
[no] lldp tlv-select dot1-tlv port-vlan-id	Отменить/настроить TLV определенные 802.1	“(config-eth)”
[no] lldp tlv-select dot3-tlv (all | link-aggregation | mac-physic | max-frame-size)	Отменить/настроить TLV определенные 802.3	“(config-eth)”

11.2 Просмотр LLDP

Пользователи могут просматривать как локальную информацию LLDP, так и информацию об удаленной системе.

Таблица 36 – Просмотр локальной информации о LLDP и удаленной системе

Команды	Описание	Режим
show lldp system-config	Посмотреть информацию о конфигурации системы LLDP	“#”
show lldp neighbor interface	Посмотреть информацию о соседних устройствах для всех интерфейсов	“#”
show lldp neighbor interface brief	Посмотреть информацию о соседних устройствах для всех интерфейсов (кратко)	“#”
show lldp neighbor interface <interface-type> <interface-number>	Посмотреть информацию о соседнем устройстве для определенного интерфейса	“#”
show lldp local	Посмотреть локальную информацию о состоянии LLDP для всех интерфейсов.	“#”

show lldp local interface <interface-type> <interface-number>	Посмотреть локальную информацию о состоянии LLDP для указанного интерфейса.	“#”
show lldp statistics	Посмотреть статистическую информацию о сообщениях LLDP, отправленных и полученных всеми интерфейсами.	“#”
show lldp statistics interface <interface-type> <interface-number>	Посмотреть статистическую информацию о сообщениях LLDP, отправленных и полученных указанным интерфейсом.	“#”
show lldp tlv-config	Посмотреть все дополнительные TLV, отправляемы интерфейсами.	“#”
show lldp tlv-config interface <interface-type> <interface-number>	Посмотреть дополнительные TLV, отправляемые указанным интерфейсом.	“#”

11.3 Пример настройки

11.3.1 Описание задач для настройки

Таблица 37 - Описание задач для настройки

Критерий задач конфигурации	Описание
Отключить/включить глобальный LLDP	Необходимый
Настроить режим работы LLDP	Необходимый
Отключить/включить LLDP trap	Необязательный
Настроить таймер	Необязательный
Отменить/настроить базовый TLV для публикации интерфейса.	Необязательный
Отменить/настроить TLV определеный 802.1	Необязательный
Отменить/настроить TLV определеный 802.3	Необязательный

11.3.2 Пример настройки

1. Требования сети

— Router1, Router2 и Router3 соединены через Ethernet, и устройства могут получать информацию о соседях через протокол LLDP.

— Устройство отправляет базовый TLV, TLV определеный 802.1 и TLV определеный 802.3.

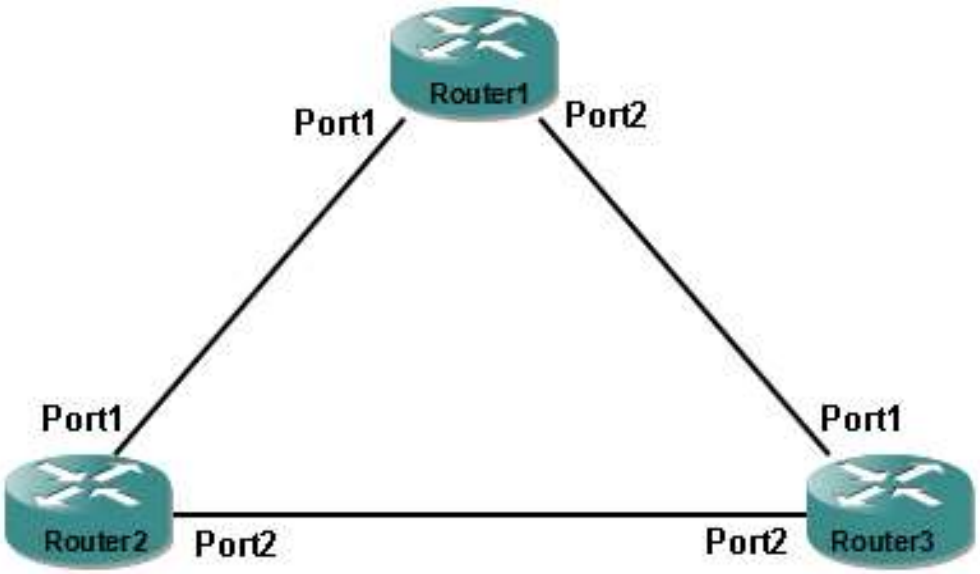

Рисунок 9 - Схема топологии сети

2. План настройки

— Настройте Порт 1– Порт 2 маршрутизаторов Router1, Router2 и Router3 как TX&RX.

— Настройте базовый TLV, чтобы включить все

— Настройте 802.1 для определения TLV, включающих все

— Настройте 802.3 для определения TLV, включающих все

3. Шаги настройки

（1）Включить LLDP глобально и на интерфейсе

#Включить LLDP на Router1

Router1# configure

Router1(config)# lldp enable

Router1(config)# interface ethernet 1/0/1

Router1(config-eth1/0/1)# lldp enable

Router1(config-eth1/0/1)# interface ethernet 1/0/2

Router1(config-eth1/0/2)# lldp enable

#Включить LLDP на Router2

Router2# configure

Router2(config)# lldp enable

Router2(config)# interface ethernet 1/0/1

Router2(config-eth1/0/1)# lldp enable

Router2(config-eth1/0/1)# interface ethernet 1/0/2

Router2(config-eth1/0/2)# lldp enable

#Включить LLDP на Router3

Router3# configure

Router3(config)# lldp enable

Router3(config)# interface ethernet 1/0/1

Router3(config-eth1/0/1)# lldp enable
Router3(config-eth1/0/1)# interface ethernet 1/0/2
Router3(config-eth1/0/2)# lldp enable

（2）Настроить порты в режим TX&RX

Настроить порт 1 и порт 2 в режим TX&RX на Router1
Router1(config)# interface ethernet 1/0/1
Router1(config-eth1/0/1)# lldp work-mode txrx
Router1(config-eth1/0/1)# interface ethernet 1/0/2
Router1(config-eth1/0/2)# lldp work-mode txrx
Настроить порт 1 и порт 2 в режим TX&RX на Router2
Router2(config)# interface ethernet 1/0/1
Router2(config-eth1/0/1)# lldp work-mode txrx
Router2(config-eth1/0/1)# interface ethernet 1/0/2
Router2(config-eth1/0/2)# lldp work-mode txrx
Настроить порт 1 и порт 2 в режим TX&RX на Router3
Router3(config)# interface ethernet 1/0/1
Router3(config-eth1/0/1)# lldp work-mode txrx
Router3(config-eth1/0/1)# interface ethernet 1/0/2
Router3(config-eth1/0/2)# lldp work-mode txrx

（3）Настроить TLV

Настроить TLV на Router1
Router1(config)# interface ethernet 1/0/1
Router1(config-eth1/0/1)# lldp tlv-select basic-tlv all
Router1(config-eth1/0/1)# lldp tlv-select dot1-tlv port-vlan-id
Router1(config-eth1/0/1)# lldp tlv-select dot3-tlv all
Настроить TLV на Router2
Router2(config)# interface ethernet 1/0/1
Router2(config-eth1/0/1)# lldp tlv-select basic-tlv all
Router2(config-eth1/0/1)# lldp tlv-select dot1-tlv port-vlan-id
Router2(config-eth1/0/1)# lldp tlv-select dot3-tlv all
Настроить TLV на Router3
Router3(config)# interface ethernet 1/0/1
Router3(config-eth1/0/1)# lldp tlv-select basic-tlv all
Router3(config-eth1/0/1)# lldp tlv-select dot1-tlv port-vlan-id
Router3(config-eth1/0/1)# lldp tlv-select dot3-tlv all

4. Проверка конфигурации

Просмотр LLDP информации о соседях

Просмотр lldp информации о соседях на Router1

Router1(config)# show lldp neighbor brief

```
Local Port |Device ID|Port ID|SysName|Capabilities|TTL
---------------------------- + ---------------- + ---------------------- + ---------------- +
ethernet 1/0/1|00:00:00:00:00:77|GE1/2/1|CVN|Bridge|   100
---------------------------- + ---------------- + ---------------------- + ---------------- +
ethernet 1/0/2|  00:00:00:00:11:00|ETH1/0/1|SWITCH|Bridge|    98
---------------------------- + ---------------- + ---------------------- + ---------------- +
# Просмотр lldp информации о соседях на Router2

Router2(config)# show lldp neighbor brief
Local Port |Device ID|Port ID|SysName|Capabilities|TTL
------------------------ + ---------------- + ---------------------- + ---------------- + -------------
ethernet 1/2/1|c8:c5:0e:01:33:01|ETH1/0/1|SWITCH|Bridge|119
------------------------ + ---------------- + ---------------------- + ---------------- + -------------
ethernet 1/2/2|00:00:00:00:11:00|ETH1/0/2|SWITCH|Bridge|95
------------------------ + ---------------- + ---------------------- + ---------------- + -------------
# Просмотр lldp информации о соседях на Router3

Router3(config)# show lldp neighbor brief
Local Port |Device ID|Port ID|SysName|Capabilities|TTL
------------------------ + ---------------- + ---------------------- + ---------------- + -------------
ethernet 1/0/1|c8:c5:0e:01:33:01|ETH1/0/2|SWITCH|Bridge|106
------------------------ + ---------------- + ---------------------- + ---------------- + -------------
ethernet 1/0/2|00:00:00:00:00:77|GE1/2/2|CVN|Bridge|115
------------------------ + ---------------- + ---------------------- + ---------------- + -------------
```

12 VLAN (VIRTUAL LOCAL AREA NETWORK)/ ВИРТУАЛЬНАЯ ЛОКАЛЬНАЯ СЕТЬ

VLAN (Virtual Local Area Network) — это сеть, которая логически объединяет несколько устройств вместе, игнорируя их физическое местоположение. Каждый VLAN представляет собой логическую сеть, обладающую всеми функциями и атрибутами традиционных физических сетей. Каждый VLAN является широковещательным доменом, и широковещательные пакеты могут пересылаться только внутри однго VLAN и не могут пересекать VLAN. Передача данных между VLAN должна осуществляться через уровень 3.

Эта рассматривает следующие темы:

- Введение в VLAN;
- Конфигурация VLAN;
- Пример настройки VLAN.

12.1 Введение в VLAN

В этом разделе подробное описание следующих тем:

— VLAN ID
— Типы VLAN на портах
— VLAN по умолчанию для портов
— Режим VLAN порта
— VLAN TRUNK
— Пересылка данных внутри VLAN

12.1.1 VLAN ID

Каждый VLAN идентифицируется VLAN ID в диапазоне от 0 до 4095. Однако сети VLAN 0 и 4095 не используются, остается эффективный диапазон от 1 до 4094. VLAN ID однозначно идентифицирует VLAN.

При создании VLAN необходимо выбрать VLAN ID в диапазоне от 1 до 4094. По умолчанию на коммутаторе создан VLAN 1, удалить который невозможно.

В сети передаются два типа кадров с VLAN: не тегированные кадры и тегированные кадры с ненулевым VID. На следующей диаграмме показаны два разных формата кадров.

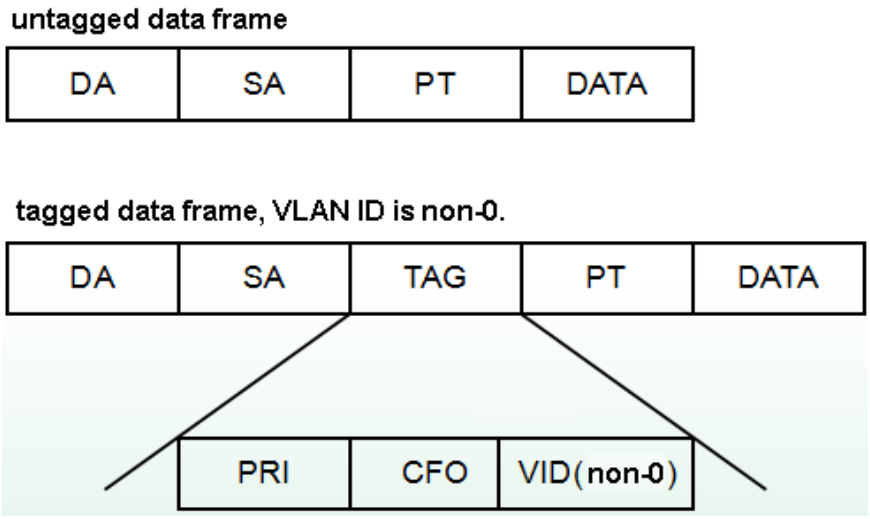

Рисунок 10 – Форматы кадров

Все кадры внутри коммутатора помечаются внутренними тегами. Если не тегированный кадр поступает в коммутатор, коммутатор добавляет к нему тег, выбирая значение VLAN ID для заполнения поля VID тега. Если на коммутатор попадает тегированный кадр с ненулевым VID, кадр остается неизменным.

12.1.2 Типы VLAN на портах

Коммутатор поддерживает сети с одним VLAN на порту и сети с VLAN на базе 802.1Q. Существует два типа vlan на портах: untagged (не тегированным) и tagged (тегированным).

К VLAN может принадлежать ноль, один или несколько портов. Порт может принадлежать одному или нескольким VLAN как тегированным или не тегированным. Если порт принадлежит двум или более VLAN в качестве тегированных, этот порт также называется trunk(магистральным) портом VLAN. Порт может одновременно принадлежать одному или нескольким VLAN в качестве не тегированных и принадлежать одному или нескольким другим VLAN в качестве тегированных.

12.1.3 VLAN по умолчанию для портов

Каждый порт имеет только один VLAN по умолчанию, который используется для определения VLAN, к которому принадлежат нетегированные пакеты, входящие в порт. VLAN по умолчанию также известен как порт VID или PVID. По умолчанию VLAN на порту равен 1.

12.1.4 Режим VLAN порта

Для портов предусмотрено три режима VLAN: ACCESS mode, TRUNK mode и HYBRID mode. При настройке VLAN для портов пользователи должны сначала указать режим VLAN порта.

— Порты в ACCESS mode — это порты доступа, обращенные непосредственно к пользователям, а VLAN по умолчанию — это VLAN, указанная пользователем.

— Порты в TRUNK mode — это магистральные порты, обычно напрямую подключенные к коммутатору. Эти порты могут принадлежать одному или нескольким VLAN в качестве тегированных, но не могут принадлежать ни одной VLAN в качестве нетегированных членов.

— Порты в HYBRID mode — это магистральные порты, напрямую подключенные к коммутатору. Эти порты могут принадлежать одной или нескольким VLAN в качестве тегированных и/или одной или нескольким VLAN в качестве нетегированных.

Пользователи могут выбирать режим портов VLAN в соответствии с конкретными требованиями.

12.1.5 8.1.5 VLAN Access

При получении пакета определяется, есть ли информация о VLAN: если нет, добавляется PVID порта и пакет пересылается. Если есть, отбрасывается (по умолчанию). Порты доступа передают пакеты, удаляя информацию о VLAN и отправляя их напрямую. Связь возможна между портами доступа с одинаковым PVID, но не между портами с разными PVID.

Пример ниже иллюстрирует связь и изоляцию с портами ACCESS:

— Порты, соединяющие User 1 и User 3, являются портами ACCESS с PVID, равным 2. Если магистральные порты VLAN позволяют использовать VLAN 2, связь между ними возможна.

— Порты, соединяющие User 2 и User 4, являются портами ACCESS с PVID, равным 3. Если магистральные порты VLAN поддерживают VLAN 3, связь между ними возможна.

— User 1 не может обмениваться данными с User 4, а User 2 не может обмениваться данными с User 3

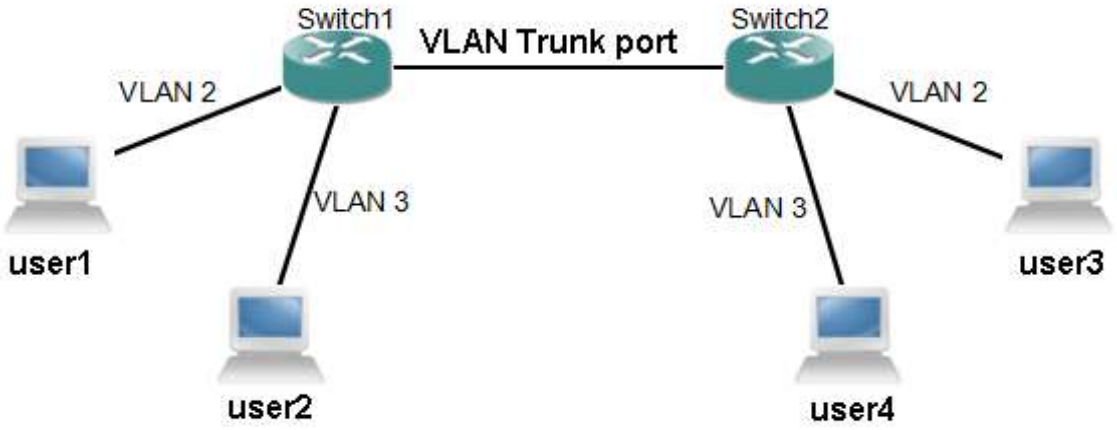

Рисунок 11 - Связь и изоляция с портами ACCESS

12.1.6 VLAN Trunk

Если порт принадлежит двум или более VLAN в качестве тегированных, то этот порт называется магистральным портом VLAN. Два коммутатора могут быть подключены через магистральные порты VLAN, что позволяет передавать два или более VLAN между коммутаторами.

В приведенном ниже примере показано транковое соединение VLAN, при котором два коммутатора подключаются через магистральные порты VLAN. Эти магистральные порты принадлежат VLAN 2 и VLAN 3 соответственно. На каждом коммутаторе есть две сети VLAN: VLAN 2 и VLAN 3, по одному пользователю в каждой VLAN. Следовательно, User 1 может общаться с User 3, User 2 может общаться с User 4, но User 1 и User 3 не могут общаться с User 2 и User 4.

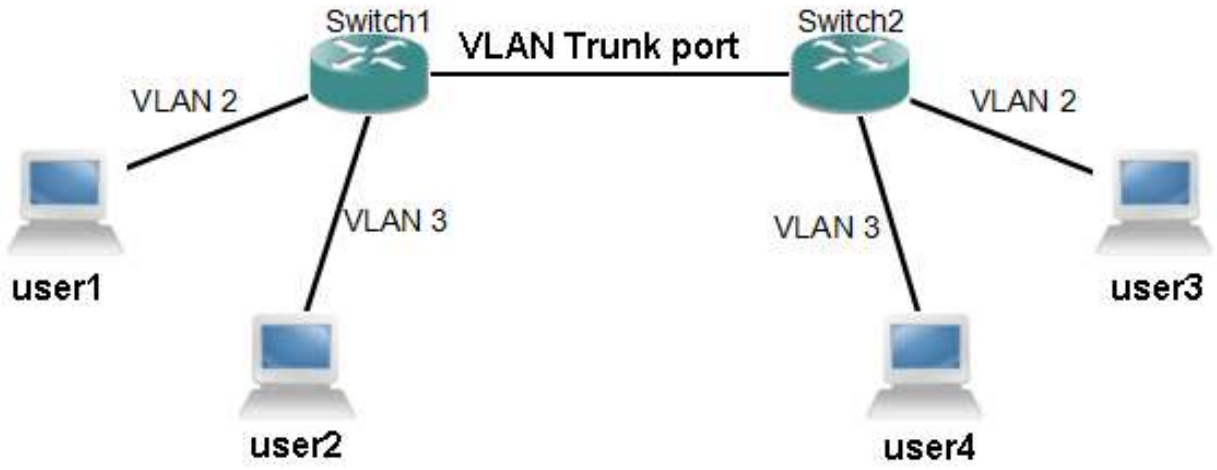

Рисунок 12 - Транковое соединение VLAN

12.1.7 VLAN Hybrid

При получении пакета гибридный порт проверяет информацию о VLAN. Если информация о VLAN отсутствует, порт добавляет PVID порта и пересылает пакет. Если информация VLAN присутствует, порт проверяет, разрешен ли данным VLAN на гибридном порту. Если разрешен, пакет пересылается; в противном случае он отбрасывается (в этот момент не тегированная конфигурация порта не учитывается, поскольку конфигурация без тегов применяется только при отправке пакетов).

12.1.8 Пересылка данных с VLAN

Когда коммутатор получает пакет от порта, он подвергается пересылке уровня 2 на основе следующих шагов:

Определяется VLAN, к которому принадлежит пакет.

Определяется, является ли пакет широковещательным, многоадресным или одноадресным.

В зависимости от типа пакета определяются выходные порты (которых может не быть, быть один или несколько). Если выходных портов нет, пакет отбрасывается.

В зависимости от типа выходных портов и их VLAN определяется, следует ли помечать исходящий пакет.

Отправляется пакет из выходного порта.

1) Определение VLAN, к которому принадлежит пакет:

Если полученный пакет тегирован и поле VID в теге не равно нулю, VLAN, к которому принадлежит пакет, определяется значением VID в теге.

Если полученный пакет не тегирован или помечен значением VID, равным 0, VLAN, к которому принадлежит пакет, является VLAN по умолчанию для порта.

2) Определение типа пакета:

Если MAC-адрес назначения полученного пакета — FF:FF:FF:FF:FF:FF, пакет является широковещательным.

Если полученный пакет не является широковещательным пакетом и 40-й бит его MAC-адреса назначения равен 1, пакет является многоадресным.

Если пакет не является ни широковещательным, ни многоадресным пакетом, это одноадресный пакет.

3) Определение выходного порта пакета:

Если входной пакет является широковещательным пакетом, все порты данного VLAN, к которому принадлежит пакет, являются выходными портами пакета.

Если входной пакет является многоадресным пакетом, выходные порты пакета определяются на основе MAC-адреса многоадресной рассылки назначения и VLAN, к которому он принадлежит. Если соответствующая запись найдена в таблице пересылки многоадресной рассылки уровня 2, общие порт между выходными портами в VLAN и записью многоадресной рассылки является выходными портами пакета. Если общих портов нет, пакет отбрасывается.

Если входной пакет является одноадресным, выходные порты пакета определяются на основе MAC-адреса назначения и VLAN, к которому он принадлежит. Если соответствующая запись найдена в таблице пересылки уровня 2, общий порт между выходными портами в VLAN и записью пересылки является выходным портам пакета. Если общих портов нет, пакет отбрасывается.

Если в таблице аппаратной пересылки уровня 2 не найдена соответствующая запись, пакет рассматривается как широковещательный пакет, а все порты данного VLAN, к которому принадлежит пакет, считаются выходными портами для пакета.

4) Отправка пакета:

После определения выходного порта входного пакета пакет отправляется со всех выходных портов.

Если выходной порт является не тегированным членом VLAN, к которому принадлежит пакет, пакет отправляется без тега.

Если выходной порт является тегированным членом VLAN к которому принадлежит пакет, пакет отправляется с тегом, а значение VID в теге является значением VLAN, к которому принадлежит пакет.

12.2 Конфигурация VLAN

В этом разделе представлено подробное описание настроек VLAN:

- Создание и удаление VLAN;
- Настрока режима VLAN для портов;
- Настройка VLAN ACCESS mode;
- Настройка VLAN TRUNK mode;
- Настройка VLAN HYBRID mode;
- Просмотр информации о VLAN.

8.2.1 Создание и удаление VLAN

Для создания и удаления VLAN пользователям необходимо создавать и удалять VLANs в режиме глобальной конфигурации.

В системе уже создан VLAN 1 по умолчанию, и VLAN 1 не может быть удален пользователем.

Таблица 38 – Команды создания и удаления VLAN

Команды	Описание	Режим
vlan VLANLIST	Создать/Войти VLAN	“(config)#”
no vlan VLANLIST	Удалить VLAN	“(config)#”
description <1-64>	Описание VLAN	“(vlan)#”

12.2.1 Настройка VLAN mode для портов

Перед настройкой VLAN для порта необходимо указать VLAN mode для порта. По умолчанию режим VLAN на порту — ACCESS mode.

Таблица 39 - Настройка VLAN mode для портов

Команды	Описание	Режим
switchport mode (access|trunk|hybrid)	Настроить режим VLAN	“(config-eth)”

12.2.2 Настройка VLAN ACCESS mode

Перед выполнением настройки VLAN на порту необходимо указать режим VLAN порта как ACCESS mode.

Таблица 40 - Настройка VLAN ACCESS mode

Команды	Описание	Режим
switchport access vlan <1-4094>	Настроить ACCESS VLAN	“(config-eth)”

12.2.3 Настройка VLAN TRUNK mode

Перед выполнением настройки VLAN на порту необходимо указать VLAN mode порта как TRUNK. В этом режиме VLAN можно настроить как тегированный.

Таблица 41 - Настройка VLAN TRUNK mode

Команды	Описание	Режим
switchport trunk allowed VLANLIST | all	Настроить VLAN порта TRUNK	“(config-eth)”
no switchport trunk allowed VLANLIST	Удалить VLAN порта TRUNK	“(config-eth)”
switchport trunk native vlan <1-4094>	Настроить не тегированный VLAN по умолчанию	“(config-eth)”
no switchport trunk	Отменить порт TRUNK и восстановить ACCESS по умолчанию.	“(config-eth)”

12.2.4 Конфигурация VLAN HYBRID Mode

Перед выполнением настройки VLAN на порту необходимо указать VLAN mode порта как HYBRID. Существуют таблицы с тегами и без тегов.

Таблица 42 - Конфигурация VLAN HYBRID Mode

Команды	Описание	Режим
switchport hybrid vlan VLANLIST untagged	Добавить не тегированный VLAN к гибридному порту	“(config-eth)”
switchport hybrid vlan VLANLIST tagged	Добавить тегированный VLAN к гибридному порту	“(config-eth)”
switchport hybrid native vlan <1-4094>	Настроить не тегированный VLAN по умолчанию	“(config-eth)”
no switchport hybrid vlan VLANLIST (tagged | untagged)	Удалить VLAN порта HYBRID	“(config-eth)”
no switchport hybrid	Отменить порт HYBRID и восстановить ACCESS по умолчанию.	“(config-eth)”

12.2.5 Просмотр информации о VLAN

Таблица 43 - Просмотр информации о VLAN

Команды	Описание	Режим
show vlan (VLANLIST | all)	Показать информацию о VLAN	“#”
show interface switchport <interface-type> <interface-number>	Показать конфигурацию VLAN порта	“#”

12.3 Пример настройки VLAN

12.3.1 VLAN на основе порта

1. Требования к сети

— User 1 принадлежит vlan2

— User 2 принадлежит vlan3

— Связь между User 1 и User 2 невозможна.

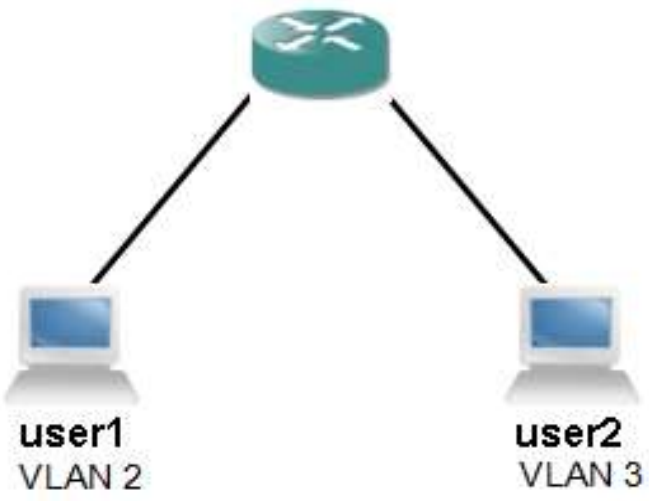

Рисунок 13 - Схема топологии сети

2. План настройки

— Создать vlan

— Настроить порт в соответсвующий VLAN

3. Шаги настройки

（1）Создать vlan 2-3

Создать vlan

SWITCH# configure

SWITCH(config)# vlan 2-3

Настроить VLAN на портах

Настроить порт 1 в режим доступа, в vlan 2

SWITCH(config)# interface ethernet 1/0/1

SWITCH(config-eth1/0/1)# switchport mode access

SWITCH(config-eth1/0/1)# switchport access vlan 2

Настроить порт 2 в режим доступа, в vlan 3

SWITCH(config)# interface ethernet 1/0/2

SWITCH(config-eth1/0/2)# switchport mode access

SWITCH(config-eth1/0/2)# switchport access vlan 3

4. Проверка конфигурации

Просмотр конфигурации VLAN

SWITCH(config)# show vlan all

Vlan : 1

Ports:

eth1/0/3,eth1/0/4,eth1/0/5,eth1/0/6,eth1/0/7,eth1/0/8,eth1/0/9,eth1/0/10,eth1/0/11,eth1/0/12,eth1/0/13,eth1/0/14,eth1/0/15,eth1/0/16,eth1/0/17,eth1/0/18,eth1/0/19,eth1/0/20,eth1/0/21,eth1/0/22,eth1/0/23,eth1/0/24,eth1/0/25,eth1/0/26,eth1/0/27,eth1/0/28,eth1/0/29,eth1/0/30,eth1/0/31,eth1/0/32,eth1/0/33,eth1/0/34,eth1/0/35,eth1/0/36,eth1/0/37,eth1/0/38,eth1/0/39,eth1/0/40,eth1/0/41,eth1/0/42,eth1/0/43,eth1/0/44,eth1/0/45,eth1/0/46,eth1/0/47,eth1/0/48,eth1/0/49,eth1/0/50,eth1/0/51,eth1/0/52,eth1/0/53,eth1/0/54,lag1,lag2,lag3,lag4,lag5,lag6,lag7,lag8,lag9,lag10,lag11,lag12,lag13,lag14,lag15,lag16,lag17,lag18,lag19,lag20,lag21,lag22,lag23,lag24,lag25,lag26,lag27,lag28,lag29,lag30,lag31,lag32,lag33,lag34,lag35,lag36,lag37,lag38,lag39,lag40,lag41,lag42,lag43,lag44,lag45,lag46,lag47,lag48,lag49,lag50,lag51,lag52,lag53,lag54,lag55,lag56,lag57,lag58,lag59,lag60,lag61,lag62,lag63,lag64

Vlan : 2

Ports : eth1/0/1

Vlan : 3

Ports : eth1/0/2

Всего 3 Vlan

12.3.2 VLAN 802.1Q

1. Требования сети

— User 1 и User 4 имеют связь между собой.

— User 2 и User 3 имеют связь между собой.

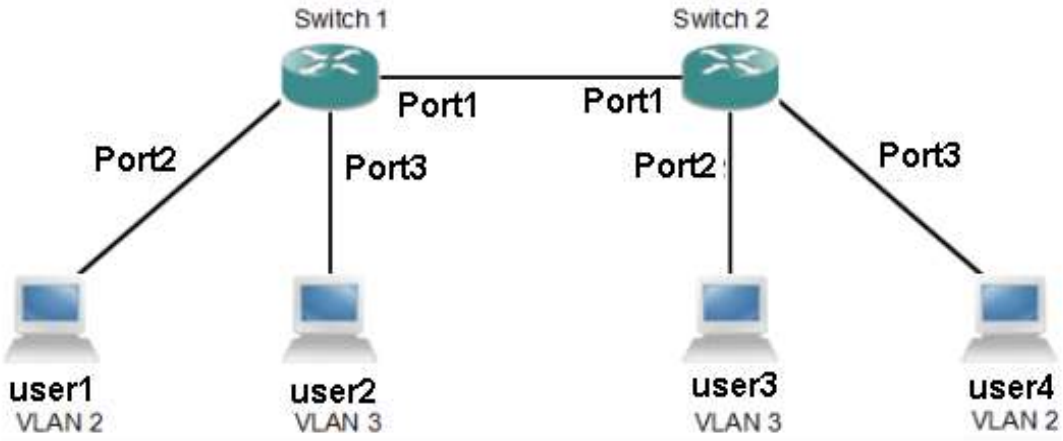

Рисунок 14 - Схема топологии сети

2. План настройки

— На Коммутаторе 1 создать VLAN 2 и 3, настроить trunk на порту 1 и разрешить всё, настроить VLAN 2 для Порта 2 и настроить VLAN 3 для порта 3.

— На Коммутаторе 2 создать VLAN 2 и 3, настроить trunk на порту 1 и разрешить всё, настроить VLAN 3 для порта 2, а VLAN 2 для порта 3.

3. Шаги настройки

（1）Создание VLAN и и настройка портов в VLAN

Настройка Switch1

SWITCH1# configure

SWITCH1(config)# vlan 2-3

SWITCH1(config)# interface ethernet 1/0/1

SWITCH1(config-eth1/0/1)# switchport mode trunk

SWITCH1(config-eth1/0/1)# switchport trunk allowed 1-3

SWITCH1(config-eth1/0/1)# interface ethernet 1/0/2

SWITCH1(config-eth1/0/2)# switchport access vlan 2

SWITCH1(config-eth1/0/2)# interface ethernet 1/0/3

SWITCH1(config-eth1/0/3)# switchport access vlan 3

Настройка Switch2.

SWITCH1# configure
SWITCH1(config)# vlan 2-3
SWITCH1(config)# interface ethernet 1/0/1
SWITCH1(config-eth1/0/1)# switchport mode trunk
SWITCH1(config-eth1/0/1)# switchport trunk allowed 1-3
SWITCH1(config-eth1/0/1)# interface ethernet 1/0/2
SWITCH1(config-eth1/0/2)# switchport access vlan 3
SWITCH1(config-eth1/0/2)# interface ethernet 1/0/3
SWITCH1(config-eth1/0/3)# switchport access vlan 2

4. Проверка конфигурации
Просмотр настройки VLAN и настройки поров в VLAN Switch1.
SWITCH1# show vlan all

Vlan : 1
Ports :
eth1/0/1,eth1/0/4,eth1/0/5,eth1/0/6,eth1/0/7,eth1/0/8,eth1/0/9,eth1/0/10,eth1/0/11,eth1/0/12,eth1/0/13,eth1/0/14,eth1/0/15,eth1/0/16,eth1/0/17,eth1/0/18,eth1/0/19,eth1/0/20,eth1/0/21,eth1/0/22,eth1/0/23,eth1/0/24,eth1/0/25,eth1/0/26,eth1/0/27,eth1/0/28,eth1/0/29,eth1/0/30,eth1/0/31,eth1/0/32,eth1/0/33,eth1/0/34,eth1/0/35,eth1/0/36,eth1/0/37,eth1/0/38,eth1/0/39,eth1/0/40,eth1/0/41,eth1/0/42,eth1/0/43,eth1/0/44,eth1/0/45,eth1/0/46,eth1/0/47,eth1/0/48,eth1/0/49,eth1/0/50,eth1/0/51,eth1/0/52,eth1/0/53,eth1/0/54,lag1,lag2,lag3,lag4,lag5,lag6,lag7,lag8,lag9,lag10,lag11,lag12,lag13,lag14,lag15,lag16,lag17,lag18,lag19,lag20,lag21,lag22,lag23,lag24,lag25,lag26,lag27,lag28,lag29,lag30,lag31,lag32,lag33,lag34,lag35,lag36,lag37,lag38,lag39,lag40,lag41,lag42,lag43,lag44,lag45,lag46,lag47,lag48,lag49,lag50,lag51,lag52,lag53,lag54,lag55,lag56,lag57,lag58,lag59,lag60,lag61,lag62,lag63,lag64

Vlan : 2
Ports : eth1/0/1,eth1/0/2

Vlan : 3
Ports : eth1/0/1,eth1/0/3

Всего 3 группы Vlan

Показать настройки VLAN и настройки портов в VLAN Switch2.

SWITCH2# show vlan all

Vlan : 1

Ports :
eth1/0/1,eth1/0/4,eth1/0/5,eth1/0/6,eth1/0/7,eth1/0/8,eth1/0/9,eth1/0/10,eth1/0/11,eth1/0/12,eth1/0/13,eth1/0/14,eth1/0/15,eth1/0/16,eth1/0/17,eth1/0/18,eth1/0/19,eth1/0/20,eth1/0/21,eth1/0/22,eth1/0/23,eth1/0/24,eth1/0/25,eth1/0/26,eth1/0/27,eth1/0/28,eth1/0/29,eth1/0/30,eth1/0/31,eth1/0/32,eth1/0/33,eth1/0/34,eth1/0/35,eth1/0/36,eth1/0/37,eth1/0/38,eth1/0/39,eth1/0/40,eth1/0/41,eth1/0/42,eth1/0/43,eth1/0/44,eth1/0/45,eth1/0/46,eth1/0/47,eth1/0/48,eth1/0/49,eth1/0/50,eth1/0/51,eth1/0/52,eth1/0/53,eth1/0/54,lag1,lag2,lag3,lag4,lag5,lag6,lag7,lag8,lag9,lag10,lag11,lag12,lag13,lag14,lag15,lag16,lag17,lag18,lag19,lag20,lag21,lag22,lag23,lag24,lag25,lag26,lag27,lag28,lag29,lag30,lag31,lag32,lag33,lag34,lag35,lag36,lag37,lag38,lag39,lag40,lag41,lag42,lag43,lag44,lag45,lag46,lag47,lag48,lag49,lag50,lag51,lag52,lag53,lag54,lag55,lag56,lag57,lag58,lag59,lag60,lag61,lag62,lag63,lag64

Vlan : 2

Ports : eth1/0/1,eth1/0/2

Vlan : 3

Ports : eth1/0/1,eth1/0/3

Всего 3 группы Vlan

13 КАЧЕСТВО ОБСЛУЖИВАНИЯ

В этой главе описывается QoS и его настройка, касательно следующих тем:

- Введение в QoS;
- Конфигурация QoS;
- Просмотр настройки QoS;
- Пример настройки QoS .

13.1 Введение в QoS

Пользователи могут использовать функции QoS для определения приоритета важных потоков данных, пересылаемых через коммутатор, обеспечивая равное использование пропускной способности сети и предсказуемую производительность сети.

Системы коммутации реализуют три типа QoS: на основе COS (802.1p), DSCP (DiffServ) и на основе локального приоритета. QoS на основе DSCP можно настроить на физическом порту, как и QoS на основе COS, при этом для физических портов значением по умолчанию является NONE.

На следующей диаграмме показан процесс пересылки пакетов с включенным QoS:

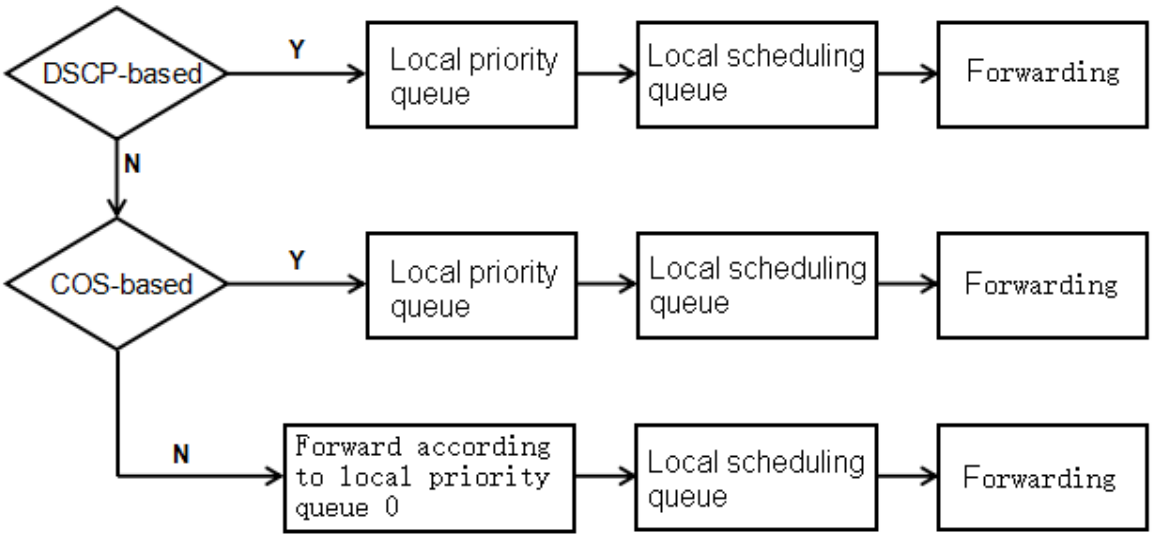

Рисунок 15 - Процесс пересылки пакетов с включенным QoS

Коммутатор поддерживает восемь очередей с приоритетом от 0 до 7, где очередь 7 имеет наивысший приоритет, а очередь 0 — самый низкий приоритет. Существует два метода планирования приоритетных очередей: WRR и HQ-WRR. WRR (Weighted Round-Robin) означает взвешенный циклический перебор, при котором коммутатор пересылает пакеты в циклическом порядке на основе настроенных весов от очередей с высоким приоритетом до очередей с низким приоритетом. Он пересылает определенное количество пакетов из очереди с наивысшим приоритетом, затем переходит на следующий уровень приоритета, пока все очереди не перешлют выделенное им количество пакетов. HQ-WFQ сочетает в себе алгоритм планирования очереди WRR с алгоритмом планирования очереди SP (Strict Priority) - строгий приоритет. Обеспечивая полную пересылку пакетов из очереди с наивысшим приоритетом, оставшаяся полоса пропускания распределяется на основе алгоритма планирования очереди WRR.

13.1.1 QoS на основе COS

По умолчанию на портах включено качество обслуживания на основе COS. Коммутатор извлекает значение приоритета из тега VLAN пакетов, входящих в этот порт, и определяет выходную очередь для пакета на основе взаимосвязи между настроенными пользователем значениями COS и очередями. Если в пакете отсутствует тег VLAN или тег VLAN равен 0, коммутатор заполняет пакет на основе настроенного пользователем VID по умолчанию и приоритета по умолчанию для этого порта, а затем определяет очередь вывода на основе приоритета по умолчанию.

13.1.2 QoS на основе DSCP

Когда на порту включено качество обслуживания на основе DSCP, коммутатор извлекает значение DSCP из IP-пакетов, входящих в этот порт, и определяет выходную очередь для пакета на основе взаимосвязи между настроенными пользователем значениями DSCP и очередями.

13.2 Настройка QoS

Описание конфигурации QoS в основном включает в себя следующие темы:

- Конфигурация QoS по умолчанию;
- Настройка политик QoS;
- Настройка методов планирования;

– Настройка веса очереди;
– Настройка взаимосвязи между политиками QoS и Local;
– Настройка приоритетов портов QoS.

13.2.1 Описание QoS по умолчанию

Таблица 44 – Описание QoS (по умолчанию)

Параметр	Значение
Количество очередей	1, 2, 3, 4
Метод планирования	WRR
Отношения сопоставления между COS и Local	802.1p: 0, 1, 2, 3, 4, 5, 6, 7 Local: 2, 1, 1, 2, 3, 3, 4, 4
Отношения отображения между DSCP и Local	DSCP0~DSCP15 [Local 1] DSCP16~DSCP31 [Local 2] DSCP32~DSCP47 [Local 3] DSCP48~DSCP63 [Local 4]

13.2.2 Настройка политик QoS

Политики QoS для указанных портов можно настроить в глобальном режиме.

Таблица 45 – Настройка политик QoS

Команда	Описание	Режим
[no] qos priority-trust (cos | dscp)	Восстановить/настроить политики QoS	“(config)#”

13.2.3 Настройка методов планирования

Метод планирования по умолчанию для коммутаторов — WRR. Методы планирования WRR и HQ-WRR можно настроить с помощью команд.

Таблица 46 – Команды настройки методов планирования

Команда	Описание	Режим
qos queue-scheduler (wrr | hq-wrr) <queue1-weight> <queue2-weight> <queue3-weight> <queue4-weight>	Настроить режим планирования QoS	“(config)#”
no qos queue-scheduler	Восстановить режим планирования по умолчанию	“(config)#”

13.2.4 Настройка приоритетов портов QoS

Определить приоритет порта можно в режиме интерфейса.

Таблица 47 - Настройка приоритета порта в режиме интерфейса

Команда	Описание	Режим
[no] qos priority <priority-level>	Восстановить/установить приоритет порта	“(config-eth)”

13.3 Просмотр конфигурации

Таблица 48 - Отображение информации о QoS

Команда	Описание	Режим
show queue-scheduler cos-queue-map-info	Посмотреть информации о сопоставлении приоритетов cos	“#”
show queue-scheduler dscp-queue-map-info	Посмотреть информации о сопоставлении приоритетов dscp	“#”
show qos (priority-trust | queue-scheduler)	Посмотреть информации о QoS	“#”

13.4 Пример базовой конфигурации QoS

13.4.1 Описание задач для настройки

Таблица 49 – Описание задач для настройки

Критерий задач конфигурации	Описание
Настроить политики QoS	Необходимый
Настроить режим планирования QoS	Необходимый
Настроить приоритет порта	Необязательный

13.4.2 Пример настройки

1. Требования сети

— Приоритетная пересылка COS с наивысшим приоритетом и пересылка с более низким приоритетом в зависимости от веса

— Устройство выполняет планирование DSCP на порту 2, причем приоритет отдается более высокому приоритету.

— Ограничение скорости на выходе из 4 порта коммутатора.

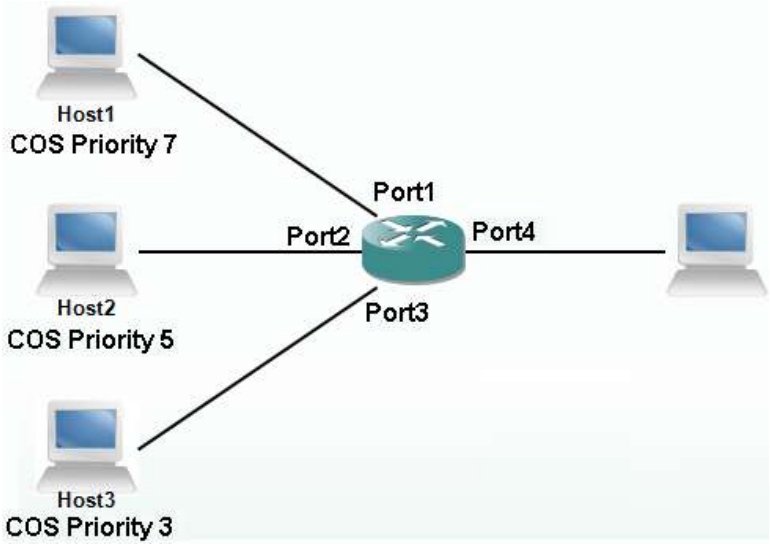

Рисунок 16 - Схема топологии сети

2. План настройки

— Настроить ограничения скорости порта 4

— Настроить политику QoS как COS

— Настроить режим планирования QoS как HQ-WRR

3. Шаги настройки

（1）Настройка ограничения скорости порта 4.

Настройка ограничения скорости порта 4

SWITCH# configure

SWITCH(config)# interface ethernet 1/0/4

SWITCH(config-eth1/0/4)# rate-limit egress 500000

Настройка политики QoS как COS.

SWITCH(config)# qos priority-trust cos

Настройка режима планирования QoS на HQ-WRR и вес 1 3 5 7.

SWITCH(config)# qos queue-scheduler hq-wrr 1 3 5 7

4. Проверка конфигурации

Просмотр ограничения скорости порта

SWITCH(config)# show interface switchport ethernet 1/0/4

Port : eth1/0/4

Port Mode: Access

Port Pvid: 1

```
Description                 : ETH1/0/4
Link State                  : Unlink
Speed/Duplex          : Auto-Negotiation
Priority                    : 0
Flow Control              : Disabled
PHY                   : Open
MDIX                     : AUTO
Isolate                   : Disabled
Jumboframe                : 1536
Ratelimit ingress             : 0
Ratelimit egress              : 499968
Broadcast suppression           : disable
Multicast suppression           : disable
Unicast suppression             : disable
Mac limit                   : 0
-----------------------------------------------------

# Просмотр политики QoS
SWITCH(config)# show qos priority-trust
priority-trust mode:cos

# Просмотр режима планирования QoS
SWITCH(config)# show qos queue-scheduler
  queue-scheduler mode: hq-wrr
  weight of queue 1: 1
  weight of queue 2: 3
  weight of queue 3: 5
  weight of queue 4: 7
```

Host1-Host3 отправляет пакеты данных со скоростью 30 Мбит/с. Host4 получает пакеты данных от Host1 со скоростью 30 Мбит/с, от Host2 со скоростью 12.5 Мбит/с, и от Host3 со скоростью 7.5 Мбит/с.

14 АГРЕГАЦИЯ КАНАЛОВ

В этом разделе представлено подробное описание настройки агрегации каналов:

- Обзор;
- Ручное агрегирование каналов;
- Группа статической агрегации;
- Список команд агрегации каналов.

14.1 Обзор

Агрегация каналов объединяет несколько портов в одну логическую порт-группу, которую можно использовать для увеличения пропускной способности, обеспечения резервных подключений и обеспечения балансировки нагрузки. В качестве выходного логического порта, коммутатор выбирает порт из группы портов на основе политики агрегации, установленной пользователем для передачи пакетов. Настройка портов в группе агрегации и политики агрегации осуществляется при помощи ОС, но пересылка пакетов происходит через коммутатор.

Все порты в агрегированной группе должны быть настроены на одинаковую скорость и работать в полнодуплексном режиме. Важно отметить, что каждый порт может принадлежать только к одной агрегированной группе, а агрегация каналов делится на агрегацию вручную и агрегацию с использованием протокола LACP.

Протокол LACP основан на стандарте IEEE 802.3ad. Протокол LACP взаимодействует с партнером используя LACPDU（Link Aggregation Control Protocol Data Unit）.

Интерфейсы в группе агрегации включают протокол LACP, и интерфейс отправляет LACPDU соседу, чтобы сообщить ему о приоритете протокола LACP системы, MAC-адресе системы, приоритете протокола LACP порта, номере порта и рабочем ключе. После получения LACPDU партнер сравнивает эту информацию с информацией, полученной от других интерфейсов, чтобы выбрать интерфейсы, которые могут находиться в состоянии «Selected» -

выбран, таким образом достигая согласованности относительно того, что интерфейсы находятся в состоянии «Selected».

Операционный ключ автоматически генерируется элементом управления агрегацией на основе определенных конфигураций портов участников во время агрегации каналов. Этот ключ включает скорость порта, дуплексный режим, состояние включен/выключен, разрешенные на порту VLAN, VLAN ID по умолчанию для порта и тип канала порта (Trunk, Hybrid, Access). В агрегированной группе порты участники в состоянии «Selected» имеют одинаковый операционный ключ.

14.2 Ручное агрегирование каналов

Ручное агрегирование каналов в режиме распределения нагрузки — это широко используемый метод агрегирования каналов. Большинство сетевых устройств корпоративного уровня поддерживают эту функцию. Когда необходимо обеспечить большую пропускную способность канала между двумя напрямую подключенными устройствами, а соседнее устройство не поддерживает протокол LACP, можно использовать режим агрегации каналов вручную.

14.3 Статическая агрегация каналов

Статическая агрегация каналов в режиме LACP — это режим агрегации, который использует протокол LACP для согласования параметров для выбора активных каналов. Этот режим определяется протоколом LACP для идентификации активных и неактивных каналов в группе агрегации, обеспечивая более высокую надежность канала. Статические группы агрегации создаются вручную, а добавление допустимых портов определяется посредством согласования LACP. Статические группы агрегации создаются вручную.

14.4 Список команд агрегации каналов

14.4.1 Общая конфигурация агрегации каналов

Таблица 50 – Общая конфигурация агрегации каналов

Команда	Описание	Режим
lag group <aggr-id> mode (static | lacp-negotiation)	Создать агрегированную группу и указать шаблон	“(config)#”
[no] interface lag <aggr-id>	Удалить/Войти в группу агрегации	“(config)#”
[no] lag group <aggr-id>	Удалить/добавить порты участники	“(config-eth)”
[no] lacp system-priority <system-priority>	Восстановить/настроить приоритет системы	“(config)#”
[no] lacp port-priority <system-priority>	Восстановить/настроить приоритет LACP для портов	“(config-eth)”
[no] description <WORD>	Описать информацию для отмены/настройки интерфейсов агрегации.	“(config-lag)”
[no] lag load-balance (both-ip | both-mac | dst-mac | src-mac)	Восстановить/настроить типы распределения нагрузки	“(config)#”
clear lacp statistics (all | interface <interface-type> <interface-number>)	Очистить статистику пакетов LACP порта	“(config)#”
debugging lacp (all | error | event | state | packet) (all | interface <interface-type> <interface-number>) (on | off)	Включить отладку агрегации для портов	“(config)#”

14.4.2 Просмотр информации об агрегации

Таблица 51 – Просмотр информации об агрегации

Команда	Описание	Режим
show lag load-balance	Показать типы распределения нагрузки	“#”
show lacp interface <interface-type> <interface-number>	Показать информацию об интерфейсах агрегации	“#”
show lag <aggr-id> (detail | summary)	Показать информацию о группе агрегации	“#”
show lag	Показать сводную информацию о группе агрегации	“#”
show lacp statistics interface <interface-type> <interface-number>	Показать статистику пакетов LACP для портов	“#”
show debugging lacp switch	Показать информацию отладки LACP коммутатора	“#”
show debugging lacp lag (all | <aggr-id>)	Показать информацию отладки о группе агрегации	“#”

show debugging lacp aggrport (lag <aggr-id> | interface <interface-type> <interface-number>)	Показать информацию отладки о порте агрегации	“#”

14.5 Пример Настройки

14.5.1 Описание задач для настройки

Таблица 52 – Задачи для настройки

Критерий задач конфигурации	Описание
Создать группы агрегации и указать шаблон	Необходимый
Порт участник	Необходимый
Системный приоритет	Необязательный
LACP-приоритет порта	Необязательный
Тип распределения нагрузки	Необязательный
Очистить статистику пакетов LACP для порта	Необязательный
Отладки агрегации для портов	Необязательный

14.5.2 Пример настройки

1. Требования сети

— DUT1 и DUT2 связаны посредством статической агрегации.

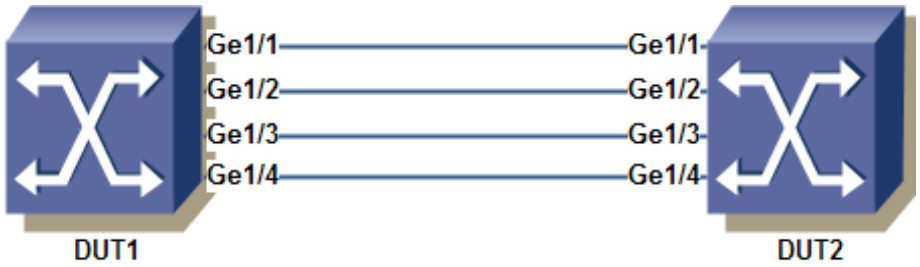

Рисунок 17 - Схема топологии сети

2. План настройки

— Создать статическую группу агрегации и присоединить к портам с 1 по 4.

3. Шаги настройки

（1）Создать статическую группу агрегации и назначить порты.

#Настройка DUT1

DUT1# configure

DUT1(config)# lag group 1 mode static

DUT1(config)# interface ethernet 1/0/1
DUT1(config-eth1/0/2)# lag group 1
DUT1(config-eth1/0/1)# interface ethernet 1/0/2
DUT1(config-eth1/0/2)# lag group 1
DUT1(config-eth1/0/2)# interface ethernet 1/0/3
DUT1(config-eth1/0/3)# lag group 1
DUT1(config-eth1/0/3)# interface ethernet 1/0/4
DUT1(config-eth1/0/4)# lag group 1
#Настройка DUT2
DUT2# configure
DUT2(config)# lag group 1 mode static
DUT2(config)# interface ethernet 1/0/1
DUT2(config-eth1/0/2)# lag group 1
DUT2(config-eth1/0/1)# interface ethernet 1/0/2
DUT2(config-eth1/0/2)# lag group 1
DUT2(config-eth1/0/2)# interface ethernet 1/0/3
DUT2(config-eth1/0/3)# lag group 1
DUT2(config-eth1/0/3)# interface ethernet 1/0/4
DUT2(config-eth1/0/4)# lag group 1

4. Проверка конфигурации
Просмотр статуса группы агрегации на DUT1
DUT1(config)# show lag 1 detail
Lag : Lag1
Description : LAG1
Port Type : eth1000M
Port Status : 1000M/FDX
Auto Negotiation: Enabled
Lag Speed : auto
Flow Control : Disabled
Fast leave : disable
Type : static
Load Mode : both-ip
Operate status : UP

Ports | Status

```
        eth1/0/1  |    Active
        eth1/0/2  |    Active
        eth1/0/3  |    Active
        eth1/0/4  |    Active

# Просмотр статуса группы агрегации на DUT2
DUT2(config)# show lag 1 detail
Lag             : Lag1
Description     : LAG1
Port Type       : eth1000M
Port Status     : 1000M/FDX
Auto Negotiation: Enabled
Lag Speed       : auto
Flow Control    : Disabled
Fast leave      : disable
Type            : static
Load Mode       : both-ip
Operate status  : UP
------------------------------------------------------------
          Ports  |    Status
        eth1/0/1  |    Active
        eth1/0/2  |    Active
        eth1/0/3  |    Active
        eth1/0/4  |    Active
```

15 IGMP SNOOPING/ОТСЛЕЖИВАНИЕ IGMP

Функция IGMP SNOOPING (отслеживание) коммутатора обслуживает многоадресные приложения. Она прослушивает сообщения IGMP в сети, облегчая динамическое изучение MAC-адресов многоадресной рассылки IP. Это позволяет коммутаторам уровня 2 эффективно управлять и ограничивать multicast трафик.

В этой главе представлен обзор и подробности настройки IGMP SNOOPING:

- Введение в IGMP SNOOPING;
- Настройка IGMP SNOOPING;
- Пример настройки IGMP SNOOPING.

15.1 Введение в IGMP SNOOPING

В традиционных сетях многоадресные пакеты внутри подсети рассматриваются как широковещательные, что приводит к увеличению сетевого трафика и перегрузке. Благодаря реализации IGMP SNOOPING на коммутаторах MAC-адреса многоадресной рассылки, связанные с IP, изучаются динамически. Это поддерживает список выходных портов для MAC-адресов многоадресной IP-адресации, гарантируя, что многоадресный трафик пересылается только на назначенные выходные порты, тем самым уменьшая перегрузку сети.

В этом разделе рассматриваются следующие темы:

- Процесс IGMP SNOOPING;
- Динамическая многоадресная рассылка уровня 2;
- Присоединение к группе;
- Выход из группы.

15.1.1 Процесс IGMP SNOOPING

IGMP SNOOPING — это сетевой протокол уровня 2, который прослушивает пакеты протокола IGMP, проходящие через коммутатор. Он поддерживает группу многоадресной рассылки на основе порта приема, идентификатора VLAN и адреса многоадресной рассылки этих пакетов протокола IGMP и пересылает их соответствующим образом. Только порты,

присоединившиеся к группе многоадресной рассылки, могут получать muticast потоком, что снижает сетевой трафик и сохраняет полосу пропускания.

Группа многоадресной рассылки включает в себя адрес группы многоадресной рассылки, порты участники, идентификатор VLAN и время устаревания. Формирование групп многоадресной рассылки в IGMP SNOOPING — это процесс обучения. Когда порт коммутатора получает пакет IGMP REPORT, IGMP SNOOPING создает новую группу многоадресной рассылки, и порт, получающий пакет IGMP REPORT, добавляется в эту группу многоадресной рассылки. Когда коммутатор получает пакет IGMP QUERY, если группа многоадресной рассылки уже существует в коммутаторе, порт, получающий IGMP QUERY, также добавляется в эту группу многоадресной рассылки; в противном случае пакет IGMP QUERY пересылается. IGMP SNOOPING также поддерживает механизм выхода из IGMP V2; Если IGMP SNOOPING настроен с включенным быстрым выходом (fast-leave), при получении пакета выхода IGMP V2 принимающий порт может немедленно покинуть группу многоадресной рассылки.

IGMP SNOOPING имеет два механизма обновления. Одним из них является механизм leave, описанный выше. В большинстве случаев IGMP SNOOPING удаляет группы многоадресной рассылки с истекшим сроком действия по мере устаревания. Когда группа многоадресной рассылки присоединяется к IGMP SNOOPING, время присоединения записывается. Если группа многоадресной рассылки остается в коммутаторе дольше настроенного времени устаревания, коммутатор удаляет группу многоадресной рассылки.

Когда порт получает пакет протокола Leave, порт немедленно удаляется из группы многоадресной рассылки, к которой он принадлежит. Эта ситуация может повлиять на непрерывность сетевых потоков данных, поскольку порт может быть подключен к сетевому устройству без функции IGMP SNOOPING, на котором множество устройств получают потоки многоадресных данных. Отправка пакета Leave с одного устройства может повлиять на способность других устройств получать потоки многоадресных данных.

11.1.2 Динамическая многоадресная рассылка уровня 2

Записи MAC-адреса многоадресной рассылки в аппаратной таблице пересылки multicast уровня 2 могут быть динамически узучены с помощью IGMP SNOOPING. IGMP SNOOPING динамически изучает MAC-адрес IP multicast.

Когда IGMP SNOOPING отключен на коммутаторе, аппаратная таблица многоадресной пересылки уровня 2 находится в незарегистрированном режиме пересылки, MAC-адреса многоадресной рассылки не могут быть изучены динамически, и в аппаратной таблице многоадресной пересылки уровня 2 нет записей. Все потоки многоадресных данных уровня 2 рассматриваются как широковещательные.

Если в сети есть multicast, для эффективного управления многоадресным трафиком коммутатор может включить IGMP SNOOPING. В этот момент аппаратная таблица многоадресной пересылки уровня 2 находится в зарегистрированном режиме пересылки. Коммутатор может узнать MAC-адреса многоадресной рассылки, прослушивая пакеты протокола IGMP в сети. Пересылаться могут только потоки многоадресной рассылки уровня 2, соответствующие записям в аппаратной таблице многоадресной пересылки уровня 2.

11.1.3 Присоединение к группе

Когда хост хочет присоединиться к группе многоадресной рассылки, он отправляет пакет IGMP REPORT, указывающий группу многоадресной рассылки, к которой он хочет присоединиться. Когда коммутатор получает пакет IGMP QUERY, он пересылает его на все остальные порты в том же VLAN. Когда хосты за портами, желающие присоединиться к группе многоадресной рассылки, получают пакет IGMP QUERY, они отвечают пакетом IGMP REPORT. Когда коммутатор получает пакет IGMP REPORT, он создает запись многоадресной рассылки уровня 2. Порты, которые получают пакет IGMP QUERY, и порты, которые получают пакет IGMP REPORT, добавляются в эту запись многоадресной рассылки уровня 2 в качестве выходных портов.

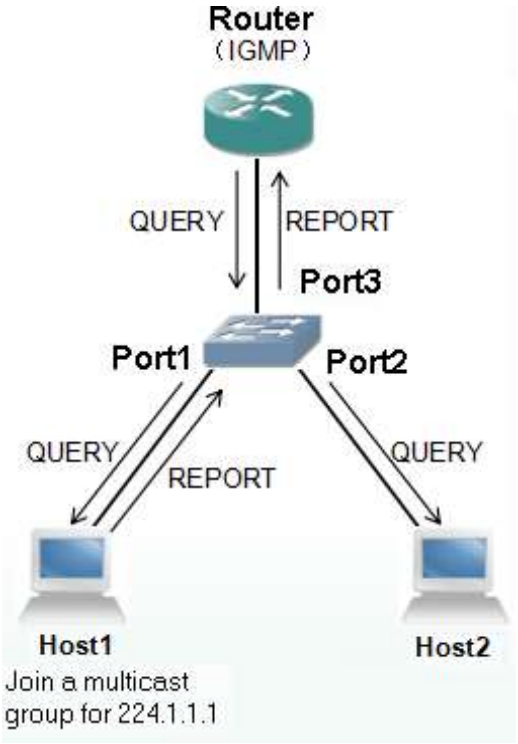

Рисунок 18 – Присоединение к группе

Все устройства на диаграмме выше находятся в одной подсети, при условии, что VLAN этой подсети равен 2. Маршрутизатор использует протокол IGMPv2 и периодически отправляет пакеты IGMP QUERY. Хост 1 хочет присоединиться к группе многоадресной рассылки 224.1.1.1. Когда коммутатор получает пакет IGMP QUERY от порта 3, он записывает этот порт и пересылает пакет на порты 1 и 2. Хост 1 отвечает на пакет IGMP QUERY, отправляя пакет IGMP REPORT, тогда как Хост 2, не заинтересованный в присоединении к группе многоадресной рассылки, не отправляет пакет IGMP REPORT. Когда коммутатор получает пакет IGMP REPORT от порта 1, он пересылает пакет из запрашивающего порта 3 и создает запись многоадресной рассылки уровня 2 (при условии, что эта запись не существует). Запись многоадресной рассылки уровня 2 включает следующие элементы:

Таблица 53 – Элементы записи многоадресной рассылки второго уровня

Адрес многоадресной рассылки уровня 2	VLAN ID	Список выходных портов
01:00:5e:01:01:01	2	Port1, Port 3

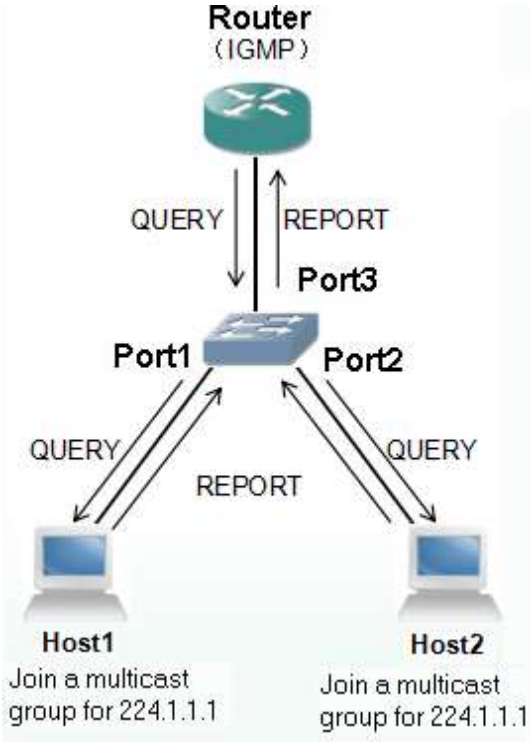

Рисунок 19 - Элементы записи многоадресной рассылки второго уровня

В том же сценарии, который изображен на диаграмме выше, где Host 1 уже присоединился к группе многоадресной рассылки 224.1.1.1, теперь Host 2 желает присоединиться к той же группе многоадресной рассылки. Получив пакет IGMP QUERY, Host 2 отвечает отправкой пакета IGMP REPORT. Когда коммутатор получает пакет IGMP REPORT от порта 2, он пересылает пакет от запрашивающего порта 3 и добавляет порт 2 к записи многоадресной рассылки уровня 2. Запись многоадресной рассылки уровня 2 становится:

Таблица 54 – Адрес многоадресной рассылки второго уровня

Адрес многоадресной рассылки уровня 2	VLAN ID	Список выходных портов
01:00:5e:01:01:01	2	Port 1, Port 2, Port 3

15.1.2 Выход из группы

Чтобы обеспечить создание стабильной среды многоадресной рассылки, устройства, использующие IGMP (например, маршрутизаторы), периодически отправляют пакет IGMP QUERY всем хостам. Хосты, которые уже присоединились к группе многоадресной рассылки или желают присоединиться к ней, отвечают на этот IGMP QUERY, отправляя IGMP REPORT.

У хоста есть два способа покинуть группу многоадресной рассылки: активно и пассивно. Активный выход предполагает, что хост отправляет маршрутизатору пакет IGMP LEAVE, тогда как пассивный выход происходит, когда хост, получив IGMP QUERY от маршрутизатора, не отвечает IGMP REPORT.

В соответствии с тем, как хосты покидают группы многоадресной рассылки, существует также два способа выхода портов коммутатора из записей многоадресной рассылки уровня 2: выход по таймауту и выход после получения пакета IGMP LEAVE.

Если коммутатор не получил пакет IGMP REPORT для группы многоадресной рассылки от порта в течение определенного периода времени, порт удаляется из соответствующей записи многоадресной рассылки уровня 2. Если в записи многоадресной рассылки уровня 2 не осталось портов, запись удаляется.

Если в конфигурации коммутатора установлено значение ENABLE для функции fast-leave, то если порт получает пакет IGMP LEAVE для группы многоадресной рассылки, порт удаляется из соответствующей записи многоадресной рассылки уровня 2. Если в записи многоадресной рассылки уровня 2 не осталось портов, запись удаляется.

15.2 MVR (Multicast VLAN Registration)/ Регистрация многоадресной сети VLAN

MVR (Multicast VLAN Registration) решает проблему лавинной рассылки (flooding), когда получатели находятся в разных VLAN. Он использует выделенный, настроенную вручную VLAN, называемый Multicast VLAN, для пересылки многоадресного трафика в сетях уровня 2.

Он также может работать в сочетании с IGMP Snooping.

15.2.1 Операции MVR

После настройки Multicast VLAN на устройствах уровня 2 устройствам уровня 3 необходимо только реплицировать данные многоадресной рассылки внутри многоадресного VLAN и отправлять их на устройства уровня 2, а не реплицировать их в каждой пользовательской VLAN. Это экономит пропускную способность сети и снижает нагрузку на устройства уровня 3.

Implementation Mode – Multicast VLAN на основе sub-VLANs

Несколько получателей находятся в разных пользовательских VLAN. Настройте вышестоящий VLAN как многоадресный VLAN, сделайте все пользовательские VLAN sub-VLAN восходящей VLAN и включите IGMP Snooping в Multicast VLAN.

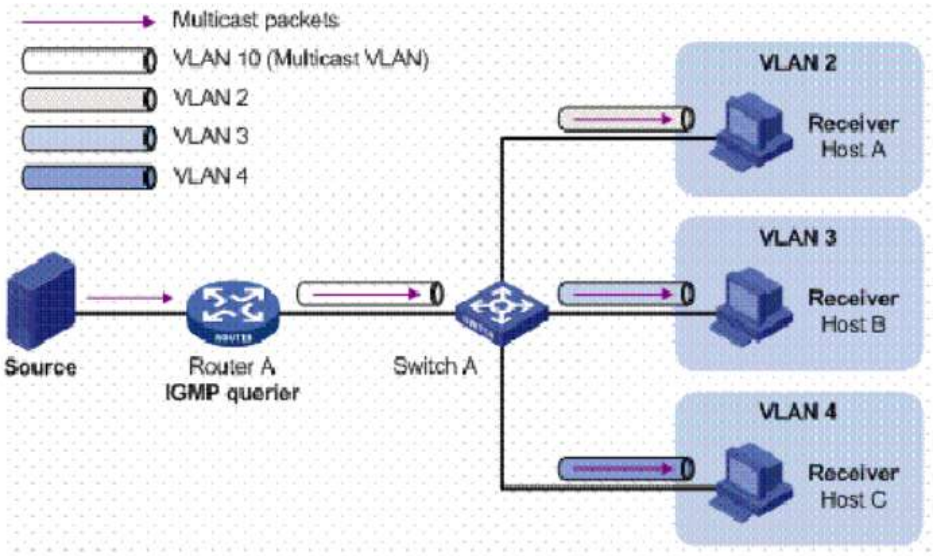

Рисунок 20 - Implementation Mode – Multicast VLAN на основе sub-VLANs

После настройки IGMP Snooping будет поддерживать порты маршрутизатора в Multicast VLAN и порты-участники в каждой sub-VLAN. Таким образом, RouterA необходимо отправить только одну копию многоадресных пакетов SwitchA, который затем распределит их по sub-VLAN с получателями в Multicast VLAN.

15.3 Настройка IGMP SNOOPING

15.3.1 Настройки IGMP SNOOPING по умолчанию

По умолчанию отслеживание IGMP отключено.

По умолчанию быстрый выход отключен.

Время устаревания портов маршрутизатора по умолчанию составляет 105 секунд.

Время устаревания хост-портов по умолчанию составляет 260 секунд.

Запросы отключены по умолчанию.

15.3.2 Общая настройка IGMP SNOOPING

Протокол IGMP Snooping можно включить глобально или индивидуально для конкретных VLAN. Только когда IGMP Snooping включен глобально, включение или отключение IGMP Snooping для конкретной VLAN может вступить в силу.

Таблица 55 – Команды общей настройки IGMP SNOOPING

Команда	Описание	Режим
[no] igmp-snooping	Отключить/включить отслеживание IGMP	“(config)#”/ “(vlan)#”
[no] multicast unknown-drop	Настройка политики неизвестного multicast	“(vlan)#”
[no] debugging igmp snooping (pkt | ipc | timer | event)	Отключить/включить отладку IGMP SNOOPING	“(config)#”
clear igmp snooping statistic	Очистить статистику IGMP SNOOPING	“#”
[no] igmp snooping max-groups <number>	Восстановить/настроить ограничение группы многоадресной рассылки	“(vlan)#”
igmp snooping version (v1/2 | v3)	Настроить версии IGMP Snooping	“(vlan)#”

15.3.3 Настройка временных интервалов

Таблица 56 – Настройка временных интервалов

Команды	Описание	Режим
[no] igmp snooping router-aging-time <interval>	Восстановить/настроить время устаревания порта маршрутизации	“(vlan)#”
[no] igmp snooping host-aging-time <interval>	Восстановить/настроить время устаревания порта участника	“(vlan)#”

15.3.4 Настройка Fast-leave

Таблица 57 – Настройка Fast-leave

Команды	Описание	Режим
[no] igmp snooping fastleave	Отключить/включить режим fastleave	“(config-eth)#”
[no] igmp snooping fastleave	Отключить/включить режим fastleave	“(vlan)#”

15.3.5 Конфигурация статической маршрутизации

Таблица 58 – Команды Конфигурации статической маршрутизации

Команды	Описание	Режим
[no] multicast static-router-port vlan <vlan-id>	Отменить/настроить порты статической маршрутизации	“(config-eth)#”
[no] multicast static-router-port <interface-list>	Отменить/настроить порты статической маршрутизации	“(vlan)#”
[no] multicast static-group <group-address> vlan <vlan-id>	Отменить/настроить статические порты участники	“(config-eth)”
[no] multicast static-group <group-address> interface <interface-list>	Удалить/настроить статических портов участники	“(vlan)#”

15.3.6 Настройка запроса

Таблица 59 – Команды настройки запросов

Команды	Описание	Режим
igmp snooping (querier | proxy)	Настроить режим работы	“(vlan)#”
[no] igmp snooping general-query source-ip <ip>	Восстановить/настроить исходный IP-адрес сообщений запросов.	“(vlan)#”
[no] igmp snooping max response-time <interval>	Восстановить/настроить максимальное время ответа	“(vlan)#”
[no] igmp snooping general-query interval <interval>	Восстановить/настроить время запроса опрашивателя	“(vlan)#”

15.3.7 Просмотр информации

Таблица 60 – Команды для просмотра информации

Команды	Описание	Режим
show igmp snooping vlan (all | <vlan-id>)	Показать статус VLAN IGMP SNOOPING	“#”
show igmp group	Показать конфигурацию IGMP SNOOPING	“#”
show igmp snooping statistic	Показать статистику IGMP SNOOPING	“#”

15.3.8 Общая конфигурация MVR

Таблица 61 -Команды общей конфигурация MVR

Команды	Описание	Режим
[no] multicast-vlan enable	Включить multicast VLAN	“(vlan)#”
[no] multicast-vlan user-vlan <vlan-id1> [to <vlan-id2>]	Привязать пользовательский VLAN	“(vlan)#”

15.4 Пример настройки IGMP SNOOPING

15.4.1 Описание задач для настройки

Таблица 62 - Описание задач для настройки

Критерий задач конфигурации	Описание
Включить igmp snooping	Необходимый
Политика неизвестной многоадресной рассылки	Необходимый
Настроить исходный IP-адрес сообщений запроса	Необязательный
Настроить режим работы	Необязательный
Статический участник/порт маршрутизации	Необязательный
Конфигурация таймера	Необязательный
Ограничить группы многоадресной рассылки	Необязательный
Очистить статистику сообщений IGMP SNOOPING	Необязательный

15.4.2 Пример настройки

1. Требования сети

— Коммутатор контролирует многоадресные сообщения.

— Коммутатор контролирует группы многоадресной рассылки vlan 1, 200 и 300.

— Участники 1, 2 и 3 могут присоединяться к группе многоадресной рассылки или выйти из нее.

Таблица 63

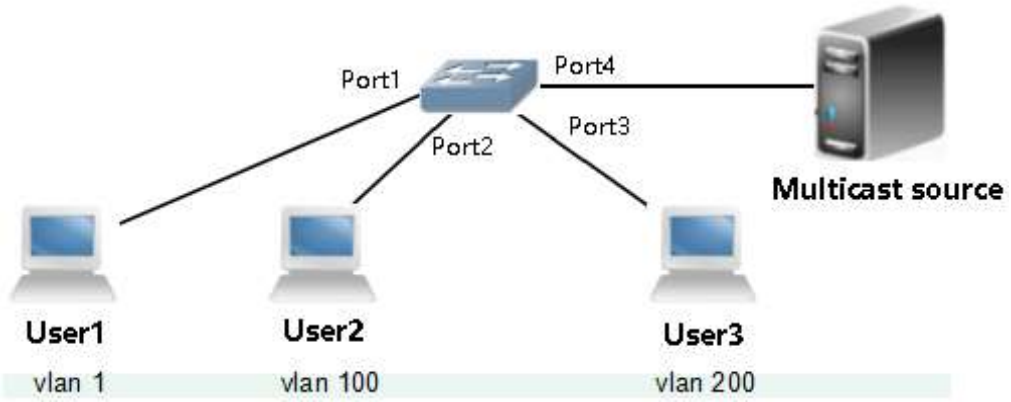

Рисунок 21 - Схема топологии сети

2. План настройки

— Создать VLAN 1, 100 и 200, настроить PVID 100 для Порта 2, PVID 200 для Порта 3, Trunk для Порта 4 и разрешить все VLAN..

— Включить igmp snooping и связать vlan1, 100, 200.

— Включить режим fastleave для igmp snooping vlan 1, 100 и 200.

3. Шаги настройки

（1）Создать VLAN и настроить VLAN на портах.

```
SWITCH# configure
SWITCH(config)# vlan 100,200
SWITCH(config)# interface ethernet 1/0/2
SWITCH(config-eth1/0/2)# switchport access vlan 100
SWITCH(config-eth1/0/2)# interface ethernet 1/0/3
SWITCH(config-eth1/0/3)# switchport access vlan 200
SWITCH(config-eth1/0/3)# interface ethernet 1/0/4
SWITCH(config-eth1/0/4)# switchport mode trunk
SWITCH(config-eth1/0/4)# switchport trunk allowed all
```

（2）Включить igmp snooping и привязать VLAN

```
SWITCH(config)# igmp snooping
SWITCH(config)# vlan 1
SWITCH(Vlan1)# igmp snooping
SWITCH(Vlan1)# vlan 100
SWITCH(Vlan100)# igmp snooping
WITCH(Vlan100)# vlan 200
SWITCH(Vlan100)# igmp snooping
```

（3）Настроить режим fastleave IGMP SNOOPING для VLAN 1, 100, 200,

```
SWITCH(Vlan1)# igmp snooping fastleave
SWITCH(Vlan1)# vlan 100
SWITCH(Vlan100)# igmp snooping fastleave
SWITCH(Vlan100)# vlan 200
SWITCH(Vlan200)# igmp snooping fastleave
```

4. Проверка конфигурации

```
# Просмотр конфигурации IGMP SNOOPING:
SWITCH(config)# show igmp snooping vlan all
vlan 1
 igmp snooping
 igmp snooping fastleave
vlan 100
 igmp snooping
 igmp snooping fastleave
```

```
vlan 200
 igmp snooping
 igmp snooping fastleave
```

16 DHCP SNOOPING/ ОТСЛЕЖИВАНИЕ DHCP

В этой главе представлено подробное описание команд CLI:

– DHCP SNOOPING;

– Option82.

16.1 Введение в DHCP SNOOPING

DHCP SNOOPING (отслеживание) — это функция безопасности DHCP, которая фильтрует ненадежную информацию DHCP путем создания и поддержания таблицы привязки DHCP SNOOPING. Эта информация относится к сообщениям DHCP, исходящим из ненадежных областей.

Таблица привязки DHCP-отслеживание содержит MAC-адреса, IP-адреса, периоды аренды, идентификаторы VLAN и информацию об интерфейсах из ненадежных областей. Назначив, доверенные и не доверенные порты, можно изолировать незаконные DHCP-серверы. Доверенные порты обычно пересылают предложения DHCP и пакеты DHCPACK, в то время как не доверенные порты отбрасывают DHCP offers и пакеты DHCPACK, полученные от неавторизованных серверов.

16.2 Настройка DHCP SNOOPING

16.2.1 Настройка DHCP SNOOPING

Таблица 64 – Команды настройки DHCP SNOOPING

Команды	Описание	Режим
[no] ip dhcp snooping	Отключить/включить DHCP SNOOPING	“(config)#”
[no] ip dhcp snooping verify mac-address	Отключить/включить проверку MAC-адреса источника	“(config)#”
[no] ip dhcp snooping static <ip-address> <mac-address> vlan <vlan-id> interface <interface-type> <interface-number>	Удалить/добавить статическте записи таблицы пользователей	“(config)#”
ip dhcp snooping auto-static	Преобразовать все записи динамической таблицы в записи статической таблицы.	“(config)#”
clear ip dhcp snooping bind (all | static | dynamic)	Очистить таблицу пользователей DHCP snooping по типу	“(config)#”
[no] ip dhcp snooping trust	Отключить/включить доверенные порты	Interface Configuration Mode
[no] ip dhcp snooping source-check	Отключить/включить защиту IP-источника	Interface Configuration Mode
ip dhcp snooping debug (none | pktinfo | options | dhcpinfo | all)	Отладить настройку DHCP-snooping	“(config)#”

16.2.2 Просмотр информации DHCP SNOOPING

Таблица 65 – команды просмотра информации DHCP SNOOPING

Команды	Описание	Режим
show ip dhcp snooping	Показать информацию о конфигурации DHCP-snooping	“#”
show ip dhcp snooping binding-table	Показать информацию о привязке пользователя DHCP-snooping	“#”

16.3 DHCP option82

Опция 82 — это опция информации агента ретрансляции (Relay Agent) в сообщениях DHCP. Когда клиент DHCP отправляет запрос на сервер DHCP и ему необходимо пройти через ретранслятор DHCP, агент ретрансляции добавляет Option 82 к сообщению запроса. Опция 82 включает в себя несколько подопций. Подопция 1 определяет идентификатор канала Circuit ID, а подопция 2 определяет Remote ID, который включает IP-адрес, добавленный DHCP relay.

Option 82 позволяет получать информацию об адресах DHCP-клиентов и устройств DHCP-relay на DHCP-сервере.

16.3.1 Настройка DHCP option82

Таблица 66 – Команды настройки DHCP option82

Команды	Описание	Режим
[no] ip dhcp snooping information	Отключить/включить option82	“(config)#”
ip dhcp snooping information strategy (drop|keep|replace)	Настроить политику обработки option82	“(config)#”
[no] ip dhcp snooping information circuit-id (string | hex) <information-string>	Отменить/Настроить circuit-id	“(config)#”
[no] ip dhcp snooping information remote-id (string | hex) <information-string>	Отменить/Настроить remote-id	“(config)#”

16.4 Пример настройки

16.4.1 Описание задач для настройки

Таблица 67 - Задачи для настройки

Критерий задач конфигурации	Описание
Включить DHCP SNOOPING	Необходимый
Настроить доверенные порты	Необходимый
Конфигурация Option82	Необязательный
Проверка исходного MAC-адреса	Необязательный
Настроить статические записи таблицы пользователей	Необязательный
Защита IP-источник	Необязательный
Отладить настройку DHCP Snooping	Необязательный

16.4.2 Пример настройки

1. Требования к сети

— Клиент DHCP может получить IP-адрес, назначенный DHCP-сервером.

— Адрес, назначенный незаконным DHCP-сервером, не будет действовать для DHCP-клиенте.

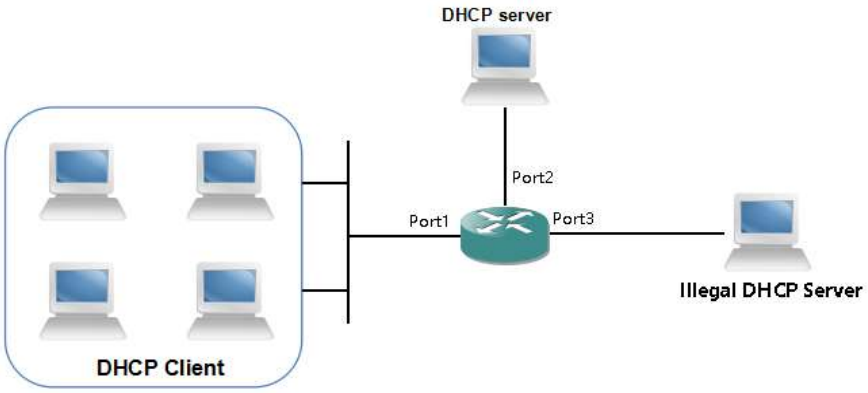

Рисунок 22 – Схема топологии сети

2. План настройки

— Включить DHCP SNOOPING

— Настроить Порт 2 как доверенный порт

— Настроить Порт 3 как недоверенный порт

3. Шаги настройки

（1）Включить DHCP SNOOPING

SWITCH# configure

SWITCH(config)# ip dhcp snooping

（2）Настроить Порт 2 как доверенный порт

SWITCH(config)# interface ethernet 1/0/2

SWITCH(config-eth1/0/2)# ip dhcp snooping trust

Настроить Порт 3 как недоверенный порт

SWITCH(config-eth1/0/2)# interface ethernet 1/0/3

SWITCH(config-eth1/0/3)# no ip dhcp snooping trust

4. Проверка конфигурации

Просмотр конфигурации DHCP SNOOPING

```
SWITCH(config)# show ip dhcp snooping
 Snooping Enable:Enable.
 Snooping Mac verify:Disable.
 Snooping Option82 Enable:Disable.
 Snooping Option82 Mode:Keep.
 Option82 Circuit-id:SWITCH(string)
 Option82 Remote-id:18c3f4b0129d(hex)
 Snooping Trust Port:eth1/0/2
 IP Source Guard:
# Просмотр таблицы привязки DHCP Snooping
SWITCH(config)# show ip dhcp snooping binding-table
-------------------------------------------------------------------------------------------------------------------------------
--
Index Client-IP   MAC     VLAN Client-UNILeaseTime  Timer Mode    HardSync
1  192.168.1.100  EC:22:80:EB:BA:36  1       eth1/0/2     1800     1830    dynamic    no
-------------------------------------------------------------------------------------------------------------------------------
--
```

17 DHCP RELAY/ АГЕНТ РЕТРАНСЛЯЦИИ DHCP

В этой главе представлено подробное описание DHCP Relay:

– Введение в DHCP Relay;

– Настройка DHCP Relay.

17.1 Введение в DHCP Relay

DHCP Relay (DHCPR), также известный как DHCP Relay Agent.

Если DHCP-клиент и DHCP-сервер находятся в одной физической подсети, клиент может правильно получать динамически выделяемые IP-адреса. Однако если они не находятся в одной физической подсети, требуется агент ретрансляции DHCP. DHCP Relay Agent устраняет необходимость в DHCP-сервере в каждой физической подсети. Он может пересылать сообщения на DHCP-серверы, расположенные в разных физических подсетях, а также ретранслировать сообщения сервера обратно DHCP-клиентам, не находящимся в той же физической подсети.

17.1.1 Принцип DHCP Relay

1. Когда DHCP-клиент запускается и инициирует инициализацию DHCP, он передает сообщение с запросом конфигурации в локальную сеть.

2. Если в локальной сети присутствует DHCP-сервер, настройку DHCP можно выполнить напрямую, без необходимости использования DHCP Relay.

3. Если в локальной сети нет DHCP-сервера, сеть с функцией DHCP Relay, подключенная к локальной сети, получает широковещательное сообщение и обрабатывает его соответствующим образом, пересылая на назначенный DHCP-сервер в другой сети.

4. DHCP-сервер настроенный соответствующим образом, на основе информации, предоставленной DHCP-клиентом отправляет информацию о конфигурации DHCP-клиенту через DHCP Relay, завершая динамическую настройку DHCP-клиента.

17.2 Конфигурация DHCP Relay

17.2.1 Настройка DHCP Relay

Таблица 68 – Команды для настройки DHCP Relay

Команды	Описание	Режим
[no] ip dhcp relay	Отключить/Включить DHCP Relay	“(config)#”
ip dhcp relay (enable | disable)	Отключить/включить виртуальный DHCP Relay	“(Vlan-interface)#”
ip dhcp relay dscp <dscp>	Настроить DSCP для сообщений DHCP	“(config)#”
[no] ip dhcp relay giaddr <ip-address>	Отменить/настроить IP-адрес шлюза для сообщений DHCP	“(Vlan-interface)#”
[no] ip dhcp relay server-address <ip-address>	Удалить/настроить IP-адрес сервера для сообщений DHCP	“(Vlan-interface)#”
ip dhcp relay debug (none | pktinfo | options | dhcpinfo | all)	Команда отладки	“(config)#”

17.2.2 Настройка Option 60

Таблица 69 – Команды для настройки Option 60

Команды	Описание	Режим
[no] ip dhcp relay option60	Отключить/Включить Option 60	“(config)#”
ip dhcp relay option60 device-type <device-type> prefix (string | hex) <prefix-word>	Создать тип устройства Option 60	“(config)#”
no ip dhcp relay option60 device-type <device-type>	Удалить указанный тип устройства	“(config)#”
no ip dhcp relay option60 device-type <device-type> prefix (string | hex) <prefix-word>	Удалить сопоставление между Option 60 и типом устройства.	“(config)#”
[no] ip dhcp relay option60 device-type <device-type> server-address <ip-address>	Отвязать/привязать сервер	“(config)#”

17.2.3 Конфигурация Option82

Таблица 70 – Команды конфигурации Option82

Команды	Описание	Режим
[no] ip dhcp relay information	Отключить/Включить Option 82	“(Vlan-interface)#”
ip dhcp relay information strategy (drop | keep | replace)	Option 82 политика обработки	“(Vlan-interface)#”
[no] ip dhcp relay information circuit-id (string | hex) <information-string>	Отменить/настроить идентификатор цепи Option82	“(Vlan-interface)#”
[no] ip dhcp relay information remote-id (string | hex) <information-string>	Отменить/настроить удаленный идентификатор Option82	“(Vlan-interface)#”

17.2.4 Просмотр информации о DHCP Relay

Таблица 71 – Команды для просмотра информации о DHCP Relay

Команды	Описание	Режим
show ip dhcp relay	Показать информацию о конфигурации DHCP Relay	“#”
show ip dhcp relay option60 device-type	Показать сопоставление всех типов устройств с Option 60	“#”
show ip dhcp relay option60 server-address	Показать информацию о привязке сервера	“#”
show ip dhcp relay client-information	Показать таблицу привязки пользователей DHCP Relay	“#”

17.3 Пример настройки

17.3.1 Критерий задач конфигурации

Таблица 72 - Критерий задач конфигурации

Критерий задач конфигурации	Описание
Включить глобально DHCP Relay	Необходимый
Настроить IP-адрес сервера для пакетов DHCP	Необходимый
Включить DHCP Relay виртуального интерфейса	Необходимый
Настроить Option 60	Необязательный
Настроить Option 82	Необязательный

17.3.2 Пример настройки

1. Требования к сети

— DHCP-клиент может получить адрес, назначенный DHCP-сервером.

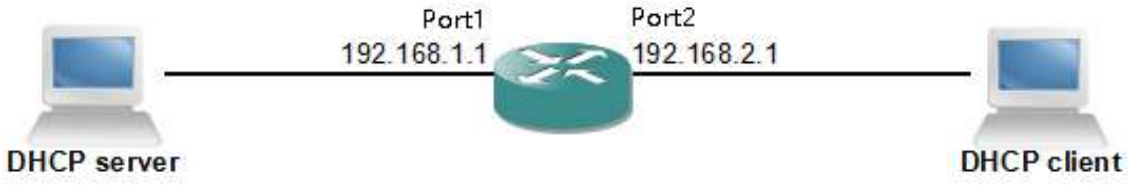

Рисунок 23 - Схема топологии сети

2. План настройки

— Настроить виртуальные интерфейсы и порты VLAN.

— Включить DHCP relay

— Настроить DHCP сервер сообщений

3. Шаги настройки

（1）Настроить виртуальные интерфейсы и порты VLAN

```
SWITCH# configure
SWITCH(config)# interface ethernet 1/0/2
SWITCH(config-eth1/0/2)# switchport access vlan 2
SWITCH(config-eth1/0/2)# exit
SWITCH(config)# interface vlan-interface 1
SWITCH(Vlan-interface1)# ip address 192.168.1.1 255.255.255.0
SWITCH(Vlan-interface1)# interface vlan-interface 2
```

SWITCH(Vlan-interface2)# ip address 192.168.2.1 255.255.255.0

（2）Включить DHCP relay

SWITCH(config)# ip dhcp relay

（#）Включить виртуальный DHCP relay

SWITCH(Vlan-interface1)# interface vlan-interface 2

SWITCH(Vlan-interface2)# ip dhcp relay enable

（4）Настроить сервер DHCP сообщений

SWITCH(config)# interface vlan-interface 2

SWITCH(Vlan-interface2)# ip dhcp relay server-address 192.168.1.5

4. Проверка конфигурации

Просмотр конфигурации DHCP relay

SWITCH(config)# show ip dhcp relay

Dhcp Relay Enable:Enable.

Dhcp Relay Option60: disable.

Dhcp Relay DSCP:56

Просмотр конфигурации виртуальных интерфейсов

SWITCH(config)# show interface vlan-interface 2

Vlan-interface 2

Hardware Address : 18:C3:f4:b0:12:9d

Mtu : 1500

Current state :UP

Protocol :Static

Internet Address : 192.168.2.1/255.255.255.0

Input: 476985bytes 6736packets 0drops 44multecasts

Output: 10885175bytes 11630packets 0drops

Dhcp-Relay enable: Enable

Dhcp-Relay giaddr:

Dhcp-Relay ServerIp: 192.168.1.5

Dhcp-Relay Option82: Disable

Dhcp-Relay Option82 Action: Keep

Dhcp-Relay Option82 Circuit-ID:

Dhcp-Relay Option82 Remote-ID:

Ospf Config

Ospf Mtu Ignore : Disable

Ospf Cost : 10
Ospf Priority : 1
#Show DHCP relay client
SWITCH(config)# show ip dhcp relay client-information

```
-----------------------------------------------------------------------------------------------------------------------------
Index      Mac       Vlan  DevType   UserIp     ServerIp  Client-UNI  Server-UNI  LeaseTime  Timer
1  EC:22:80:EB:BA:36   2      192.168.1.100  192.168.1.5  eth1/0/2   eth1/0/1     1800       1560
-----------------------------------------------------------------------------------------------------------------------------
```

18 DHCP-сервер

18.1 Введение в DHCP-сервер

DHCP-сервер назначает IP-адреса при входе в систему рабочих станций и гарантирует, что каждой рабочей станции будет присвоен отдельный IP-адрес. DHCP-сервер значительно упрощает некоторые задачи управления сетью, которые раньше выполнялись вручную.

18.1.1 Настройка DHCP-сервера

Таблица 73 – Команды настройки DHCP-сервера

Команды	Описание	Режим
[no] ip dhcp server	Отключить/включить глобальный DHCP-сервер	“(config)#”
ip dhcp server (enable | disable)	Отключить/включить DHCP-сервер	“(Vlan-interface)#”
ip dhcp server enable <ip-pool>	Привязать пул адресов	“(Vlan-interface)#”
ip dhcp server ip-pool <pool-name>	Создать/войти пул IP-адресов	“(config)#”
no ip dhcp server ip-pool <pool-name>	Удалить пул IP-адресов	“(config)#”
network <network-address> <mask>	Настроить сегменты сети пула IP-адресов	“(ip-pool)#”
vendor-class-identifier (string| hex) <client-identifier> ip-range <min-address> <max-address>	Настроить выделение зарезервированных диапазонов адресов для указанных клиентов DHCP.	“(ip-pool)#”
no vendor-class-identifier (string| hex) <client-identifier>	Отменить назначение зарезервированного диапазона адресов для клиентов DHCP	“(ip-pool)#”
[no] static ip <ip-address> mac-address <mac-address>	Удалить/добавить статическую привязку IP-адрес MAC	“(ip-pool)#”

[no] excluded-ip <low-ip-address> <high-ip-address>	Удалить/добавить сегменты адресов, которые не участвуют в автоматическом распределении	“(ip-pool)#”
[no] lease (day <day> hour <hour> minute <minute> | unlimited)	Восстановить/настроить время аренды	“(ip-pool)#”
[no] domain-name <domain-name>	Отменить/настроить суффикс домена	“(ip-pool)#”
[no] dns <ip-address>	Отменить/настроить DNS	“(ip-pool)#”
[no] nbns <ip-address>	Отменить/настроить адрес WINS-сервера	“(ip-pool)#”
[no] netbios-type (b-node | h-node | m-node | p-mode | none)	Восстановить/настроить типы узлов NextBIOS, назначенные DHCP-клиенту.	“(ip-pool)#”
[no] gateway <ip-address>	Отменить/Настроить шлюз	“(ip-pool)#”
[no] tftp-server ip-address <ip-address>	Отменить/настроить адрес сервера TFTP, назначенный клиенту DHCP	“(ip-pool)#”
[no] tftp-server domain-name <domain-name>	Отменить/настроить имя сервера TFTP, назначенное клиенту DHCP.	“(ip-pool)#”
[no] bootfile-name <bootfile-name>	Отменить/настроить имя файла запуска, назначенное DHCP-клиенту.	“(ip-pool)#”
[no] next-server <ip-address>	Отменить/настроить пул адресов DHCP выделяя IP-адрес следующего сервера, предоставляющего услуги клиенту DHCP.	“(ip-pool)#”
[no] option <code> (string <option-string> | hex <option-string> | ip <ip-address>)	Удалить/настроить пользовательские параметры DHCP	“(ip-pool)#”
[no] ip dhcp server threshold (global | peer-pool) allocated-ip <threshold-value>	Отменить/настроить пороговые значения Trap DHCP-сервера	“(config)#”
clear ip dhcp server conflict (all | <ip-address> | pool <pool-name>)	Очистить информацию о конфликте пула адресов	“#”
clear ip dhcp serveer ip-in-use (all | <ip-address> | pool <pool-name>)	Очистить информацию о динамической привязке пула адресов	“#”
ip dhcp server database auto-write (enable | disable)	Отключить/включить функцию сохранения текущих данных DHCP в память.	“(config)#”
[no] ip dhcp server database auto-write file-name <file-name>	Восстановить/настроить имя файла загрузки пакета данных DHCP	“(config)#”
[no] ip dhcp server database auto-write interval <interval>	Восстановить/настроить интервал загрузки пакетов данных DHCP	“(config)#”
ip dhcp server database recover <file-name>	Восстановить данные аренды указанного файла	“(config)#”
ip dhcp server database save <file-name>	Сохранить данные аренды в указанный файл	“(config)#”

debugging dhcp server (none | pktinfo | options | all)	Настроить отладку DHCP-сервера	“(config)#”

18.1.2 Просмотр DHCP Server

Таблица 74 – Команды просмотра DHCP Server

Команды	Описание	Режим
show ip dhcp server ip-in-use (all | <ip-address> | pool <pool-name>)	Показать информацию о привязке адресов в пуле адресов	“#”
show ip dhcp server config (all | pool <pool-name>)	Показать информацию о конфигурации DHCP-сервера	“#”
show ip dhcp server conflict (all | <ip-address> | pool <pool-name>)	Показать статистику конфликтов адресов DHCP	“#”

18.2 Пример настройки

18.2.1 Критерии задач конфигурации

Таблица 75 - Критерий задач конфигурации

Критерий задач конфигурации	Описание
Включить глобальный DHCP-сервер	Необходимый
Запустить DHCP-сервер на виртуальном интерфейсе	Необходимый
Создать/войти пул IP-адресов	Необходимый
Настроить сегменты сети пула IP-адресов	Необходимый
Привязать пул адресов	Необходимый
Указать DHCP-клиенту выделение зарезервированного диапазона адресов	Необязательный
Добавить статическую запись привязки IP-адрес MAC	Необязательный
Добавить сегменты адресов, которые не участвуют в автоматическом распределении.	Необязательный
Настройка таймера	Необязательный
Назначить адресную информацию	Необязательный
Настроить адрес WINS-сервера	Необязательный
TFTP-сервер, назначенный DHCP-клиенту	Необязательный
Пользовательские параметры DHCP	Необязательный

18.2.2 Пример настройки

1. Требования к сети

— Клиент DHCP может получить IP-адрес, назначенный DHCP-сервером.

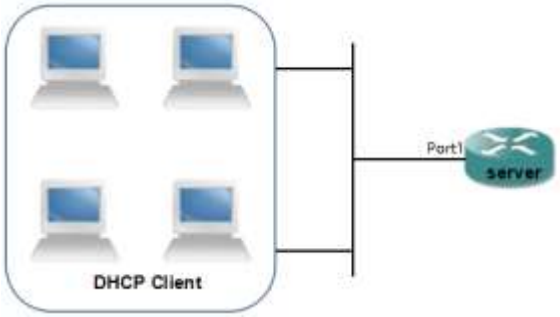

Рисунок 24 - Схема топологии сети

2. План настройки

— Включить DHCP-сервер и DHCP-сервер виртуального интерфейса.

— Создать пул адресов и настроить диапазон адресов.

— Привязать пул адресов

3. Шаги настройки

（1）Включить DHCP-сервер и DHCP-сервер виртуального интерфейса.

SWITCH# configure

SWITCH(config)# ip dhcp server

SWITCH(config)# interface vlan-interface 1

SWITCH(Vlan-interface1)# ip dhcp server enable

（2）Создать пул адресов и настроить диапазон адресов

SWITCH(config)# ip dhcp server ip-pool pool1

SWITCH(ip-pool-pool1)# network 192.168.1.0 255.255.255.0

（3）Привязать пул адресов

SWITCH(Vlan-interface1)# ip dhcp server enable pool1

4. Проверка конфигурации

SWITCH(config)# show ip dhcp server ip-in-use all

Global Ip-pool Resource: 253

Ip Used: 1

INDEXLEASE-IPLEASE-MAC VLAN TYPE GW-IPLEASE-TIMEAGE POOL-NAME

---

1 192.168.1.1 EC:22:80:EB:BA:36 1 leased N/A 1-0:0:00-23:58:57 pool1

19 STP (SPANNING TREE PROTOCOL)/ ПРОТОКОЛ КАНАЛЬНЫЙ

В этой главе представлено подробное описание команды CLI:

- Обзор связующего дерева (Spanning Tree Protocol);
- Процесс выбора корневого моста (Root bridge) в STP;
- Процесс выбора роли порта в STP;
- Примеры конфигурации STP.

19.1 Обзор Spanning Tree Protocol/

В коммутируемых сетях уровня 2 наличие петель может вызвать зацикливание пакетов, их распространение и широковещательные штормы, что приводит к использованию всей доступной полосы пропускания и делает сеть непригодной для использования.

В таких средах можно использовать Spanning Tree Protocol (STP). STP — это протокол управления уровня 2, который выборочно блокирует резервные сетевые каналы для устранения сетевых петель уровня 2, обеспечивая при этом функцию резервного копирования каналов. Как и другие протоколы, STP постоянно развивается по мере развития сетей. Первоначально широко использовался IEEE 802.1D-1998 STP (Spanning Tree Protocol), за ним последовали IEEE 802.1w RSTP (Rapid Spanning Tree Protocol), протокол PVST (Per VLAN Spanning Tree) и IEEE 802.1s MSTP (Multiple Spanning Tree Protocol), основанный на STP. Текущая система PVRP поддерживает STP и RSTP.

19.1.1 Введение в STP

STP имеет два определения: в узком смысле STP относится к протоколу STP, определенному в IEEE 802.1D-1998, тогда как в широком смысле STP относится к различным Spanning Tree протоколам, включая протокол STP, определенный в IEEE 802.1D-1998 и на его основе различные улучшенные Spanning Tree протоколы. В этой статье STP относится к STP в узком смысле. Основная идея STP довольно проста. Точно так же, как деревья в природе не имеют петель, если бы сети могли расти как деревья, петель бы не возникало. Таким образом, STP определяет такие понятия, как корневой мост (Root

Bridge), корневой порт (Root Port), назначенный порт (Designated Port) и стоимость пути (Path Cost), с целью сокращения избыточных петель путем построения дерева и одновременного резервного копирования канала и выбора оптимального пути. Алгоритм, используемый для построения этого дерева, называется Spanning Tree Algorithm.

Для достижения этих функций мосты должны обмениваться некоторой информацией, и единицы этого обмена информацией называются блоками данных протокола моста (BPDU-Bridge Protocol Data Units), также известными как сообщения конфигурации. В этой статье все протокольные сообщения Spanning Tree Protocol называются BPDU. STP BPDU — это сообщение уровня 2 с MAC-адресом назначения multicast address 01-80-C2-00-00-00. Все мосты, поддерживающие STP, будут получать и обрабатывать полученные сообщения BPDU. Область данных этого сообщения содержит всю полезную информацию для вычисления Spanning Tree.

19.1.2 Процесс работы STP

Процесс работы STP выглядит следующим образом:

1. Сначала выбирается корневой мост. Выбор основан на комбинации приоритете моста и MAC-адреса моста, образующей Bridge ID. Мост с наименьшим Bridge ID становится корневым мостом в сети. Все его порты подключаются к нисходящим мостам, поэтому все роли портов становятся назначенными портами (designated ports).

2. Затем каждый нисходящий мост, подключенный к корневому мосту, выбирает «самую надежную» ветвь в качестве пути к корневому мосту, и соответствующие порты становятся корневыми портами. Этот процесс повторяется до тех пор, пока не достигент границы сети, и как только назначенные порты и корневые порты будут определены, формируется Spanning Tree.

3. После периода стабильности (по умолчанию около 30 секунд) назначенные порты и корневые порты переходят в состояние пересылки (forwarding state), а другие порты переходят в состояние блокировки (blocking state). STP BPDU периодически отправляются из назначенных портов каждого моста для поддержания состояния линии.

Если топология сети изменится, связующее дерево будет пересчитано, и состояния портов соответственно изменятся. Это основной принцип Spanning Tree.

С развитием приложений и сетевых технологий выявились и недостатки STP. Главный недостаток STP заключается в скорости сходимости.

При изменении топологии возникает задержка перед распространением новых сообщений конфигурации по сети, известная как ForwardDelay, со значением по умолчанию 15 секунд. Если до того, как все мосты получат сообщение об изменении, порты, которые осуществляли пересылку в старой топологии, не осознают, что им следует прекратить пересылку в новой топологии, могут возникнуть временные петли. Для решения проблем с временными петлями STP использует стратегию таймера, вводя промежуточное состояние между состояниями блокировки и пересылки, при котором порт только изучает MAC-адреса, но не участвует в пересылке. Длительность обоих переходов между состояниями равна ForwardDelay, что гарантирует отсутствие временных петель во время изменений топологии. Однако это, казалось бы, хорошее решение на самом деле удваивает время сходимости, что неприемлемо для некоторых сервисов реального времени (таких как голос и видео).

19.1.3 Введение в RSTP

Чтобы решить проблему недостатка скорости сходимости STP, в 2001 году IEEE определил Rapid Spanning Tree Protocol (RSTP) на основе стандарта IEEE 802.1w (который был включен в IEEE 802.1D-2004). RSTP имеет три существенных улучшения по сравнению с STP, ускоряя скорость сходимости (которая может достигать 1 секунды):

1. RSTP вводит две дополнительные роли порта для быстрого переключения: альтернативный порт (Alternate Port) и резервный порт (Backup Port). При выходе из строя корневого порта альтернативный порт быстро превращается в новый корневой порт и без задержки переходит в состояние пересылки. Аналогично, в случае сбоя назначенного порта резервный порт быстро становится новым назначенным портом и переходит в состояние пересылки.

2. В канале point-to-point, соединяющем только два порта коммутатора, назначенный порт может перейти в состояние пересылки без задержки после одного подтверждения связи (handshake) с нисходящим мостом. Однако в общем канале, соединяющем три или более мостов, нисходящие мосты не отвечают на запросы handshake от вышестоящих назначенных портов и должны ждать в два раза больше Forward Delay, чтобы войти в состояние пересылки.

3. Порты, напрямую подключенные к конечным устройствам, а не к другим мостам, определяются как пограничные порты (Edge Ports). Пограничные порты могут напрямую переходить в состояние пересылки без каких-либо задержек. Поскольку мосты не могут автоматически определить, подключен ли порт напрямую к конечному устройству, требуется настройка вручную.

Эти улучшения значительно повышают скорость сходимости протокола Spanning Tree, делая RSTP более подходящим для современных сетевых сред.

Хотя RSTP предлагает множество улучшений по сравнению с STP и обратно совместим, что позволяет использовать смешанные сети, и RSTP, и STP относятся к категории Single Spanning Tree (SST), каждый из которых имеет свой собственный набор недостатков. Эти недостатки в основном проявляются в трех аспектах:

1. Из-за наличия только одного связующего дерева во всей коммутационной сети время сходимости может увеличиваться, особенно в сетях большего масштаба.

2. Поскольку RSTP — это Single Spanning Tree Protocol, все VLAN используют Single Spanning Tree. Чтобы обеспечить связь внутри VLAN, каждый VLAN должна быть непрерывно распределен по пути Spanning Tree. В противном случае сети VLAN могут стать сегментированными из-за блокировки внутренних каналов, что приведет к проблемам со связью внутри сетей VLAN.

3. Когда канал заблокирован, он не может передавать трафик, что приводит к значительной потере пропускной способности и невозможности балансировки нагрузки. Эти недостатки присущи протоколам Single Spanning Tree и не могут быть преодолены. Следовательно, для решения этих проблем появились протоколы с поддержкой VLAN, такие как PVST и MSTP. PVST и

MSTP будут представлены в последующих разделах после того, как поддержка PVRP будет описана в этом документе.

19.2 Роли портов в Spanning Tree

Топология Spanning Tree в сети определяется несколькими факторами мостов:

- ID каждого моста (приоритет и MAC-адрес).
- Стоимость пути для каждого порта моста.
- ID каждого порта моста.

В локальной сети MAC-адреса мостов уникальны, что гарантирует, что каждый мост имеет уникальный идентификатор. Мост с наименьшим идентификатором становится корневым мостом в локальной сети. После определения корневого моста bridge ID, path cost, and port ID используются для определения того, какие порты могут стать корневыми портами, какие порты могут стать назначенными портами и какие порты должны быть заблокированы. Корневой мост имеет назначенные порты, но не имеет корневого порта. Назначенный мост должен иметь ровно один корневой порт и хотя бы один назначенный порт.

1. Процесс выбора корневого моста:

Если после инициализации моста не получено ни одного моста с меньшим идентификатором или информацией о конфигурации более высокого приоритета моста, мост продолжит считать себя корневым мостом. Он периодически отправляет configuration BPDU на порты, которые, по его мнению, являются назначенными, пока не получит информацию о мосте с меньшим идентификатором или мосте с лучшим приоритетом, указывающую, что это не корневой мост. Затем он выбирает лучший мост в качестве корневого моста. Изменения состояния порта из-за управления конфигурацией (например, включение порта, отключение порта, установка приоритета моста и т. д.) также могут вызвать перевыборы корневого моста. Если мост настроен с защитой BPDU, он не будет принимать сообщения о лучшей конфигурации моста и продолжит считать себя корневым мостом.

2. Процесс выбора корневого порта:

Когда мост получает информацию configuration BPDU, указывающую более высокий приоритет, чем его собственный, он не может стать корневым мостом. Ему необходимо обновить информацию о корневом мосте и, помимо информации о назначенном мосте, повторно выбрать корневой порт. Стратегия выбора, следующая: порт моста с минимальной общей стоимостью пути до корневого моста, которая представляет собой сумму назначенной стоимости пути и стоимости самого порта, выбирается в качестве корневого порта. Если есть два или более порта, обеспечивающих одинаковую стоимость пути к корневому мосту, в качестве корневого порта выбирается порт с наивысшим приоритетом. Если есть два или более порта, обеспечивающих одинаковую стоимость пути к корневому мосту и содержащих одинаковые назначенные параметры моста, порт с с наивысшим priority designated port выбирается в качестве корневого порта. Наконец, если есть два или более порта с одинаковой стоимостью пути к корневому мосту, одним и тем же назначенным мостом и одинаковыми параметрами назначенного порта, порт с самым высоким port ID выбирается в качестве корневого порта (т. е. порт с lowest port ID). Каждый идентификатор порта одного и того же моста уникален и часто используется для определения корневых портов, назначенных портов и заблокированных портов. Краткое описание правил: Порядок сравнения приоритетов, следующий: path cost, designated bridge ID, designated port, port ID.

3. Процесс выбора назначенных портов:

Определение того, какой порт моста может стать назначенным портом для LAN. LAN обменивается данными с внешним миром через этот назначенный порт. Правила выбора: после выбора корневого порта среди портов, подключенных к LAN, в качестве назначенного порта выбирается порт с минимальной стоимостью пути до корневого моста. Если в LAN имеется несколько портов моста с минимальной стоимостью пути к корневому коммутатору, то порт с наименьшим идентификатором моста на локальном мосту выбирается в качестве назначенного порта для этой LAN. Если несколько портов на одном мосту имеют кратчайший путь к корневому мосту, то порт с наименьшим идентификатором порта выбирается в качестве назначенного порта для LAN.

4. Выбор заблокированных портов:

Предполагая, что порт включен и участвует в расчете активной топологии, если он не является корневым портом или назначенным портом, он становится заблокированным портом.

19.3 Конфигурация Spanning Tree

19.3.1 Общая настройка Spanning Tree

Таблица 76 – Команды для общей настройки Spanning Tree

Команды	Описание	Режим
spanning-tree (enable | disable)	Отключить/включить Spanning Tree	“(config)#”
spanning-tree mode (stp | rstp | mstp)	Настроить рабочий режим Spanning Tree	“(config)#”
spanning-tree transparent (enable | disable)	Настроить функции прозрачности сообщений BPDU	“(config)#”
spanning-tree path-cost method (dot1d-1998 | dot1t)	Метод стоимости пути конфигурации	“(config)#”
spanning-tree forward-delay <time>	Настроить время задержки пересылки	“(config)#”
spanning-tree max-age <time>	Настроить время устаревания	“(config)#”
spanning-tree hello-time <time>	Настроить интервал времени приветствия	“(config)#”
spanning-tree priority <priority>	Установить значение приоритета моста	“(config)#”
spanning-tree (enable | disable)	Отключить/включить Port Spanning Tree	“(config-eth)”

19.3.2 Конфигурация STP/RSTP

Таблица 77 – Команды конфигурации STP/RSTP

Команды	Описание	Режим
spanning-tree edged-port (enable | disable)	Настроить пограничные порты	“(config-eth)”
spanning-tree bpdu-guard (enable | disable)	Настроить защиту BPDU	“(config-eth)”
spanning-tree bpdu-filter (enable | disable)	Настроить функции фильтрации BPDU	“(config-eth)”
spanning-tree pathcost <cost>	Настройка стоимости пути	“(config-eth)”
spanning-tree priority <priority>	Настроить приоритет портов	“(config-eth)”
spanning-tree link-type (auto | share | point-to-point)	Настроить статус управления типом ссылки	“(config-eth)”

19.3.3 Конфигурация MSTP

Таблица 78 – Команды конфигурации MSTP

Команды	Описание	Режим
spanning-tree mst configuration	Войти в обзор конфигурации mst	“(config)#”
name WORD	Настроить имена регионов Multi Spanning Tree Protocol	mst configuration view
revision <version>	Настроить multiple spanning tree версию редакции региона	mst configuration view
instance <id> vlan VLANLIST	Настроить сопоставление VLAN с экземплярами MSTP	mst configuration view
check configuration	Проверить конфигурации домена MST, которые еще не вступили в силу	mst configuration view
spanning-tree mst max-hops <hop>	Настроить максимальное количество прыжков в домене MST	“(config)#”
spanning-tree mst instance <id> priority <priority>	Настроить значение приоритета моста для указанного экземпляра spanning tree	“(config)#”

19.3.4 Просмотр Spanning Tree

Таблица 79 – Команды для просмотра Spanning Tree

Команды	Описание	Режим
show spanning-tree mst instance <id>	Показать информацию об экземпляре MSTP	“#”
show spanning-tree mst configuration	Показать конфигурацию MST	“#”
show spanning-tree status	Показать конфигурацию STP	“#”
show spanning-tree interface <interface-type> <interface-number>	Показать информацию об интерфейсе STP	“#”
show spanning-tree statistics interface <interface-type> <interface-number>	Показать информацию о статистике сообщений STP	“#”

19.4 Пример настройки Spanning Tree

19.4.1 Критерии задач конфигурации

Таблица 80 - Критерий задач конфигурации

Критерий задач конфигурации	Описание
Включить Spanning Tree	Необходимый
Настроить режим работы Spanning Tree	Необходимый
Включить Port Spanning Tree	Необходимый
Метод стоимости пути конфигурации	Необязательный
Значение приоритета моста	Необязательный
Таймер	Необязательный
Настроить пограничне порты	Необязательный
Настроить защиту BPDU	Необязательный
Настроить стоимость пути	Необязательный
Настроить приоритет портов	Необязательный
Настроить статус управления типом ссылки	Необязательный
Настроить домен MST	Необязательный

19.4.2 Пример настройки

1. Требования к сети

— Выполняйте сборку в соответствии со схемой топологии многоадресной рассылки и предотвращайте образование петель, включив STP.

— Router1, Router2, Router3 и Router4 имеют доступ друг к другу.

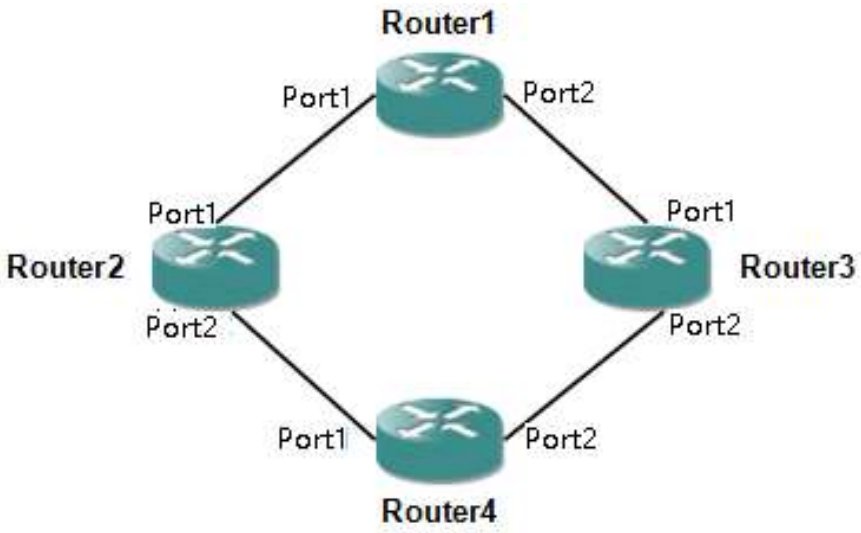

Рисунок 25 - Схема топологии сети

2. План настройки

— Настроить виртуальные IP-интерфейсы для каждого сетевого моста.

— Настроить порты с поддержкой STP, участвующие в топологии.

3. Шаги настройки

（1）Настроить виртуальные IP-интерфейсы для каждого моста

```
# Настройка Router1
Router1# configure
Router1(config)# interface vlan-interface 1
Router1(Vlan-interface1)# ip address 192.168.1.1 255.255.255.0
# Настройка Router2
Router2# configure
Router2(config)# interface vlan-interface 1
Router2(Vlan-interface1)# ip address 192.168.1.2 255.255.255.0
# Настройка Router3
Router3# configure
Router3(config)# interface vlan-interface 1
Router3(Vlan-interface1)# ip address 192.168.1.3 255.255.255.0
# Натсройка Router4
Router4# configure
Router4(config)# interface vlan-interface 1
Router4(Vlan-interface1)# ip address 192.168.1.4 255.255.255.0
```

（2）Включить STP для портов, участвующих в топологии

```
# Настройка Router1
Router1(config)# interface ethernet 1/0/1
Router1(config-eth1/0/1)# spanning-tree enable
Router1(config-eth1/0/1)# interface ethernet 1/0/2
Router1(config-eth1/0/2)# spanning-tree enable
# Настройка Router2
Router2(config)# interface ethernet 1/0/1
Router2(config-eth1/0/1)# spanning-tree enable
Router2(config-eth1/0/1)# interface ethernet 1/0/2
Router2(config-eth1/0/2)# spanning-tree enable
# Настройка Router3
Router3(config)# interface ethernet 1/0/1
```

Router3(config-eth1/0/1)# spanning-tree enable
Router3(config-eth1/0/1)# interface ethernet 1/0/2
Router3(config-eth1/0/2)# spanning-tree enable
Настройка Router4
Router4(config)# interface ethernet 1/0/1
Router4(config-eth1/0/1)# spanning-tree enable
Router4(config-eth1/0/1)# interface ethernet 1/0/2
Router4(config-eth1/0/2)# spanning-tree enable

4. Проверка конфигурации
Просмотр глобальной конфигурации STP для Router1:
SWITCH(config)# show spanning-tree status
Global Settings
Spanning tree status : enable
STP Operation Mode : mstp
BPDU transparent : disable
Path Cost Method : dot1t
Bridge Settings
Priority : 32768
Hello-Time : 2 sec
Max-Age : 20 sec
Forward-delay : 15 sec
Status
Root Bridge : 32768 / 18:c3:f4:00:00:00
External Root Path Cost : 0
Regional Root Bridge : 32768 / 18:c3:f4:00:00:00
Internal Root Path Cost : 0
Designated Bridge : 32768 / 18:c3:f4:00:00:00
Root Port : 0.0
Topology changes : 0
Last Topology Change : 4

Просмотр конфигурации порта STP для Router1:
SWITCH(config)# show spanning-tree interface ethernet 1/0/1
[Ethernet1(eth1/0/1)][Disabled]
Port Protocol: Enabled(MSTP)

Port.ID: 1.128
Port Edged: Config=Disabled / Active=disabled
Port Type(PointToPoint): Config=Auto / Active=PointToPoint
Port Guard: Disabled
Port Filter: Disabled
Rapid transition: Enabled

20 ERPS (ETHERNET RING PROTECTION SWITCHING)/ КОММУТАЦИЯ КОЛЬЦЕВОЙ ЗАЩИТЫ ETHERNET

В этой главе представлено подробное описание:
- Введение в ERPS;
- Технические характеристики;
- Команды конфигурации ERPS;
- Пример настройки ERPS.

20.1 Обзор ERPS

ERPS (Ethernet Ring Protection Switching), также известный как G.8032, представляет собой протокол защиты от колец, разработанный ITU для колец Ethernet. Это протокол канального уровня, специально разработанный для кольцевых сетей Ethernet. Он предотвращает широковещательные штормы, вызванные петлями данных в кольцевых сетях Ethernet, когда сеть не повреждена, и быстро восстанавливает связь между узлами в кольце при возникновении сбоя канала. Протокол ERPS обеспечивает быстрый механизм защиты кольцевых сетей Ethernet, обеспечивая быстрое восстановление сети в случае сбоев, гарантируя тем самым высокую доступность и надежность коммутаторов в кольцевых топологиях сетей.

20.2 Введение в ERPS

20.2.1 Кольцо ERPS

Кольцо ERPS следует принципу минимизации кольца, где каждое кольцо должно быть минимальным и состоять из главного кольца и подколец: главное кольцо представляет собой замкнутый контур, а подкольцо может быть либо разомкнутым, либо замкнутым, и оба должны быть настроены с помощью команд.

Каждое кольцо ERPS (главное или подчиненное) имеет пять состояний: (1) Состояние простоя (Idle state): состояние, когда все физические каналы в кольце подключены; (2) Состояние защиты (Protection state): состояние, когда одно или несколько физических каналов в кольце отключены; (3) Состояние ручного переключения (Manual switch state): состояние, когда статус кольца изменяется вручную; (4) Состояние принудительного переключения (Forced switch state): состояние, когда статус кольца принудительно изменяется; (5) Состояние ожидания (Pending state): промежуточное состояние, ожидающее разрешения.

16.2.2 Узел ERPS

Устройства, присоединяющиеся к кольцу ERPS при коммутации уровня 2, называются узлами. Каждый узел не может иметь более двух портов, присоединяющихся к одному кольцу ERPS, причем один порт является портом RPL (Ring Port for Link), а другой порт является обычным кольцевым портом.

В глобальном контексте узлы делятся на два типа: (1) Пересекающиеся узлы (Intersecting nodes): в пересекающихся кольцах ERPS узлы, принадлежащие нескольким кольцам одновременно, называются пересекающимися узлами. (2) Непересекающиеся узлы (Non-intersecting nodes): в пересекающихся кольцах ERPS узлы, принадлежащие только одному кольцу ERPS, называются непересекающимися узлами.

Режимы узла, определенные в протоколе ERPS, в основном включают три типа:

RPL Owner Node: кольцо ERPS имеет только один узел владельца RPL, который определяется конфигурацией пользователя. Он блокирует порт RPL, чтобы предотвратить образование петель в кольце ERPS. Когда узел-владелец RPL получает сообщения о сбоях, указывающие на неисправности в других узлах или каналах кольца ERPS, он автоматически разблокирует порт RPL, позволяя порту возобновить прием и отправку трафика, обеспечивая бесперебойный поток.

RPL Neighbour Node: узлы, напрямую подключенные к порту RPL узла-владельца RPL. Обычно и порт RPL узла-владельца RPL, и порт RPL соседнего узла RPL блокируются во избежание образования петель. При возникновении

неисправности в кольце ERPS разблокируются, как порт RPL узла-владельца RPL, так и порт RPL соседнего узла RPL.

Regular Ring Node: в кольце ERPS узлы, отличные от узла-владельца RPL и соседнего узла RPL, являются обычными кольцевыми узлами. Порт RPL и обычный кольцевой порт обычных кольцевых узлов неотличимы. Обычный кольцевой порт обычных кольцевых узлов отвечает за мониторинг состояния канала протокола ERPS, к которому он напрямую подключен, и оперативное уведомление других узлов о любых изменениях состояния канала.

20.2.2 Links and Channels/Ссылки и каналы

1. RPL (Ring Protection Link): каждое кольцо ERPS имеет один и только один RPL, который является каналом, по которому расположен порт RPL узла-владельца RPL. Когда кольцо Ethernet находится в состоянии простоя, канал RPL находится в заблокированном состоянии и не пересылает пакеты данных во избежание образования петли.

2. Sub-Ring Links: внутри пересекающихся колец — ссылки, принадлежащие подкольцам, контролируемым подкольцом.

3. RAPS (Ring Auto Protection Switch) Virtual Channel: в пересекающихся кольцах каналы, используемые для передачи протокольных сообщений подкольца между пересекающимися узлами, называются виртуальным каналом RAPS подкольца.

20.2.3 ERPS VLAN/Протокол VLAN

RAPS VLAN (также известный как протокол VLAN): используется для передачи сообщений протокола ERPS. Порты, имеющие доступ к кольцу ERPS на устройствах, принадлежат RAPS VLAN. RAPS VLAN для разных колец должны быть разными. IP-адреса нельзя настраивать на интерфейсах RAPS VLAN.

20.2.4 Принцип работы ERPS

Нормальное состояние

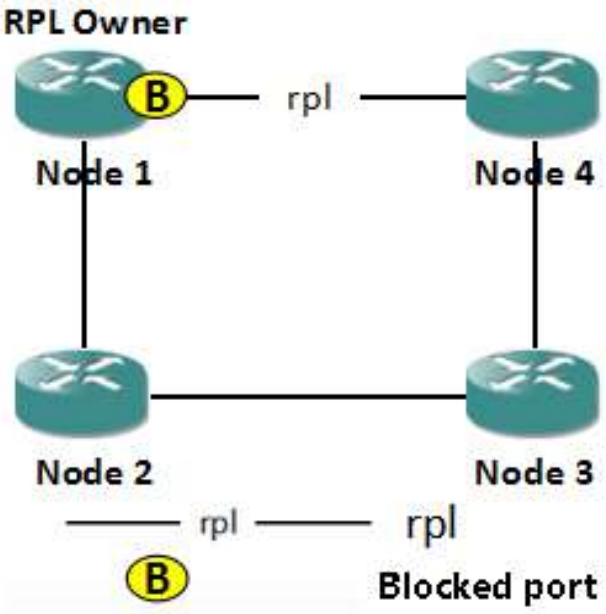

Рисунок 26 - Нормальное состояние

1. Все узлы физически соединены в кольцевую топологию.

2. Протокол защиты кольца гарантирует отсутствие петель путем блокировки канала RPL. На диаграмме выше связь между Node1 и Node4 — это link RPL.

3. Обнаружение неисправности выполняется на каждом канале между соседними узлами.

Отказ канала

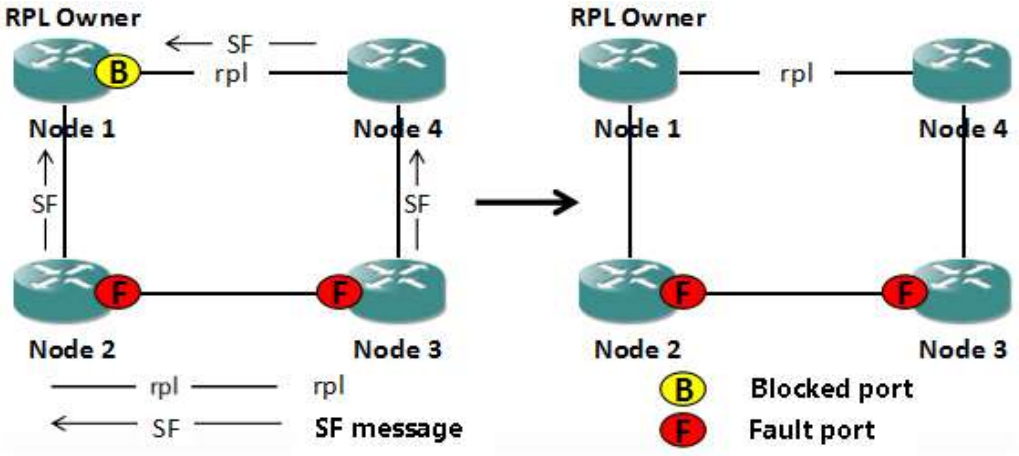

Рисунок 27 - Отказ канала

1. Узлы, соседние с отказавшим каналом, блокируют канал и используют сообщения RAPS (SF), чтобы сообщить о сбое другим узлам в кольце. Например, предполагая сбой канала между Node2 и Node3, Node2 и Node3 будут ждать истечения таймера задержки, затем блокируют неисправный канал и отправляют сообщения RAPS (SF) всем узлам в кольце.

2. Сообщения RAPS (SF) заставляют узел владельца RPL открыть порт RPL. Сообщения RAPS (SF) также побуждают все узлы обновить свои записи таблицы MAC, а затем узлы переходят в состояние защиты.

Восстановление канала

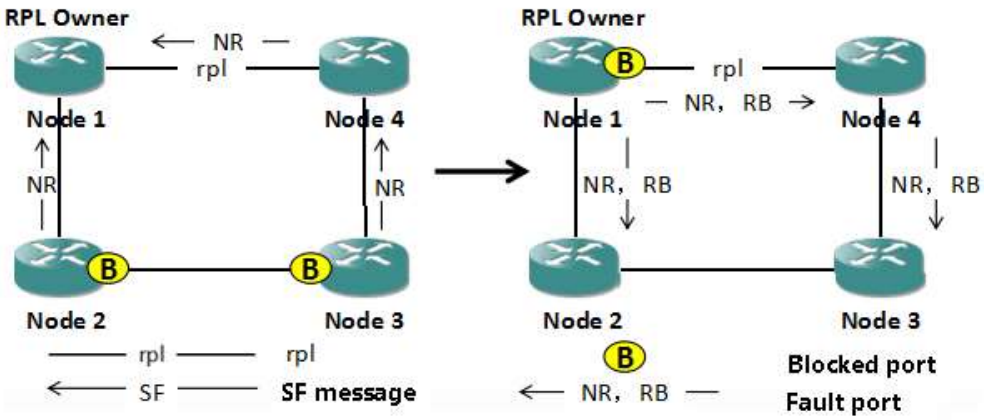

Рисунок 28 – Восстановление канала

1. Когда неисправность устранена, соседние с неисправностью узлы продолжают оставаться в заблокированном состоянии и отправлять сообщения RAPS (NR), указывая на отсутствие локальной неисправности.

2. По истечении времени защитного таймера при получении первого сообщения RAPS (NR) узел владельца RPL запускает таймер WTR.

3. По истечении времени таймера WTR узел владельца RPL блокирует RPL и отправляет сообщения RAPS (NR, RB).

4. Получив это сообщение, другие узлы обновляют свои записи таблицы MAC. Узел, отправляющий сообщение RAPS (NR), прекращает отправку периодических сообщений и открывает ранее заблокированный порт. Кольцевая сеть восстанавливается в исходное нормальное состояние.

20.3 Поддержка Multi-Ring Intersection and Cutting

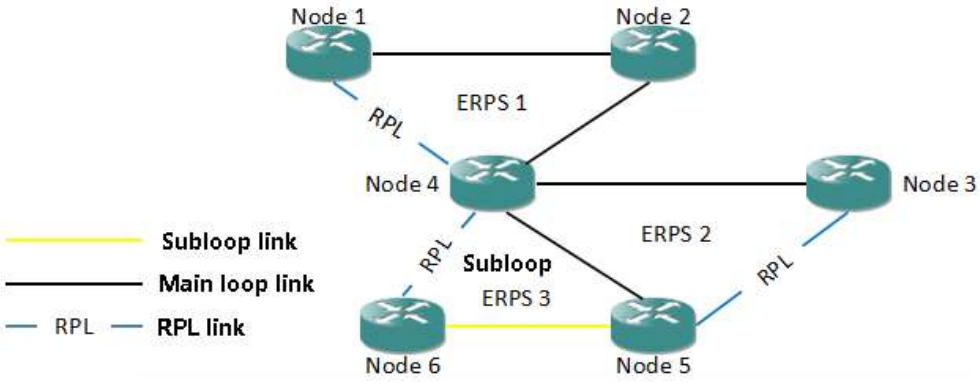

Рисунок 29 – Поддержка Multi-Ring Intersection and Cutting

Как показано на рисунке выше, ERPS поддерживает добавление нескольких колец в один и тот же узел (Node4) в форме касания или пересечения, что значительно повышает гибкость сети.

20.4 Конфигурация ERPS (Ethernet Ring Protection Switching)/ Коммутация кольцевой защиты Ethernet

20.4.1 Общая настройка ERPS

Таблица 81 – Команды общей настройки ERPS

Команды	Описание	Режим
[no] erps	Отключить/Включить ERPS	“(config)#”
[no] erps ring <ring-id>	Удалить/создать идентификатор кольца	“(config)#”
erps ring <ring-id> ring-mode sub major-ring <ring-id>	Настроить указанное кольцо как подкольцо и указать домашнее главное кольцо	“(config)#”
no erps ring <ring-id> ring-mode	Настроить дополнительные кольца в качестве основных колец	“(config)#”
erps ring <ring-id> node-mode (owner | neighbor)	Настроить роли узла как основной/соседний	“(config)#”
no erps ring <ring-id> node-mode	Настроить роль узла как обычный узел	“(config)#”
[no] erps ring <ring-id> non-revertive	Настроить резервный/нерезервный режим кольца ERPS	“(config)#”
[no] erps ring <1-239> [rpl-port] interface <interface-type> <interface-number>	Отменить/настроить кольцевой порт RPL	“(config)#”

[no] erps ring <1-239> virtual channel	Конфигурация невиртуального канала/виртуального канала	“(config)#”
[no] erps ring <1-239> ctrl-vlan <1-4094>	Протокол VLAN для отмены/настройки кольца	“(config)#”
erps ring <ring-id> fs interface <interface-type> <interface-number>	Настроить принудительноге переключение портов	“(config)#”
erps ring <ring-id> manual switch interface <interface-type> <interface-number>	Настроить ручное переключение портов	“(config)#”
erps ring <ring-id> clear	Очистить статус переключения	“(config)#”
[no] erps ring <ring-id> hold-off-time <time>	Восстановить/настроить время задержки	“(config)#”
[no] erps ring <ring-id> guard-time <time>	Восстановить/настроить время охраны	“(config)#”
[no] erps ring <ring-id> wtr-time <time>	Восстановить/настроить время wtr	“(config)#”
[no] debugging erps (pkt | ipc | timer | fsm | all)	Настроить отладку	“(config)#”

20.4.2 Показать ERPS

Таблица 82 – Команды для просмотра ERPS

Команды	Описание	Режим
show erps	Показать статус всех колец ERPS	“#”
show erps ring <1-239>	Показать статус кольца, указанный в ERPS	“#”

20.5 Пример настройки ERPS

20.5.1 Критерии задач конфигурации

Таблица 83 - Критерий задач конфигурации

Критерий задач конфигурации	Описание
Включить ERPS	Необходимый
Создать идентификатор кольца	Необходимый
Настроить роль узла	Необходимый
Настроить кольцевой порт RPL	Необходимый
Настроить протокол VLAN для кольца	Необходимый
Настроить резервный режим кольца ERPS	Необязательный
Конфигурация виртуального канала	Необязательный
Настроить функции переключения конфигурации	Необязательный
Таймер	Необязательный

20.5.2 Пример настройки

1. Требования к сети

— Node1, Node2 и Node3 принадлежат основному кольцу 1. Node1 — владелец, Node2 — сосед, а Node3 — обычный узел.

— Протокол VLAN основного кольца 1 равен 10.

— Node2, Node3 и Node4 принадлежат подкольцу 1. Node4 является владельцем, Node2 — соседом, а Node3 — обычным узлом.

— Протокол vlan подкольца 2 — 9.

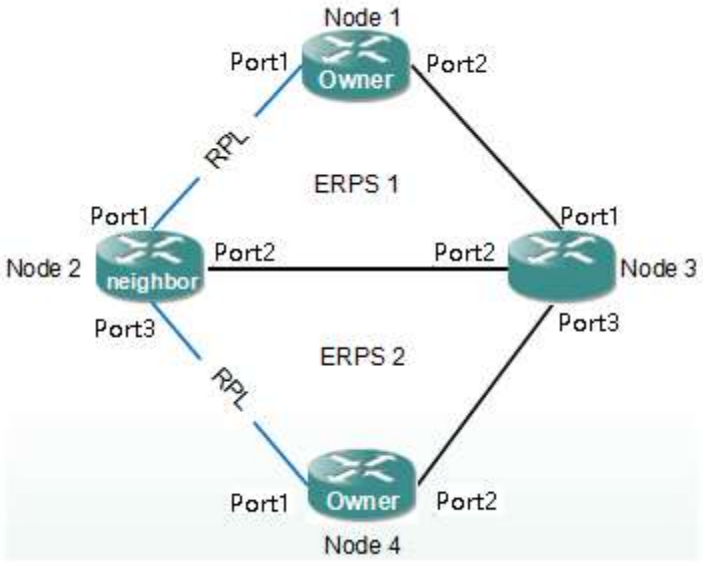

Рисунок 30 - **Схема топологии сети**

2. План настройки

— Создать VLAN 1–10 для Node1, Node2 и Node3, используя Trunk для Port 1 и 2, и разрешить все VLAN. Node4 создать VLAN 1–9, а Port 1–2 являются магистральными, что позволяет использовать все VLAN.

— Настроить узлы в соответствии с основной схемой топологии сети.

— Настроить узлы в соответствии со схемой топологии сети подкольца.

3. Шаги настройки

（1）Настройка параметров VLAN для каждого узла

Настройка Node1

Node1# configure

Node1(config)# vlan 1-10

```
Node1(config)#interface ethernet 1/0/1
Node1(config-eth1/0/1)# switchport mode trunk
Node1(config-eth1/0/1)# switchport trunk permit 1-10
Node1(config-eth1/0/1)# spanning-tree disable
Node1(config-eth1/0/1)# interface ethernet 1/0/2
Node1(config-eth1/0/2)# switchport mode trunk
Node1(config-eth1/0/2)# switchport trunk permit 1-10
Node1(config-eth1/0/2)# spanning-tree disable
# Настройка Node2
Node1# configure
Node1(config)# vlan 1-10
Node1(config)#interface ethernet 1/0/1
Node1(config-eth1/0/1)# switchport mode trunk
Node1(config-eth1/0/1)# switchport trunk permit 1-10
Node1(config-eth1/0/1)# spanning-tree disable
Node1(config-eth1/0/1)# interface ethernet 1/0/2
Node1(config-eth1/0/2)# switchport mode trunk
Node1(config-eth1/0/2)# switchport trunk permit 1-10
Node1(config-eth1/0/2)# spanning-tree disable
Node1(config-eth1/0/2)# interface ethernet 1/0/3
Node1(config-eth1/0/3)# switchport mode trunk
Node1(config-eth1/0/3)# switchport trunk permit 1-10
Node1(config-eth1/0/3)# spanning-tree disable
# Настройка Node3
Node3# configure
Node3(config)# vlan 1-10
Node3(config)#interface ethernet 1/0/1
Node3(config-eth1/0/1)# switchport mode trunk
Node3(config-eth1/0/1)# switchport trunk permit 1-10
Node3(config-eth1/0/1)# spanning-tree disable
Node3(config-eth1/0/1)# interface ethernet 1/0/2
Node3(config-eth1/0/2)# switchport mode trunk
Node3(config-eth1/0/2)# switchport trunk permit 1-10
Node3(config-eth1/0/2)# spanning-tree disable
Node3(config-eth1/0/2)# interface ethernet 1/0/3
Node3(config-eth1/0/3)# switchport mode trunk
```

Node3(config-eth1/0/3)# switchport trunk permit 1-10
Node3(config-eth1/0/3)# spanning-tree disable
Настройка Node4
Node4# configure
Node4(config)# vlan 1-10
Node4(config)#interface ethernet 1/0/1
Node4(config-eth1/0/1)# switchport mode trunk
Node4(config-eth1/0/1)# switchport trunk permit 1-10
Node4(config-eth1/0/1)# spanning-tree disable
Node4(config-eth1/0/1)# interface ethernet 1/0/2
Node4(config-eth1/0/2)# switchport mode trunk
Node4(config-eth1/0/2)# switchport trunk permit 1-10
Node4(config-eth1/0/2)# spanning-tree disable

（2）Настройка параметров ERPS для каждого узла в главном кольце.
Настройка Node1
Node1# configure
Node1(config)# erps
Node1(config)# erps ring 1
Node1(config)# erps ring 1 ctrl-vlan 10
Node1(config)# erps ring 1 node-mode owner
Node1(config)# erps ring 1 rpl-port interface ethernet 1/0/1
Node1(config)# erps ring 1 interface ethernet 1/0/2
Настройка Node2
Node2# configure
Node2(config)# erps
Node2(config)# erps ring 1
Node2(config)# erps ring 1 ctrl-vlan 10
Node2(config)# erps ring 1 node-mode neighbor
Node2(config)# erps ring 1 rpl-port interface ethernet 1/0/1
Node2(config)# erps ring 1 interface ethernet 1/0/2
Node2(config)# erps ring 1 virtual-channel
Настройка Node3
Node3# configure
Node3(config)# erps
Node3(config)# erps ring 1

Node3(config)# erps ring 1 ctrl-vlan 10
Node3(config)# erps ring 1 interface ethernet 1/0/1
Node3(config)# erps ring 1 interface ethernet 1/0/2
Node3(config)# erps ring 1 virtual-channel

Настройка параметров ERPS для каждого узла в подкольце
Настройка Node2
Node2(config)# erps ring 2
Node2(config)# erps ring 2 ctrl-vlan 9
Node2(config)# erps ring 2 node-mode neighbor
Node2(config)# erps ring 2 ring-mode sub major-ring 1
Node2(config)# erps ring 2 rpl-port interface ethernet 1/0/3
Node2(config)# erps ring 2 interface ethernet 1/0/2
Node2(config)# erps ring 2 virtual-channel
Настройка Node3
Node3(config)# erps ring 2
Node3(config)# erps ring 2 ctrl-vlan 9
Node3(config)# erps ring 2 ring-mode sub major-ring 1
Node3(config)# erps ring 2 interface ethernet 1/0/3
Node3(config)# erps ring 2 interface ethernet 1/0/2
Node3(config)# erps ring 2 virtual-channel
Настройка Node4
Node4# configure
Node4(config)# erps
Node4(config)# erps ring 2
Node4(config)# erps ring 2 ctrl-vlan 9
Node4(config)# erps ring 2 node-mode owner
Node4(config)# erps ring 2 rpl-port interface ethernet 1/0/1
Node4(config)# erps ring 2 interface ethernet 1/0/2

4. Проверка конфигурации

Просмотрите каждый узел, статус ERP — все в режиме idle, порт RPL — в блокировке, другие порты — в режиме пересылки, конфигурация успешна и эффективна.

Проверка конфигурации на Node 1
Node1(config)# show erps ring 1

Ring ID: 1
Control Vlan: 10
Protected Instance: 0
WTR Timer(min): 5
Guard Timer(ms): 500
Holdoff Timer(ms): 0
WTB Timer(ms): 5000
Ring State: idle
Revertive Mode: True
Node Mode: owner
R-APS Virtual Channel Mode: False
Sub-ring: False

PortPort RolePort StatusSignal StatusForced SwitchManual Switch
---
eth1/0/17RPL PortDiscardingNon-failedFalseFalse
eth1/0/18NormalForwardingNon-failedFalseFalse

Проверка конфигурации на Node 2
Node2(config)# show erps ring 1
Ring ID: 1
Control Vlan: 10
Protected Instance: 0
WTR Timer(min): 5
Guard Timer(ms): 500
Holdoff Timer(ms): 0
WTB Timer(ms): 5000
Ring State: idle
Revertive Mode: True
Node Mode: neighbour
R-APS Virtual Channel Mode: True
Sub-ring: False

PortPort RolePort StatusSignal StatusForced SwitchManual Switch
---
eth1/0/1RPL PortDiscardingNon-failedFalseFalse

eth1/0/2NormalForwardingNon-failedFalseFalse
Node2(config)# show erps ring 2
Ring ID: 2
Control Vlan: 1
Protected Instance: 0
WTR Timer(min): 5
Guard Timer(ms): 500
Holdoff Timer(ms): 0
WTB Timer(ms): 5000
Ring State: idle
Revertive Mode: True
Node Mode: neighbour
R-APS Virtual Channel Mode: True
Sub-ring: True
Major-ring ID: 1

PortPort RolePort StatusSignal StatusForced SwitchManual Switch
---
eth1/0/3RPL PortDiscardingNon-failedFalseFalse
eth1/0/2NormalForwardingNon-failedFalseFalse

Проверка конфигурации на Node 3
Node3(config)# show erps ring 1
Ring ID: 1
Control Vlan: 10
Protected Instance: 0
WTR Timer(min): 5
Guard Timer(ms): 500
Holdoff Timer(ms): 0
WTB Timer(ms): 5000
Ring State: idle
Revertive Mode: True
Node Mode: normal
R-APS Virtual Channel Mode: True
Sub-ring: False

```
 PortPort RolePort StatusSignal StatusForced SwitchManual Switch
--------------------------------------------------------------------------------
 eth1/0/2NormalForwardingNon-failedFalseFalse
 eth1/0/1NormalForwardingNon-failedFalseFalse
Node3(config)# show erps ring 2
Ring ID: 2
Control Vlan: 9
Protected Instance: 0
WTR Timer(min): 5
Guard Timer(ms): 500
Holdoff Timer(ms): 0
WTB Timer(ms): 5000
Ring State: idle
Revertive Mode: True
Node Mode: normal
R-APS Virtual Channel Mode: True
Sub-ring: True
Major-ring ID: 1
--------------------------------------------------------------------------------
 PortPort RolePort StatusSignal StatusForced SwitchManual Switch
--------------------------------------------------------------------------------
 eth1/0/3NormalForwardingNon-failedFalseFalse
 eth1/0/2NormalForwardingNon-failedFalseFalse

# Проверка конфигурации на 4
Node4(config)# show erps ring 2
Ring ID: 2
Control Vlan: 9
Protected Instance: 0
WTR Timer(min): 5
Guard Timer(ms): 500
Holdoff Timer(ms): 0
WTB Timer(ms): 5000
Ring State: idle
Revertive Mode: True
Node Mode: owner
```

R-APS Virtual Channel Mode: False
Sub-ring: False

PortPort RolePort StatusSignal StatusForced SwitchManual Switch
---
eth1/0/17RPL PortDiscardingNon-failedFalseFalse
eth1/0/18NormalForwardingNon-failedFalseFalse

21 ACL (ACCESS CONTROL LIS)/ СПИСОК УПРАВЛЕНИЯ ДОСТУПОМ

21.1 Обзор ACL

Список управления доступом (ACL) — это список инструкций для интерфейсов маршрутизатора и коммутатора, используемый для управления потоком пакетов, входящих и исходящих из портов. Это сетевая технология, используемая для контроля доступа. После настройки ACL можно ограничить сетевой трафик, разрешить доступ определенным устройствам и указать пересылку пакетов через определенные порты.

21.2 Введение в технологию ACL

На примере одного порта определение того, какой ACL будет выполняться на порту, зависит от последовательности выполнения условий в списке. Если заголовок пакета соответствует оператору условия в списке, последующие операторы игнорируются и дальнейшие проверки не выполняются.

Пакет сравнивается со следующим оператором условия в ACL, только если он не соответствует первому оператору условия. Если совпадение есть (при условии, что его отправка разрешена), независимо от последующих операторов, данные будут немедленно отправлены на интерфейс назначения. Если все условия ACL проверены и совпадений по-прежнему нет, пакет будет считаться отклоненным и отброшен.

21.2.1 Список контроля доступа

Список управления доступом на уровне канала передачи данных

Таблица соответствия MAC-адресов источника/назначения пакетов канального уровня, позволяющая выполнять операции отказа, разрешения или перенаправления. Диапазон нумерации 2000-2999.

Список контроля доступа уровень канала передачи данных, сетевого уровня и транспортного уровня

Таблица соответствия исходных MAC-адресов, исходных IP-адресов, номеров портов и типов протоколов пакетов канального уровня, сетевого уровня и транспортного уровня, позволяющая выполнять операции отказа, разрешения или перенаправления. Диапазон нумерации: 3000-3999.

Список управления доступом на уровне канала передачи данных

Таблица соответствия MAC-адресов назначения, IP-адресов назначения, номеров портов и типов протоколов пакетов уровня канала передачи данных, сетевого уровня и транспортного уровня, позволяющая выполнять операции отклонения, разрешения или перенаправления. Диапазон нумерации от 4000-4999.

21.2.2 Маски подстановочных знаков (Wildcard Masks)

В масках с подстановочными знаками «1» указывает биты, которые необходимо проверить, а «0» указывает на биты, которые не нужно проверять. Например, при сопоставлении MAC-адресов, если MAC-адрес — 8c1f64:000001, а подстановочная маска — FF:FF:FF:FF:FF:00, он соответствует MAC-адресам в формате 8c1f64:0000XX.

В масках с подстановочными знаками все 0 могут использоваться для обозначения всех адресов (MAC-адресов, IP-адресов, номеров портов, типов протоколов). Это связано с тем, что все 0 указывают на то, что биты не нуждаются в проверке, и в этом случае в качестве замены можно использовать «любой». И наоборот, когда все биты в подстановочной маске установлены на 1, это означает, что все поля должны совпадать, что указывает только на один IP-адрес.

21.3 Конфигурация ACL

21.3.1 Общие настройки ACL

Таблица 84 – Команды для общей настройки ACL

Команды	Описание	Режим
acl number <acl-number> [name <acl-name>]	Создать/войти ACL	“(config)#”
no acl (all | name <acl-name> | number <acl-number>)	Удалить ACL	“(config)#”
description <text>	Настроить описание ACL	“(acl)#”
rule <rule-id> (deny | permit) <src-ip/mask>	Создать базовые правила IP ACL.	“(acl-basic)#”
rule <rule-id> (deny | permit) <tcp | udp> src-ip <src-port> dst-ip <dst-port> (dscp <dscp> | precedence <precedence> | tcp-flag <+ack+fin+psh+rst+syn+urg>)	Создать расширенные правила IP ACL	“(acl-adv)#”
rule <rule-id> (deny | permit) <src-mac> <dst-mac> [cos <cosvalue> | ethtype <ethtype> | vlan <vlan-id>]	Создать правила MAC ACL уровня 2	“(acl-l2)#”
no rule <rule-id>	Удалить правило ACL	“(acl)#”
acl ipv6 number <acl-number> name <acl-name>	Создать список контроля доступа IPv6	“(config)#”

21.3.2 Конфигурация привязки портов

Таблица 85 – Команды конфигурации привязки портов

Команды	Описание	Режим
traffic filter (ingress | engress) acl [ipv6] (name <string> | number <index>) <acl-rule>	Фильтровать поток	“(config-eth)”
traffic limit (ingress | engress) acl [ipv6] (name <string> | number <index>) <target-rate>	Ограничить скорость	“(config-eth)”
traffic priority ingress acl [ipv6] (name <string> | number <index>) (cos | dscp) <value>	Приоритет трафика	“(config-eth)”
traffic redirect ingress acl [ipv6] (name <string> | number <index>) [acl-rule] (cpu | interface <interface-type> <interface-number>)	Перенаправить трафик	“(config-eth)”
traffic mirrored-to (ingress | egress) acl [ipv6] (name <string> | number <index>) interface	Мониторинг трафика	“(config-eth)”

<interface-type> <interface-number>		
traffic remark-vlanid ingress acl [ipv6] (name <string> | number <index>) vlan <vlan-id>	Сопоставить трафик VLAN	“(config-eth)”
traffic statistic (ingress | egress) acl [ipv6] (name <string> | number <index>) <acl-rule>	Статистика трафика	“(config-eth)”
clear traffic-statistic (ingress | egress) acl [ipv6] (name <string> | number <index>) <acl-rule>	Очистить статистику трафика	“(config-eth)”

21.3.3 Показать ACL

Таблица 86 – Команды для просмотра ACL

Команды	Описание	Режим
show acl [ipv6] (<all | acl-number> | name <acl-name>)	Показать ACL и привязку	“#”
show acl resource	Показать системные ресурсы ACL	“#”
show traffic (ilter | limit | redirect | mirrored-to | remark-vlanid | statistic) (all | interface <interface-type> <interface-number>)	Показать информацию об управлении трафиком	“#”

21.4 Пример настройки

1. Требования к сети

— Port 2 маршрутизатора фильтрует исходный IP-адрес 192.168.2.200.

— Port 1 маршрутизатора фильтрует исходный MAC-адрес C8C50E-000001.



Рисунок 31 - Схема топологии сети

2. План настройки

— Создать индекс 2000 и назвать его 2000. Войти в индекс 1, чтобы создать правило 1 с условием фильтра, установленным на src-ipv4 192.168.2.200, настроить действие как отбросить и привязать его к Port 1.

— Создать индекс 4000 и назвать его 4000. Войти в индекс 1, чтобы создать правило 1 с условием фильтра, установленным на src-mac C8C50E-000001, настроить действие как отбросить и привязать его к Port 2.

3. Шаги настройки

#Настройка правила на port 1

SWITCH# configure

SWITCH(config)# acl number 2000 name 2000

SWITCH(acl-basic-2000)# rule 1 deny 192.168.2.200/24

SWITCH(acl-basic-2000)# exit

SWITCH(config)# interface ethernet 1/0/1

SWITCH(config-eth1/0/1)# traffic filter ingress acl number 2000 1

Настройка правила на port 1

SWITCH# configure

SWITCH(config)# acl number 4000 name 4000

SWITCH(acl-l2-4000)# rule 1 deny c8:c5:0e:00:00:01/ff:ff:ff:ff:ff:ff any

SWITCH(acl-basic-4000)# exit

SWITCH(config-eth)# interface ethernet 1/0/2

SWITCH(config-eth1/0/2)# traffic filter ingress acl number 4000 1

4. Проверка конфигурации

Просмотр созданных правил ACL и соответствующей привязки на портах коммутатор

SWITCH# show acl all

Basic ACL number 2000 name 2000

rule 1 deny 192.168.2.200/0.0.0.0

L2 ACL number 4000 name 4000

rule 1 deny C8:C5:0E:00:00:01/FF:FF:FF:FF:FF:FF any

Total ACL number is 2

22 Защита IP-источника/ IP Source Guard

В этой главе представлено подробное описание защиты IP-источника:

- Введение в защиту IP-источника;
- Настройка IP Source Guard;
- Пример настройки IP Source Guard;

22.1 Обзор защиты IP-источника

IP Source Guard (IPSG) — это технология фильтрации трафика на основе IP/MAC-адресов, которая предотвращает атаки с подменой IP-адреса в локальной сети (LAN). IPSG гарантирует, что IP-адреса терминальных устройств в сетях уровня 2 не будут перехвачены, а неавторизованные устройства не смогут получить доступ к сети или атаковать ее, указав свои собственные IP-адреса, тем самым вызывая сбои в сети.

22.1.1 Принципы IPSG

Внутри коммутатора имеется таблица привязки IP-источника (IP Source Binding Table), служащая стандартом обнаружения пакетов, полученных на каждом порту. Коммутатор передает данные только при двух условиях:

1. Полученный IP-пакет соответствует соотношению порт/IP/MAC в таблице привязки источника IP.

2. Полученный пакет является пакетом DHCP.

Все остальные пакеты будут отброшены коммутатором.

Таблица привязки IP-источника может быть статически настроена пользователями коммутатора или автоматически создана коммутатором из таблицы привязки DHCP SNOOPING . Статическая конфигурация — простой и фиксированный метод, но ему не хватает гибкости. Поэтому пользователям рекомендуется комбинировать IP Source Guard с технологией DHCP-snooping, что позволяет генерировать таблицу привязки IP-источника на основе таблицы привязки DHCP-snooping.

22.2 Настройка IPSG

22.2.1 18.2.1 Общая конфигурация IPSG

Таблица 87 – Команды для общей настройки конфигурации IPSG

Команда	Описание	Режим
[no] user-bind	Отключить/включить защиту IP-источника	“(config-eth)”

22.2.2 Привязка IP-MAC

Таблица 88 – команды для привязки IP-MAC

Команды	Описание	Режим
user-bind [ip <ip-addr>] [mac <mac-addr>] [vlan <vlan-id>] interface <interface-type> <interface-number>	Добавить привязку IP и MAC	“(config)#”
user-bind [ip <ip-addr>] [mac <mac-addr>] [vlan <vlan-id>]	Добавить привязку IP и MAC	“(config-eth)”
no user-bind [ip <ip-addr>] [mac <mac-addr>]	Удалить привязку IP и MAC	“(config)#”

22.2.3 Показать IPSG

Таблица 89 – Команды для просмотра IPSG

Команды	Описание	Режим
show user-bind (all | interface <interface-type> <interface-number>)	Показать информацию о привязке пользователя	“#”
show user-bind state interface <interface-type> <interface-number>	Показать статус пользователя IPSG	“#”

23 SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)/ СЕТЕВОЙ ПРОТОКОЛ УПРАВЛЕНИЯ

23.1 Обзор SNMP

Простой протокол сетевого управления (Simple Network Management Protocol) SNMP состоит из набора стандартов управления сетью, включая протокол прикладного уровня, схему базы данных и набор объектов ресурсов. Этот протокол поддерживает системы управления сетью для мониторинга устройств, подключенных к сети, на предмет любых условий, вызывающих беспокойство при управлении. SNMP является частью Internet Protocol Suite определённого в Internet Engineering Task Force (IETF).

Целью SNMP является управление разнообразным набором программных и аппаратных платформ, выпускаемых различными поставщиками в Интернете, и на него сильно влияет стандартная структура управления сетью Интернет. SNMP развился до третьей версии протокола со значительно расширенной и улучшенной функциональностью по сравнению с его предшественниками.

23.2 Введение в технологию SNMP

SNMP — это стандарт управления сетью, основанный на наборе протоколов TCP/IP, служащий стандартным протоколом для управления сетевыми узлами (такими как серверы, рабочие станции, маршрутизаторы, коммутаторы и т. д.) в IP-сетях. SNMP позволяет сетевым администраторам повысить эффективность управления сетью, оперативно обнаруживать и решать сетевые проблемы, а также планировать рост сети. Сетевые администраторы также могут получать уведомления и отчеты о тревожных событиях от сетевых узлов через SNMP, чтобы быть в курсе проблем с сетью.

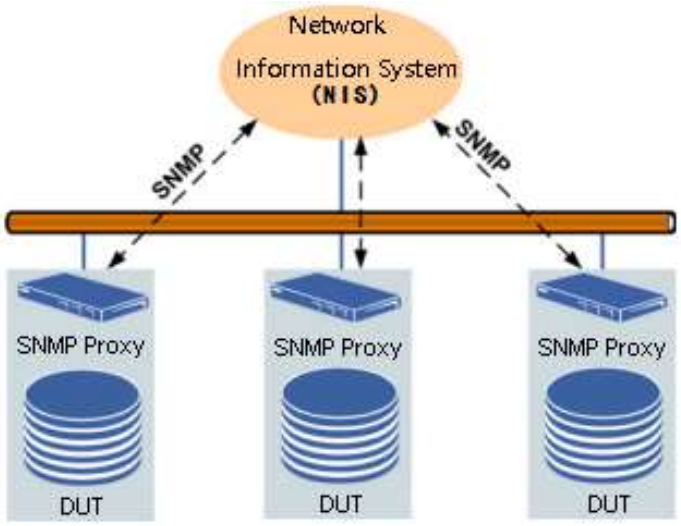

Рисунок 32 - Топология сети управления SNMP

Сеть, управляемая SNMP, в основном состоит из трех частей: управляемые устройства, агенты SNMP и Система управления NMS (Network Management System).

1. Каждое управляемое устройство в сети имеет базу управляющей информации MIB (Management Information Base), используемую для сбора и хранения информации управления. С помощью протокола SNMP NMS может получить эту информацию. Управляемые устройства, также известные как сетевые блоки или сетевые узлы, могут быть маршрутизаторами, коммутаторами, серверами или хостами, поддерживающими протокол SNMP.

2. Агенты SNMP — это программные модули управления сетью на управляемых устройствах, которые содержат соответствующую информацию управления локального устройства. Они отвечают за преобразование этой информации в SNMP-совместимые форматы и передачу ее в NMS.

3. NMS запускает приложения для мониторинга управляемых устройств. Кроме того, NMS предоставляет широкий спектр программ обработки и необходимые ресурсы хранения для управления сетью.

23.2.1 SNMP v3

SNMPv3 в первую очередь улучшает аспекты безопасности за счет применения технологий USM и VACM. USM обеспечивает функции

аутентификации и шифрования, а VACM определяет, разрешен ли пользователям доступ к определенным объектам MIB и каким образом.

USM (User-based Security Model)/Модель безопасности ориентированная на пользователя:

USM представляет концепции имен пользователей и групп, позволяющие настраивать аутентификацию и шифрование. Аутентификация используется для проверки легитимности отправителей сообщений, предотвращая несанкционированный доступ, а шифрование шифрует сообщения, передаваемые между NMS и агентами, для предотвращения подслушивания. Комбинируя функции аутентификации и шифрования, можно достичь более высокого уровня безопасности связи между NMS и агентами.

VACM (View-based Access Control Model)/ Модель управления доступом на основе представлений):

Технология VACM определяет пять элементов: группы, уровни безопасности, контексты, представления MIB и политики доступа. Эти элементы в совокупности определяют, имеют ли пользователи права доступа, при этом только пользователи с такими разрешениями могут управлять операционными объектами. Для одного и того же объекта SNMP можно определить разные группы, при этом группы будут привязаны к представлениям MIB, а в каждой группе будет определено несколько пользователей. При доступе с определенным именем пользователя доступ ограничивается до объектов, определенных в соответствующем представлении MIB.

23.3 Настройка SNMP

23.3.1 Общая конфигурация SNMP

Таблица 90 – Команды общей настройки конфигурации SNMP

Команды	Описание	Режим
snmp status (enable | disable)	Отключить/Включить SNMP	“(config)#”
snmp max-size <max-size>	Максимальная длина сообщения SNMP	“(config)#”
snmp sys-info location <TEXT>	Конфигурация информации о локации SNMP	“(config)#”
snmp sys-info contact <TEXT>	Конфигурация контактной информации SNMP	“(config)#”

snmp sys-info version (v1 | v2c | v3)	SNMP версия	“(config)#”
snmp trust-host (<ip-address> | default)	Доверенный хост	“(config)#”
snmp engineid <enginedidstr>	Engine Flag	“(config)#”
snmp community (public | private | <name>)(ro | rw)	Создать название группы	“(config)#”
[no] snmp community <name>	Удалить название группы	“(config)#”
snmp group <name> (noauthnopriv | authnopriv | authpriv) (ro | rw)	Создать группу	“(config)#”
no snmp group <name>	Удалить группу	“(config)#”
snmp group <name> noauthnopriv user <name>	Создать неаутентифицированных незашифрованных пользователей	“(config)#”
snmp group <name> authnopriv user <name> auth md5 <passwd>	Создать аутентифицированных незашифрованных пользователей	“(config)#”
snmp group <name> authpriv user <name> auth md5 <passwd> priv des <passwd>	Создать аутентифицированных зашифрованных пользователей	“(config)#”
no snmp group <name> user <name>	Удалить пользователя	“(config)#”
snmp trap status (enable | disable)	Включить/отключить SNMP Trap	“(config)#”
[no] snmp trap name <name>	Удалить/создать Trap Server	“(config)#”
snmp trap ip <ip-address>	Настроить Trap Server	“(trap_name)#”
[no] snmp trap udpport <portid>	Установить номер Trap порта	“(trap_name)#”
snmp trap version (v1|v2c|v3) security <name>	Установить версию Trap и имя группы	“(trap_name)#”

23.3.2 Показать SNMP

Таблица 91 – Команды для просмотра SNMP

Команды	Описание	Режим
show snmp status	Показать статус SNMP	“#”
show snmp sys-info (contact | location | version | max-size | engineid | trust-host)	Показать системную информацию SNMP	“#”
show snmp community (all | ro | rw)	Показать информацию community SNMP	“#”
show snmp trap-info	Показать информацию о SNMP Trap	“#”

24 СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Статическая маршрутизация — это информация о маршрутизации, которая настраивается вручную пользователями или сетевыми администраторами. При изменении топологии сети или состояния каналов сетевым администраторам необходимо вручную изменить соответствующую статическую информацию о маршрутизации в таблице маршрутизации. Статическая маршрутизация обычно подходит для относительно простых сетевых сред, где сетевые администраторы имеют четкое представление о топологии сети, что упрощает настройку правильной информации о маршрутизации. Функция статической маршрутизации применима в системах версии L3.

24.1 Введение в технологию

Еще одним преимуществом использования статической маршрутизации является более высокая безопасность и конфиденциальность сети. Динамическая маршрутизация требует, чтобы маршрутизаторы часто обменивались своими таблицами маршрутизации, и анализ этих таблиц может выявить информацию о топологии сети и сетевых адресах. Таким образом, статическую маршрутизацию можно использовать и из соображений безопасности. Статическая маршрутизация не потребляет пропускную способность сети, поскольку не генерирует трафик обновлений.

Большие и сложные сетевые среды обычно не подходят для статической маршрутизации. С одной стороны, сетевым администраторам сложно полностью понять топологию всей сети. С другой стороны, когда меняется топология сети или состояние канала, корректировку статической информации о маршрутизации в маршрутизаторах необходимо производить в больших масштабах, что очень трудно. При изменении сети или возникновении сетевого сбоя статическая маршрутизация не выполняет повторный выбор маршрута, что может привести к сбоям маршрутизации.

24.2 Настройка статической маршрутизации

24.2.1 Общая конфигурация статической маршрутизации

Таблица 92 – Команды общей конфигурации статической маршрутизации

Команды	Описание	Режим
[no] ip route-static <ip-address> <ip-mask> (<next-hop-address> | reject | blackhole) description <WORD>	Создать/удалить статические таблицы маршрутизации	“(config)#”
clear ip route-static (all | static | reject | blackhole)	Удалить таблицу маршрутизации в зависимости от типа	“(config)#”
gratuitous-arp-sending enable interval <timer>	Включить функцию отправки gratuitous ARP	“(config)#”
gratuitous-arp-sending disable	Отключить функцию отправки gratuitous ARP	“(config)#”
gratuitous-arp-learning (enable | disable)	Включить/отключить функцию изучения gratuitous ARP	“(config)#”

24.2.2 Показать конфигурацию статической маршрутизации

Таблица 93 – Просмотр конфигурации статической маршрутизации

Команды	Описание	Режим
show ip routing-table (all | static | direct | reject | blackhole)	Показать таблицу маршрутизации в зависимости от типа	“#”
show ip routing-table <ip-address> <ip-mask>	Показать таблицу маршрутизации на основе сегмента сети	“#”

24.3 Пример настройки статической маршрутизации

1. Требования к сети

Реализовать взаимодействие между хостами путем настройки функции статической маршрутизации.

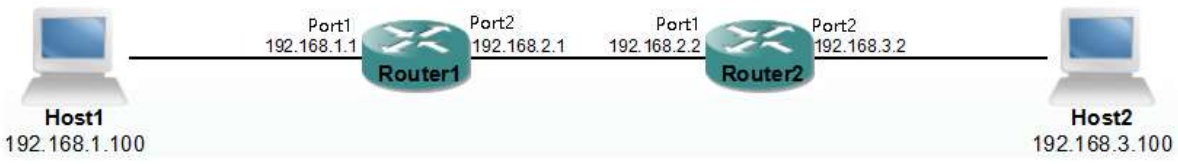

Рисунок 33 - Схема топологии сети

2.План настройки

— Настроить виртуальный интерфейс и Port VLAN

— Добавить соответствующие статические маршруты топологии на всех маршрутизаторах

Шаги настройки

（1）Настроить виртуальный интерфейс и порт VLAN

Настройка виртуальный интерфейс и портов VLAN для Router1

Router1# configure

Router1(config)# vlan 2

Router1(Vlan2)# exit

Router1(config)# interface ethernet 1/0/2

Router1(config-eth1/0/2)# switchport access vlan 2

Router1(config-eth1/0/2)# exit

Router1(config)# interface vlan-interface 1

Router1(Vlan-interface1)# ip address 192.168.1.1 255.255.255.0

Router1(config)# interface vlan-interface 2

Router1(Vlan-interface2)# ip address 192.168.2.1 255.255.255.0

Настройка виртуальных интерфейсов и портов VLAN для Router2

Router2# configure

Router2(config)# vlan 2

Router2(Vlan2)# exit

Router2(config)# interface ethernet 1/0/2

Router2(config-eth1/0/2)# switchport access vlan 2

Router2(config)# interface vlan-interface 1

Router2(Vlan-interface1)# ip address 192.168.2.2 255.255.255.0

Router2(Vlan-interface1)# interface vlan-interface 2

Router2(Vlan-interface2)# ip address 192.168.3.2 255.255.255.0

Добавить статические маршруты

Добавить статические маршруты для Router1

Router1(config)# ip route-static 192.168.3.0 255.255.255.0 192.168.2.2

Добавить статические маршруты для Router2

Router2(config)# ip route-static 192.168.1.1 255.255.255.0 192.168.2.1

4. Проверка конфигурации

Просмотр таблицы маршрутизации

Просмотр таблицы маршрутизации на Router1

Router1(config)# show ip routing-table all

Total Entry: 3

Destination/MaskProtoNextHopInterfaceDes

192.168.1.0/24 Direct192.168.1.1Vlanif1

192.168.2.0/24 Direct192.168.2.1Vlanif2

192.168.3.0/24Static192.168.2.2Vlanif2

Просмотр таблицы маршрутизации на Router2

Router2(config)# show ip routing-table all

Total Entry: 3

Destination/ MaskProtoNextHopInterfaceDes

192.168.1.0/24 Static192.168.2.1Vlanif1

192.168.2.0/24 Direct192.168.2.2Vlanif1

192.168.3.0/24Direct192.168.3.2Vlanif2

25 RIP (ROUTING INFORMATION PROTOCOL)/ ПРОТОКОЛ МАРШРУТИЗАЦИИ ИНФОРМАЦИИ

25.1 Обзор RIP

The Routing Information Protocol (RIP) — это протокол маршрутизации, основанный на алгоритме distance-vector и использующий в качестве метрики количество переходов. Он требует низких затрат на пропускную способность, настройку и управление, что делает его в первую очередь подходящим для небольших сетей.

25.2 Принцип работы

1. Установление маршрутизации

После запуска RIP на маршрутизаторах они сначала отправляют запросы на обновление маршрута. Маршрутизаторы, получающие эти запросы,

отвечают, отправляя свои собственные маршруты RIP. Как только сеть стабилизируется, маршрутизаторы периодически отправляют информацию об обновлении маршрута.

2. Расчет вектора и расстояния

RIP измеряет расстояния в прыжках, при этом каждому прыжку присваивается стоимость, равная 1. Это означает, что стоимость каждого канала считается равной 1, без учета таких факторов, как фактическая пропускная способность или задержка. RIP допускает максимум 15 прыжков.

RIP использует метрики для представления расстояний между собой и всеми известными пунктами назначения. Когда получено сообщение обновления RIP, принимающий маршрутизатор сравнивает его с каждой записью в своей собственной таблице маршрутизации RIP и соответствующим образом корректирует свою таблицу, используя алгоритм маршрутизации по вектору расстояний.

3. Таймеры

Таймер периодического обновления: используется для запуска обновлений таблицы маршрутизации маршрутизатора RIP. Каждый узел RIP имеет только один таймер обновления, установленный на 30 секунд. Каждые 30 секунд маршрутизаторы передают информацию о своей таблице маршрутизации своим соседям. Таймеры обновления каждого RIP-маршрутизатора не зависят от других маршрутизаторов в сети, поэтому вероятность их одновременного вещания минимальна.

Таймер тайм-аута: используется для определения возможности использовать маршрут. Каждый маршрут имеет тайм-аута, установленный на 180 секунд. Когда маршрут активирован или обновлен, этот таймер инициализируется. Если в течение 180 секунд не поступает никаких обновлений об этом маршруте, маршрут помечается как недействительный.

Таймер очистки: используется для определения необходимости очистки маршрута. Каждый маршрут имеет таймер очистки, установленный на 120 секунд. Когда маршрутизатор понимает, что маршрут недействителен, он инициализирует таймер очистки. Если в течение 120 секунд не поступает никаких обновлений об этом маршруте, маршрут удаляется из таблицы маршрутизации.

Таймер удержания: случайный таймер задержки, установленный на время от 1 до 5 секунд, введенный для предотвращения запуска обновлений, которые могут привести к широковещательному шторму.

4. Предотвращение петель маршрутизации

В случае сетевых сбоев в сетях RIP могут возникать петли маршрутизации. Чтобы избежать образования петель, используются такие методы, как разделение горизонта (split horizon), обратное отравление (poison reverse), запускаемые обновления (triggered updates) и таймеры подавления маршрутов (route suppression timers).

25.3 Настройка RIP

25.3.1 Общая конфигурация RIP

Таблица 94 – Команды для конфигурации RIP

Команды	Описание	Режим
[no] router rip	Отключить/включить RIP	“(config)#”
[no] network <ip-address>/<mask-len>	Отменить/объявить указанную сеть	“(rip-router)”
[no] timers basic <update-timer> <timeout-timer> <collection-timer>	Восстановить/установить значение таймера	“(rip-router)”
debugging rip	Включить отладку	“(config)#”

25.3.2 Показать RIP

Таблица 95 – Команды для просмотра RIP

Команды	Описание	Режим
show ip rip	Показать информацию о протоколе RIP	“#”
show ip rip status	Показать информацию о состоянии протокола RIP	“#”

25.4 Пример настройки

25.4.1 Критерий задач конфигурации

Таблица 96 - Критерий задач конфигурации

Критерий задач конфигурации	Описание
Включить RIP	Необходимый
Объявить назначенную сеть	Необходимый
Установить значение таймера	Необязательный

25.4.2 Пример настройки

1. Требования к сети

— Router1, Router2, и Router3 динамически изучают и поддерживают маршрут через RIP.

— Host1, Host2, и Host3 могут иметь доступ друг к другу.

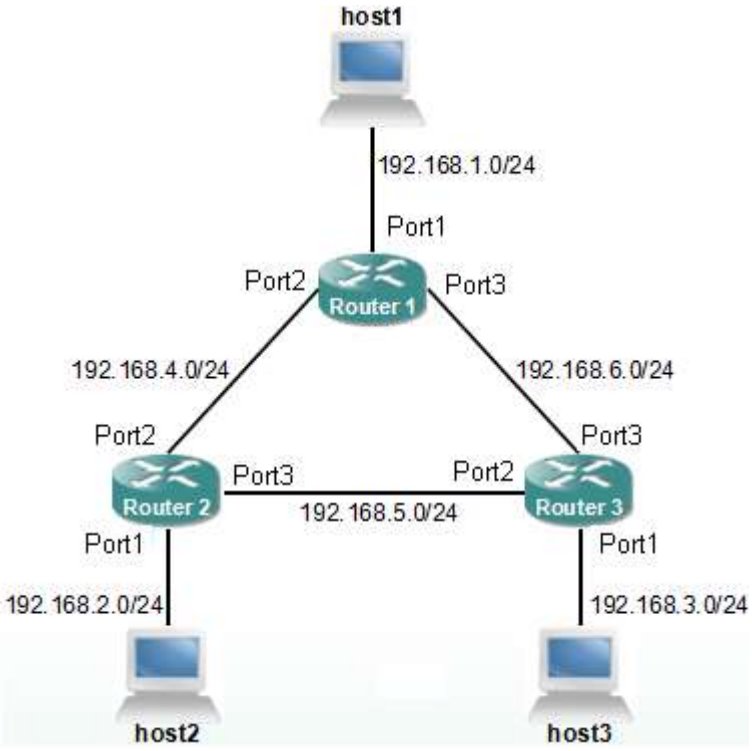

Рисунок 34 - Схема топологии сети

2. План настройки

— Настроить виртуальные IP-интерфейсы и соответствующие порты для Router1, Router2, и Router3.

— Включить RIP на Router1, Router2, и Router3 и анонсировать сети.

3. Шаги настройки

（1）Создать VLAN 2–3, настроить виртуальные интерфейсы и соответствующие порты.

```
# Настройка Router1
Router1# configure
Router1(config)# vlan 2-3
Router1(config)# interface ethernet 1/0/2
Router1(config-eth1/0/2)# switchport access vlan 2
Router1(config-eth1/0/2)# interface ethernet 1/0/3
Router1(config-eth1/0/3)# switchport access vlan 3
Router1(config-eth1/0/3)# exit
Router1(config)# interface vlan-interface 1
Router1(Vlan-interface1)# ip address 192.168.1.1 255.255.255.0
Router1(Vlan-interface1)# interface vlan-interface 2
Router1(Vlan-interface2)# ip address 192.168.4.1 255.255.255.0
Router1(Vlan-interface2)# interface vlan-interface 3
Router1(Vlan-interface3)# ip address 192.168.6.1 255.255.255.0
# Настройка Router2
Router2# configure
Router2(config)# vlan 2-3
Router2(config)# interface ethernet 1/0/2
Router2(config-eth1/0/2)# switchport access vlan 2
Router2(config-eth1/0/2)# interface ethernet 1/0/3
Router2(config-eth1/0/3)# switchport access vlan 3
Router2(config-eth1/0/3)# exit
Router2(config)# interface vlan-interface 1
Router2(Vlan-interface1)# ip address 192.168.2.2 255.255.255.0
Router2(Vlan-interface1)# interface vlan-interface 2
Router2(Vlan-interface2)# ip address 192.168.4.2 255.255.255.0
Router2(Vlan-interface2)# interface vlan-interface 3
Router2(Vlan-interface3)# ip address 192.168.5.2 255.255.255.0
# Настройка Router3
Router3# configure
Router3(config)# vlan 2-3
Router3(config)# interface ethernet 1/0/2
Router3(config-eth1/0/2)# switchport access vlan 2
```

Router3(config-eth1/0/2)# interface ethernet 1/0/3
Router3(config-eth1/0/3)# switchport access vlan 3
Router3(config-eth1/0/3)# exit
Router3(config)# interface vlan-interface 1
Router3(Vlan-interface1)# ip address 192.168.3.3 255.255.255.0
Router3(Vlan-interface1)# interface vlan-interface 2
Router3(Vlan-interface2)# ip address 192.168.5.3 255.255.255.0
Router3(Vlan-interface2)# interface vlan-interface 3
Router3(Vlan-interface3)# ip address 192.168.6.3 255.255.255.0

（2）Включить RIP и анонсировать сеть.

Настройка Router1
Router1# configure
Router1(config)# router rip
Router1(rip-router)# network 192.168.1.0/24
Router1(rip-router)# network 192.168.4.0/24
Router1(rip-router)# network 192.168.6.0/24
Настройка Router2
Router2# configure
Router2(config)# router rip
Router2(rip-router)# network 192.168.2.0/24
Router2(rip-router)# network 192.168.4.0/24
Router2(rip-router)# network 192.168.5.0/24
Настройка Router3
Router3# configure
Router3(config)# router rip
Router3(rip-router)# network 192.168.3.0/24
Router3(rip-router)# network 192.168.5.0/24
Router3(rip-router)# network 192.168.6.0/24

4. Проверка конфигурации

Просмотр таблицы маршрутизации на Router1
Router1# show ip routing-table all
Total Entry: 6

Destination/MaskProtoNextHopInterfaceDes

192.168.1.0/24Direct192.168.1.1Vlanif1
192.168.2.0/24ip192.168.4.2Vlanif2
192.168.3.0/24Rip192.168.6.3Vlanif3
192.168.4.0/24Direct192.168.4.1Vlanif2
192.168.5.0/24Rip192.168.6.3Vlanif3
192.168.6.0/24Direct192.168.6.1Vlanif3
Просмотр таблицы маршрутизации на Router2
Router2# show ip routing-table all
Total Entry: 5

Destination/MaskProtoNextHopInterfaceDes
192.168.1.0/24Rip192.168.4.1Vlanif2
192.168.2.0/24Direct192.168.2.2Vlanif1
192.168.4.0/24Direct 192.168.4.2Vlanif2
192.168.5.0/24Direct 192.168.5.2Vlanif3
192.168.6.0/24Rip 192.168.4.1Vlanif2
Просмотр таблицы маршрутизации на Router3
Router3# show ip routing-table all
Total Entry: 6

Destination/MaskProtoNextHopInterfaceDes
192.168.1.0/24Rip 192.168.6.1Vlanif3
192.168.2.0/24Rip 192.168.5.2Vlanif2
192.168.3.0/24Direct192.168.3.3Vlanif1
192.168.4.0/24Rip192.168.5.2Vlanif2
192.168.5.0/24Direct192.168.5.3Vlanif2
192.168.6.0/24Direct192.168.6.3Vlanif3

26 OSPF (OPEN SHORTEST PATH FIRST)/ ПРОТОКОЛ ВНУТРЕННЕГО ШЛЮЗА

26.1 Обзор OSPF

OSPF (Open Shortest Path First) это протокол внутреннего шлюза IGP (Interior Gateway Protocol), используемый для принятия решений о маршрутизации внутри одной автономной системы AS (Autonomous System). Это реализация протокола маршрутизации по состоянию канала (link-state), которая работает в рамках автономной системы как IGP. Для вычисления дерева кратчайших путей используется известный алгоритм Дейкстры. OSPF разделен на две версии: OSPFv2 и OSPFv3, где OSPFv2 используется в сетях IPv4, а OSPFv3 — в сетях IPv6. OSPFv2 определен в RFC 2328, а OSPFv3 — в RFC 5340. По сравнению с RIP, OSPF — это link-state протокол, тогда как RIP — это distance-vector протокол.

26.2 Терминология и понятия

Router-ID: router-ID служит уникальным идентификатором маршрутизаторов в OSPF.

DR/BDR: Выделенный маршрутизатор DR (Designated Router) и Резервный выделенный маршрутизатор BDR (Backup Designated Router) назначаются для подключения к локальной сети. OSPF выбирает один маршрутизатор в качестве DR, а другой — в качестве BDR. Все остальные маршрутизаторы, подключенные к DR и BDR, образуют полностью смежные состояния и передают только объявления о состоянии канала LSA (Link State Advertisements) на DR и BDR.

OSPFArea: Маршрутизаторам внутри области не обязательно понимать детали топологии за пределами своей области. OSPF разделяет Autonomous System (AS) на несколько областей и соединяет их через магистральную зону (backbone area). Маршрутизаторам необходимо иметь ту же самую базу данных состояния каналов LSDB (Link State Database), что и другие маршрутизаторы в их зоне, что позволяет сократить количество обрабатываемых LSA и ограничить рассылку в пределах одной области.

Внутри области существует три типа трафика: внутриобластной трафик, межобластной трафик и внешний трафик.

Internal Router: Маршрутизаторы с одинаковым Area-ID.

Area Border Routers (ABR) : Маршрутизатор, расположенный между одной или несколькими OSPF Area и соединяющий эти области с магистральной сетью.

Backbone Router : Маршрутизаторы, у которых хотя бы один интерфейс принадлежит магистральной области (идентификатор Area 0). Таким образом, все ABR и внутренние маршрутизаторы, расположенные в Area 0, являются магистральными маршрутизаторами.

Autonomous System Boundary Router (ASBR) : Маршрутизатор, обменивающийся информацией о маршрутизации с другими AS. ASBR, не обязательно могут располагаться на границе AS; это могут быть внутренние маршрутизаторы или ABR. Любой маршрутизатор OSPF, предоставляющий информацию о внешнем маршруте, становится ASBR.

Area-id : Маршрутизаторы должны быть настроены в одной и той же OSPF Area для формирования соседей; в противном случае они не смогут установить смежность.

Hello and Dead Interval : Интервалы Hello и Dead между маршрутизаторами должны быть одинаковыми для формирования соседей; в противном случае смежность не может быть установлена.

Authentication : Маршрутизаторы должны быть настроены с одним и тем же паролем аутентификации; в противном случае они не смогут устанавливать соседство.

Adjacency : Два маршрутизатора OSPF могут устанавливать соседство, но они не обязательно могут обмениваться LSA. Если они обмениваются LSA, отношения называются смежностью (adjacency). В то время как соседи (neighbors) обмениваются только пакетами Hello, смежныен маршрутизаторы обмениваются как пакетами Hello, так и LSA.

26.3 Конфигурация OSPF

26.3.1 Общая конфигурация OSPF

Таблица 97 – Команды общей конфигурация OSPF

Команды	Описание	Режим
[no] router ospf	Отключить/включить OSPF	“(config)#”
[no] ospf router-id <router-Id>	Отменить/настроить идентификатор маршрутизатора	“(ospf-router) #”
[no] network <ip-address>/<mask-len> area <area-id>	Удалить/включить объявление сети OSPF	“(ospf-router) #”

26.3.2 Конфигурация домена OSPF

Таблица 98 – Команды для конфигурации домена OSPF

Команда	Описание	Режим
[no] area <area-id> stub	Отменить/настроить область STUB	“(ospf-router) #”
[no] area <area-id> stub no-summary	Отключить/включить отсутствие сводки домена STUB	“(ospf-router) #”
[no] area <area-id> nssa	Отменить/настроить домен NSSA	“(ospf-router) #”
[no] area <area-id> nssa no-summary	Отключить/включить отсутствие сводки домена NSSA	“(ospf-router) #”
area <area-id> nssa (translate-candidate | translate-never | translate-always) [no-summary]	Установить свойства домена NSSA	“(ospf-router) #”
[no] area <area-id> default-cost <cost-value>	Установить стоимость по умолчанию для домена OSPF	“(ospf-router) #”
[no] area <area-id> virtual-link <router-id>	Удалить/создать virtual-link	“(ospf-router) #”
area <area-id> virtual-link <router-id> hello-interval <time>	Отменить/настроить интервал приветствия виртуального соединения	“(ospf-router) #”
[no] area <area-id> virtual-link <router-id> authentication	Отключить/включить режим аутентификации виртуального соединения как открытый текст	“(ospf-router) #”
[no] area <area-id> virtual-link <router-id> authentication authentication-key <auth-key>	Удалить/настроить ключ для текстовой аутентификации виртуальных соединений	“(ospf-router) #”
[no] area <area-id> virtual-link <router-id> authentication authentication-key message-digest	Отменить/настроить режим аутентификации виртуального канала — аутентификация MD5	“(ospf-router) #”
[no] area <area-id> virtual-link <router-id> authentication authentication-key message-	Удалить/настроить ключ для аутентификации MD5 виртуального канала	“(ospf-router) #”

digest message-digest-key <key-id> md5 <md-key>		
[no] area <area-id> virtual-link <router-id> retransmit-interval <time>	Восстановить/Настроить Virtual Link интервал повторной передачи	“(ospf-router) #”
[no] area <area-id> virtual-link <router-id> dead-interval <time>	Восстановить/настроить время простоя виртуального канала	“(ospf-router) #”
[no] area <area-id> virtual-link <router-id> transmit-delay <time>	Восстановить/настроить время задержки транзита виртуального канала	“(ospf-router) #”

26.3.3 Конфигурация агрегации междоменной маршрутизации OSPF

Таблица 99 – Команды для конфигурации агрегации междоменной маршрутизации OSPF

Команда	Описание	Режим
[no] area <area-id> range <ip-address>/<mask-len>	Удалить/создать агрегацию интервальной маршрутизации	“(ospf-router) #”
area <area-id> range <ip-address>/<mask-len> (advertise | not-advertise)	Настроить объявления/необъявления агрегации маршрутизации	“(ospf-router) #”
[no] area <area-id> range <ip-address>/<mask-len> [advertise] cost <cost-value>	Восстановить/настроить служебную маршрутизацию агрегации	“(ospf-router) #”
[no] area <area-id> range <ip-address>/<mask-len> substitute <ip-address>/<mask-len>	Удалить/создать заменяющий сегмент сети агрегации маршрутизации	“(ospf-router) #”

26.3.4 Настройка интерфейса OSPF

Таблица 100 – Команды для настройки интерфейса OSPF

Команда	Описание	Режим
[no] ospf cost <cost-value>	Восстановить/настроить издержки интерфейса	«(Vlan-interface)#”
[no] ospf priority <priority-value>	Восстановить/настроить приоритет интерфейса	«(Vlan-interface)#”
[no] ospf mtu-ignore	Отключить/включить mtu-ignore	«(Vlan-interface)#”

26.3.5 Показать OSPF

Таблица 101 – Команды для просмотра OSPF

Команда	Описание	Режим
show ip ospf	Показать конфигурацию OSPF	“#”
show ip ospf neighbor [all | detail]	Показать соседства OSPF	“#”
show ip ospf database [asbr-summary | external | network | router | summary | nssa-external | opaque-link | opaque-link | opaque-area | opaque-as | max-age | self-originate]	Показать информацию о базе данных OSPF	“#”
show ip ospf route	Показать маршрутизатор OSPF	“#”
show ip ospf border-routers	Показать таблицу выбора граничной маршрутизации	“#”

26.4 Пример настройки

26.4.1 Критерий задач конфигурации

Таблица 102 - Критерий задач конфигурации

Критерий задач конфигурации	Описание
Включить OSPF	Необходимый
Настроить идентификатор маршрутизатора	Необязательный
Объявить сеть OSPF	Необходимый
Настроить домен STUB	Необязательный
Настроить домена NSSA	Необязательный
Накладные расходы по умолчанию для домена OSPF	Необязательный
Настройка виртуального канала	Необязательный
Настройка агрегации интервальной маршрутизации	Необязательный
Настройка интерфейса	Необязательный

26.4.2 Пример настройки

1. Требования к сети

— Router1, Router2 и Router3 динамически изучают и поддерживают маршрут через OSPF.

— Сегмент сети 192.168.1.0 разделен на область «1», 192.168.2.0/24 сегмент сети 192.168.3.0/24 разделен на область «0», 192.168.4.0/24 сегмент сети разделен на область 2.

— Host1 and Host2 могут иметь доступ друг к другу.

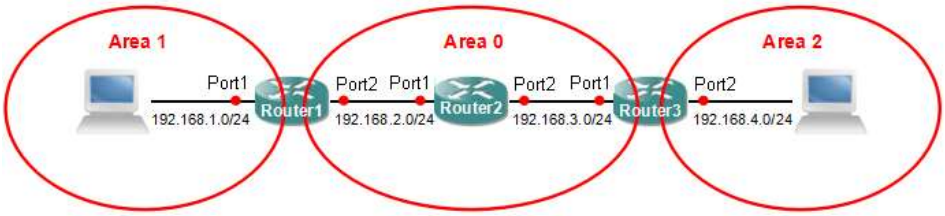

Рисунок 35 - Схема топологии сети

2. План настройки

— Настроить виртуальные IP-интерфейсы и порты для Router1, Router2 и Router3.

— На Router1, Router2 и Router3 включить OSPF и объявление сетей.

3. Шаги настройки

（1）Создать VLAN 2, настроить виртуальные интерфейсы и настроить соответствующие связанные порты.

Настройка Router1

Router1# configure

Router1(config)# vlan 2

Router1(config)# interface ethernet 1/0/2

Router1(config-eth1/0/2)# switchport access vlan 2

Router1(config-eth1/0/2)# exit

Router1(config)# interface vlan-interface 1

Router1(Vlan-interface1)# ip address 192.168.1.1 255.255.255.0

Router1(Vlan-interface1)# interface vlan-interface 2

Router1(Vlan-interface2)# ip address 192.168.2.1 255.255.255.0

Настройка Router2

Router2# configure

Router2(config)# vlan 2

Router2(config)# interface ethernet 1/0/2

Router2(config-eth1/0/2)# switchport access vlan 2

Router2(config-eth1/0/2)# exit

Router2(config)# interface vlan-interface 1

Router2(Vlan-interface1)# ip address 192.168.2.2 255.255.255.0

Router2(Vlan-interface1)# interface vlan-interface 2

Router2(Vlan-interface2)# ip address 192.168.3.2 255.255.255.0

Настройка Router3

Router3# configure

Router3(config)# vlan 2
Router3(config)# interface ethernet 1/0/2
Router3(config-eth1/0/2)# switchport access vlan 2
Router3(config-eth1/0/2)# exit
Router3(config)# interface vlan-interface 1
Router3(Vlan-interface1)# ip address 192.168.3.3 255.255.255.0
Router3(Vlan-interface1)# interface vlan-interface 2
Router3(Vlan-interface2)# ip address 192.168.4.3 255.255.255.0

（2）Включить OSPF и объявить сети.

Настройка Router1
Router1(config)# router ospf
Router1(ospf-router)# network 192.168.1.0/24 area 1
Router1(ospf-router)# network 192.168.2.0/24 area 0
Настройка Router2
Router2(config)# router ospf
Router2(ospf-router)# network 192.168.2.0/24 area 0
Router2(ospf-router)# network 192.168.3.0/24 area 0
Настройка Router3
Router3(config)# router ospf
Router3(config-ospf)# network 192.168.3.0/24 area 0
Router3(config-ospf)# network 192.168.4.0/24 area 2

4. Проверка конфигурации
Просмотр таблицы маршрутизации на Router1
Router1# show ip routing-table all
Total Entry: 4

Destination/MaskProtoNextHopInterfaceDes
192.168.1.0/24 Direct192.168.1.1Vlanif1
192.168.2.0/24 Direct192.168.2.1Vlanif2
192.168.3.0/24 Ospf192.168.2.2Vlanif2
192.168.4.0/24 Ospf192.168.2.2Vlanif2
Просмотр таблицы маршрутизации на Router2
Router2# show ip routing-table all
Total Entry: 4

```
------------------------------------------------------
Destination/MaskProtoNextHopInterfaceDes
192.168.1.0/24Ospf192.168.2.1Vlanif1
192.168.2.0/24Direct192.168.2.2Vlanif1
192.168.3.0/24Direct192.168.3.2Vlanif2
192.168.4.0/24Ospf192.168.3.3Vlanif2
 # Просмотр таблицы маршрутизации на Router3
Router3# show ip routing-table all
Total Entry: 4
------------------------------------------------------
Destination/MaskProtoNextHopInterfaceDes
192.168.1.0/24      Ospf192.168.3.2Vlanif1
192.168.2.0/24      Ospf192.168.3.2Vlanif1
192.168.3.0/24Direct192.168.3.3Vlanif1
192.168.4.0/24Direct192.168.4.3Vlanif2
```

27 POE (POWER OVER ETHERNET)/ ПИТАНИЕ ЧЕРЕЗ ETHERNET

В этой главе представлены подробные описания команд CLI, связанных с функцией Power over Ethernet (PoE).

Примечание - функции этой главы поддерживаются только на коммутаторах, оснащенных функцией PoE. Конкретные функции могут различаться в зависимости от конкретного устройства и его модели.

27.1 Введение в PoE

Power over Ethernet (PoE), также известное как удаленное питание, означает способность устройств подавать питание на питаемые устройства (PD) удаленно через кабели Ethernet. PoE предлагает несколько преимуществ:

Надёжность: централизованное электроснабжение упрощает резервирование.

Простое подключение: сетевые терминалы не требуют внешних источников питания, только один сетевой кабель.

Стандартизация: соответствует стандартам IEEE 802.3af/IEEE 802.3at, использует глобально унифицированный интерфейс питания.

Широкое применение: подходит для IP-телефонов, беспроводных точек доступа (AP), портативных зарядных устройств, устройств считывания карт, сетевых камер, устройств сбора данных и т. д.

Система PoE показана на схеме ниже и состоит из источника питания PoE, оборудования источника питания (PSE), интерфейса питания (PI) и питаемого устройства (PD).

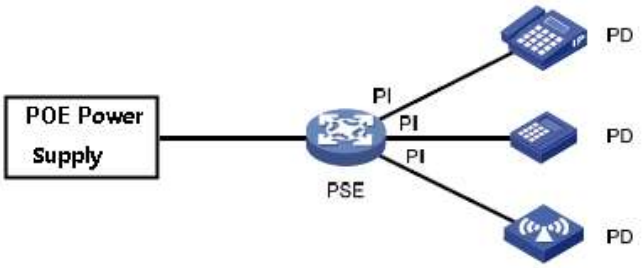

Рисунок 36 – Схема PoE

Устройства PSE относятся к оборудованию, которое напрямую подает питание на PD. PSE делятся на два типа: встроенные (Endpoint) и внешние (Midspan). «Встроенные» относятся к PSE, интегрированным в коммутаторы/маршрутизаторы, а «внешние» относятся к PSE, независимым от коммутаторов/маршрутизаторов. Все устройства нашей компании используют встроенный подход.

PI относится к интерфейсам Ethernet с возможностью подачи питания PoE, также известным как интерфейсы PoE, включая интерфейсы FE и GE.

Под устройствами PD подразумевается оборудование, которое принимает питание от PSE, например IP-телефоны, точки беспроводного доступа (AP), зарядные устройства для портативных устройств, устройства считывания карт и сетевые камеры. Устройства PD могут подключаться к другим источникам питания для резервирования, получая питание по PoE.

Устройства PD подразделяются на стандартные PD и нестандартные PD. Стандартные PD относятся к устройствам, соответствующим стандартам IEEE

802.3af/at. Обычно PSE могут обнаруживать только стандартные PD и подавать на них питание. Только когда функция обнаружения нестандартных PD включена, PSE могут обнаруживать и подавать питание на нестандартные PD.

27.2 Конфигурация POE

27.2.1 Конфигурация POE

Таблица 103 – Команды конфигурации POE

Команда	Описание	Режим
poe (enable | disable)	Отключить/включить POE	“(config-eth)”
poe legacy (enable|disable)	Отключить/включить нестандартный POE	“(config-eth)”
poe power limit <power-limit>	Установить ограничение мощности	“(config-eth)”
poe priority (low | high | critical) **no poe priority**	Установить приоритет ограничения мощности	“(config-eth)”

27.2.2 Показать POE

Таблица 104 – Команда для просмотра PoE

Команда	Описание	Режим
show poe info	Показать информацию о конфигурации POE	“#”
show poe status	Показать информацию о статусе POE	“#”

27.3 Пример настройки

27.3.1 Критерий задач конфигурации

Таблица 105 - Критерий задач конфигурации

Критерий задач конфигурации	Описание
Включить POE	Необходимый
Включить нестандартное POE	Необязательный
Установить ограничение мощности	Необязательный
Установить приоритет ограничения мощности	Необязательный

27.3.2 Пример настройки

1. Требования к сети
— POE-питание

2. План настройки
— Включить функцию POE порта

3. Шаги настройки
（1）Включить POE

```
SWITCH# configure
SWITCH(config)# interface ethernet 1/0/1
SWITCH(config-eth1/0/1)# poe enable
```

4. Проверка конфигурации
Просмотр конфигурации POE

```
SWITCH(config)# show poe info
Global Config :
 Max Power Limit : 370
-----------------------------------------------
       PORT   ENABLE   LEGACY  LIMIT  PRI
     eth1/0/1  enable  disable    15  low
     eth1/0/2   enable  disable    15  low
     eth1/0/3   enable  disable    15  low
     eth1/0/4   enable  disable    15  low
     eth1/0/5   enable  disable    15  low
     eth1/0/6   enable  disable    15  low
     eth1/0/7   enable  disable    15  low
     eth1/0/8   enable  disable    15  low
     eth1/0/9   enable  disable    15  low
    eth1/0/10   enable  disable    15  low
    eth1/0/11   enable  disable    15  low
    eth1/0/12   enable  disable    15  low
    eth1/0/13   enable  disable    15  low
    eth1/0/14   enable  disable    15  low
    eth1/0/15   enable  disable    15  low
```

eth1/0/16 enable disable 15 low
eth1/0/17 enable disable 15 low
eth1/0/18 enable disable 15 low
eth1/0/19 enable disable 15 low
eth1/0/20 enable disable 15 low
eth1/0/21 enable disable 15 low
eth1/0/22 enable disable 15 low
eth1/0/23 enable disable 15 low
eth1/0/24 enable disable 15 low

Просмотр статуса POE

SWITCH(config-eth1/0/1)# show poe status

Global Config :

Max Power Limit : 370 (W)

Used Power : 2 (W)

Poe Port Num : 24

PORT	ENABLE	LEGACY	STATUS	TEMP	POWER(W)	ELECTRIC(mA)	VOLTAG(V)	CLASS
eth1/0/1	enable	disable	up	27	2	416	48	unknown
eth1/0/2	enable	disable	down	27	0	0	48	unknown
eth1/0/3	enable	disable	down	27	0	0	48	unknown
eth1/0/4	enable	disable	down	27	0	0	48	unknown
eth1/0/5	enable	disable	down	27	0	0	48	unknown
eth1/0/6	enable	disable	down	27	0	0	48	unknown
eth1/0/7	enable	disable	down	27	0	0	48	unknown
eth1/0/8	enable	disable	down	27	0	0	48	unknown
eth1/0/9	enable	disable	down	27	0	0	48	unknown
eth1/0/10	enable	disable	down	27	0	0	48	unknown
eth1/0/11	enable	disable	down	27	0	0	48	unknown
eth1/0/12	enable	disable	down	27	0	0	48	unknown
eth1/0/13	enable	disable	down	27	0	0	48	unknown
eth1/0/14	enable	disable	down	27	0	0	48	unknown
eth1/0/15	enable	disable	down	27	0	0	48	unknown
eth1/0/16	enable	disable	down	27	0	0	48	unknown
eth1/0/17	enable	disable	down	27	0	0	48	unknown
eth1/0/18	enable	disable	down	27	0	0	48	unknown

eth1/0/19	enable	disable	down	27	0	0	48	unknown
eth1/0/20	enable	disable	down	27	0	0	48	unknown
eth1/0/21	enable	disable	down	27	0	0	48	unknown
eth1/0/22	enable	disable	down	27	0	0	48	unknown
eth1/0/23	enable	disable	down	27	0	0	48	unknown
eth1/0/24	enable	disable	down	27	0	0	48	unknown

28 RMON (REMOTE MONITORING)/ УДАЛЁННЫЙ МОНИТОРИНГ

28.1 Общая конфигурация RMON

Таблица 106 – Команды конфигурации RMON

Команда	Описание	Режим
[no] rmon statistics entry-number [owner owner-name]	Удалить/добавить записи в статистические таблицы	“(config-eth)”
[no] rmon history <entry-number> buckets <number> interval <sampling-interval> [owner <owner-name>]	Удалить/добавить записи в таблице истории	“(config-eth)”
[no] rmon alarm <entry-number> <alarm-variable> <sampling-interval> (absolute | delta) rising-threshold <threshold-value1> <event-entry1> falling-threshold <threshold-value2> <event-entry2> startup-alarm (falling | rising | risingorfalling)	Удалить/добавить записи в таблице тревог	“(config)#”
[no] rmon event <entry-number> [description <object>] (log | trap <object> | log-trap <object> | none) [owner owner-name]	Удалить/добавить записи таблицы по расписанию RMON	“(config)#”

28.2 Просмотр RMON

Таблица 107 – Команды для просмотра RMON

Команда	Описание	Режим
show rmon statistics (all | <interface-type> <interface-number>)	Показать статистическую информацию Ethernet RMON	“#”
show rmon history (all | <interface-type> <interface-number>)	Показать историческую информацию о выборке RMON	“#”
show rmon alarm (all | <entry-number>)	Отобразить информацию о конфигурации для сигналов тревоги RMON	“#”
show rmon event (all | <entry-number>)	Показать информацию о конфигурации для событий RMON	“#”
show rmon eventlog	Показать конкретную информацию, записанную в журнале событий RMON.	“#”

29 IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)/ ПРОТОКОЛ УПРАВЛЕНИЯ ИНТЕРНЕТ-ГРУППАМИ

IGMP (Internet Group Management Protocol) используется для установления и поддержания отношений членства в группах многоадресной рассылки между хостами на устройствах уровня 3 и их напрямую подключенными подсетями. В этой главе описываются концепции и конфигурации IGMP, включая:

- Версии IGMP;
- Механизм IGMP;
- Конфигурация IGMP;
- Примеры конфигурации IGMP;

29.1 Введение в IGMP

На данный момент IGMP имеет три версии:

- IGMPv1 (определен в RFC 1112).
- IGMPv2 (определен в RFC 2236).
- IGMPv3 (определен в RFC 3376).

Все версии IGMP поддерживают модель многоадресной рассылки из любого источника ASM (Any-Source Multicast). IGMPv3 может быть

непосредственно применен к модели многоадресной рассылки с учетом источника SSM (Source-Specific Multicast), тогда как IGMPv1 и IGMPv2 требуют поддержки метода сопоставления IGMP SSM, который будет применяться к модели SSM.

29.1.1 Механизм IGMPv1

IGMPv1 в основном работает на основе механизма запросов и ответов для управления членством в группах многоадресной рассылки.

Когда в подсети присутствует несколько маршрутизаторов, использующих IGMP, только одному маршрутизатору необходимо отправить сообщение запроса IGMP (Query Message), поскольку все маршрутизаторы могут получать сообщения отчета о членстве (Membership Report Messages) от хостов. Этот маршрутизатор называется запросчиком IGMP. Для определения того, какой маршрутизатор действует как запросчик IGMP, необходим механизм выбора.

Для IGMPv1 назначенный маршрутизатор DR (Designated Router), выбранный протоколами многоадресной маршрутизации, такими как PIM, служит запросчиком IGMP.

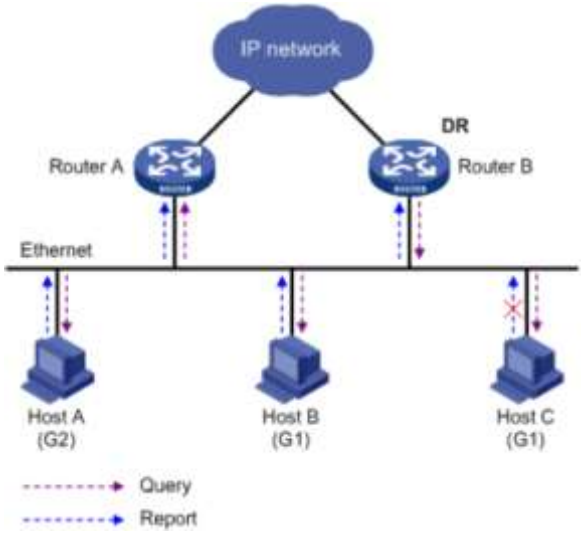

Рисунок 37 - Диаграмма ответа на запрос IGMP

Как показано на диаграмме выше, предположим, что Host B и Host C хотят получать данные многоадресной рассылки, предназначенные для группы многоадресной рассылки G1, а Host A хочет получать данные многоадресной рассылки, предназначенные для группы многоадресной

рассылки G2. Основной процесс присоединения хостов к группам многоадресной рассылки и поддержания членства в группах многоадресной рассылки запросчиком IGMP (Router B) выглядит следующим образом:

1. Хосты активно отправляют сообщения о членстве IGMP, чтобы заявить о своем намерении присоединиться к интересующей их группе многоадресной рассылки, не дожидаясь сообщений запроса IGMP от запросчика IGMP.

2. Запросчик IGMP периодически рассылает IGMP Query Messages (адрес назначения: 224.0.0.1) всем хостам и маршрутизаторам в локальной подсети.

3. После получения сообщения запроса один из хостов, заинтересованных в группе G1 (либо Host B, либо Host C, в зависимости от того, чей таймер истечет первым) - например, Host B - передает сообщение отчета о членстве IGMP для G1, чтобы объявить о своем членстве. Поскольку все хосты и маршрутизаторы в локальной подсети могут получать отчетное сообщение от Host B для G1, когда Host C получает отчетное сообщение, он не будет отправлять аналогичное отчетное сообщение для G1, поскольку маршрутизаторы IGMP (Router A и Router B) уже знают о хостах, заинтересованных в G1 в локальной подсети. Этот механизм называется механизмом подавления отчетов о членстве IGMP на узлах, который помогает уменьшить информационный трафик в локальной подсети.

4. Между тем, поскольку Host A заинтересован в G2, он продолжает рассылать многоадресные отчетные сообщения для G2, чтобы объявить о своем членстве.

5. Посредством процесса запроса и ответа, описанного выше, маршрутизаторы IGMP узнают, что в локальной подсети есть члены G1 и G2. Записи многоадресной пересылки (G1) и (G2) затем генерируются протоколами многоадресной маршрутизации (такими как PIM) в качестве основы для пересылки данных многоадресной рассылки, где “*” представляет любой источник многоадресной рассылки.

6. Когда данные многоадресной рассылки, предназначенные для G1 или G2, поступают на маршрутизатор IGMP через маршрутизацию многоадресной рассылки, маршрутизатор пересылает данные многоадресной рассылки в локальную подсеть, поскольку существуют записи пересылки многоадресной рассылки (G1) и (G2). Следовательно, хосты-получатели могут получать данные многоадресной рассылки.

IGMPv1 не определяет конкретные сообщения о выходе из группы. Когда хост, на котором работает IGMPv1, покидает группу многоадресной рассылки, он не отправляет отчетные сообщения в эту группу многоадресной рассылки. Если в подсети больше нет членов группы многоадресной рассылки, маршрутизатор IGMP не будет получать отчетные сообщения для этой группы многоадресной рассылки и впоследствии удалит запись для этой группы многоадресной рассылки через определенный период времени.

29.1.2 Механизм IGMPv2

IGMPv2, сохраняя совместимость с IGMPv1 и наследуя от него механизм работы, вводит механизмы выбора запросчика и выхода из групп многоадресной рассылки.

Механизм выборов Запросчика:

В IGMPv1, когда в подсети присутствует несколько маршрутизаторов, использующих IGMP, назначенный маршрутизатор, выбранный протоколами многоадресной маршрутизации (например, PIM), выступает в качестве запросчика. IGMPv2 добавляет отдельный механизм выбора запросчика, который работает следующим образом:

1. Первоначально все маршрутизаторы IGMPv2 считают себя запросчиками и отправляют сообщения общего запроса IGMP (адрес назначения: 224.0.0.1) всем хостам и маршрутизаторам в локальной подсети.

2. Получив это сообщение, другие маршрутизаторы IGMPv2 в локальной подсети сравнивают IP-адрес источника сообщения с адресами своих интерфейсов. Маршрутизатор с наименьшим IP-адресом становится запрашивающим, а остальные перестают запрашивать.

3. Все пользователи, не запрашивающие, запускают таймер (таймер присутствия другого запроса Other Querier Present Timer). Если до истечения

этого таймера от запрашивающего получено сообщение с запросом, таймер сбрасывается. В противном случае исходный запрос считается неудачным, инициируется новый процесс выбора запроса.

Механизм выхода из многоадресной группы:

В IGMPv1, когда хост покидает группу многоадресной рассылки, он не отправляет никаких уведомлений маршрутизаторам многоадресной рассылки. Маршрутизаторы многоадресной рассылки полагаются на тайм-аут запросов на членство, чтобы определить, когда участники покинули группу. В IGMPv2, когда хост покидает группу многоадресной рассылки:

1. Хост отправляет сообщение о выходе из группы всем многоадресным маршрутизаторам в локальной подсети (адрес назначения: 224.0.0.2).

2. После получения этого сообщения запрашивающий отправляет сообщение группового запроса в группу многоадресной рассылки, которую хост объявил о выходе (поля адреса назначения и адреса группы заполняются адресом группы для запроса).

3. Если в подсети существуют другие члены группы многоадресной рассылки, они отвечают сообщениями с отчетом о членстве в течение максимального времени ответа, указанного в сообщении запроса для конкретной группы.

4. Если сообщения с отчетом о членстве получены от других участников в течение максимального времени ответа, запрашивающая сторона продолжает поддерживать членство в группе многоадресной рассылки. В противном случае запрашивающая сторона приходит к выводу, что в подсети больше нет членов группы многоадресной рассылки, и перестает поддерживать членство в этой группе.

29.1.3 Механизм IGMPv3

IGMPv3, сохраняя совместимость и наследуя механизм работы от IGMPv1 и IGMPv2, еще больше расширяет возможности управления хостами и функциональность сообщений запросов и отчетов.

1. Расширенные возможности управления хостом:

IGMPv3 вводит режимы фильтрации (INCLUDE/EXCLUDE) для источников многоадресной рассылки, позволяя хостам явно запрашивать получение или отклонение информации многоадресной рассылки от определенных источников многоадресной рассылки при присоединении к группе многоадресной рассылки G. Когда хост присоединяется к группе многоадресной рассылки:

– Чтобы запросить получение информации многоадресной рассылки только из указанных источников многоадресной рассылки, таких как S1, S2, ..., его сообщение отчета может быть помечено как включить (INCLUDE) источники (S1, S2, ...).

– Чтобы отказаться от получения информации многоадресной рассылки от указанных источников многоадресной рассылки, таких как S1, S2, ..., его сообщение отчета может быть помечено как исключить (EXCLUDE) источники (S1, S2, ...).

Как показано на диаграмме ниже, есть два источника многоадресной рассылки, Source 1 (S1) и Source 2 (S2), оба отправляют пакеты многоадресной рассылки в группу многоадресной рассылки G. Хост B интересуется только информацией, отправленной из Source 1 в G, но не заинтересован. в информации из Source 2.

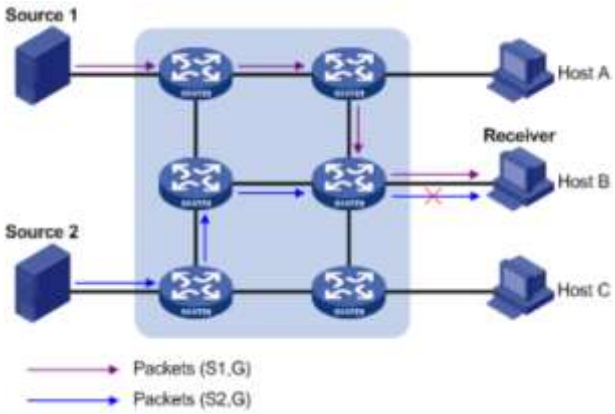

Рисунок 38 - Путь многоадресной рассылки определённого источника выглядит следующим образом

Если между хостом и маршрутизатором работает IGMPv1 или IGMPv2, Host B не может выбирать источники многоадресной рассылки при присоединении к группе многоадресной рассылки G. Следовательно, независимо от того, нужно ли это для Host B, информация многоадресной рассылки как от Source 1, так и от Source 2 будет пересылаться на Host B.

После запуска IGMPv3 между хостом и маршрутизатором Host B может запросить получение только многоадресной информации от Source 1, предназначенной для группы G (S1, G), или запросить отклонение многоадресной информации от Source 2, предназначенной для группы G (S2, G). Таким образом, на Host B будет доставляться только многоадресная информация из Source 1.

2. Расширение функциональности запросов и сообщений отчетов:

Сообщения запроса с адресом источника

IGMPv3 не только поддерживает общий групповой запрос IGMPv1 и групповой запрос IGMPv2, но также добавляет поддержку групповых запросов, с определённым источником:

– В сообщениях общего группового запроса (General Group Query) не передаются ни адрес группы, ни адрес источника.

– В сообщениях определённого группового запроса (Group-Specific Query) передается адрес группы, но адрес источника не передается.

– В сообщениях группового запроса с определённым источником (Source-Specific Group Query), передаются как адрес группы, так и один или несколько адресов источника.

Сообщения отчёта с несколькими групповыми записями

Адрес назначения сообщений отчетов IGMPv3 — 224.0.0.22, и они могут содержать одну или несколько групповых записей. Каждая групповая запись содержит адрес группы многоадресной рассылки и список адресов источников многоадресной рассылки. Групповые записи могут быть разных типов, в том числе:

IS_IN： указывает, что режим фильтрации между группой многоадресной рассылки и списком источников многоадресной рассылки — INCLUDE, что означает, что принимаются только данные многоадресной рассылки, отправленные из указанного списка источников многоадресной рассылки в группу многоадресной рассылки.

IS_EX： указывает, что режим фильтрации между группой многоадресной рассылки и списком источников многоадресной рассылки - EXCLUDE, что означает, что принимаются только данные многоадресной рассылки, отправленные из источников за пределами указанного списка источников многоадресной рассылки в группу многоадресной рассылки.

TO_IN： указывает на переход из режима фильтрации EXCLUDE в режим фильтрации INCLUDE между группой многоадресной рассылки и списком источников многоадресной рассылки.

TO_EX： указывает на переход из режима фильтрации INCLUDE в режим фильтрации EXCLUDE между группой многоадресной рассылки и списком источников многоадресной рассылки.

ALLOW： указывает на желание получать данные многоадресной рассылки от определенных источников многоадресной рассылки в дополнение к существующему состоянию. Если текущая связь — INCLUDE, эти источники многоадресной рассылки добавляются в существующий список источников многоадресной рассылки; если текущая связь — EXCLUDE, эти источники многоадресной рассылки удаляются из существующего списка источников многоадресной рассылки.

BLOC： указывает на желание прекратить получение многоадресных данных от определенных источников многоадресной рассылки в дополнение к существующему состоянию. Если текущая связь — INCLUDE, эти источники многоадресной рассылки удаляются из существующего списка источников многоадресной рассылки; если текущая связь — EXCLUDE, эти

источники многоадресной рассылки добавляются в существующий список источников многоадресной рассылки.

29.2 Настройка IGMP

29.2.1 Общая конфигурация IGMP

Таблица 108 – Команды общей конфигурации IGMP

Команда	Описание	Режим
[no] multicast route-enable	Отключить/включить функцию многоадресной маршрутизации	“(config)#”
[no] igmp enable	Отключить/включить функцию IGMP	«(Vlan-interface)#”
multicast unknown route (forward | tocpu)	Обрабатывать многоадресные сообщения неизвестной маршрутизации	“(config)#”
[no] igmp query-interval <time>	Интервал сообщений с запросом на восстановление/конфигурацию	“(config)#”
[no] igmp querier-timeout <time>	Тайм-аут ответа на восстановление/конфигурацию	“(config)#”
igmp (igmpv2 | igmpv3)	Функция переключения версии IGMP	«(Vlan-interface)#”

25.2.2 Показать IGMP

Таблица 109 – Команды просмотра IGMP

Команда	Описание	Режим
show multicast route	Показать конфигурацию многоадресной маршрутизации	“#”
show multicast routing-table	Показать таблицу маршрутизации многоадресной пересылки	“#”
show igmp info	Показать информацию о конфигурации IGMP	“#”
show igmp group	Показать информацию о статусе IGMP	“#”
show multicast rpf-info <src-ip-address>	Показать проверку адреса источника RPF	“#”

30 PIM (PROTOCOL INDEPENDENT MULTICAST)/ МНОГОАДРЕСНАЯ РАССЫЛКА

PIM, что означает “Protocol Independent Multicast”, представляет собой независимую от протокола многоадресную рассылку. В этой главе описывается концепция и конфигурация PIM-SM в PIM:

- Введение в PIM;
- Введение в PIM-SM;
- Механизм протокола PIM-SM;
- Принципы работы;
- Конфигурация PIM-SM;
- Примеры конфигурации PIM-SM.

30.1 Введение в PIM

PIM (Protocol Independent Multicast) многоадресная рассылка, независимая от протокола, которая обеспечивает маршрутизацию для многоадресной рассылки IP с использованием протоколов одноадресной маршрутизации, таких как статические маршруты, RIP, OSPF, IS-IS, BGP и т. д. Многоадресная маршрутизация не зависит от протоколов одноадресной маршрутизации; пока протокол одноадресной рассылки может генерировать записи таблицы маршрутизации, его можно использовать.

Номер протокола: 103

Адрес многоадресной рассылки для маршрутизаторов PIM: 224.0.0.13.

Протокол PIM делится на:

- PIM-DM (Protocol Independent Multicast - Dense Mode);
- PIM-SM (Protocol Independent Multicast - Sparse Mode).

30.2 Введение в PIM-SM

PIM-SM также известный как многоадресная рассылка, независимая от протокола, Sparse режим, представляет собой протокол многоадресной маршрутизации с разреженным режимом, который в основном используется в сетях, где члены группы широко рассредоточены и область действия обширна.

– Допущения протокола: когда источник многоадресной рассылки начинает отправлять данные многоадресной рассылки, никакие сетевые узлы в домене не должны их получать.

— Основным компонентом модели многоадресной пересылки PIM-SM является построение и обслуживание однонаправленного общего дерева. Общее дерево выбирает маршрутизатор в PIM в качестве корневого узла, известного как точка встречи RP (Rendezvous Point). Многоадресные данные пересылаются получателям по общему дереву через RP.

-Получатели обнаруживают и выбирают Designated Router (DR), который создает записи (*,G) и отправляет сообщения о присоединении к RP.

— Аналогично, источники многоадресной рассылки выбирают DR и регистрируют информацию об источнике на RP через DR.

— PIM-SM включает два типа деревьев: общее дерево (Shared tree) и исходное дерево (Source tree).

Source tree — отдельное дерево строится от каждого источника ко всем получателям.

Shared tree — создаются пути передачи трафика, которые основаны на центральном маршрутизаторе, который работает rendezvous point (RP) между источниками multicast и получателями.

— PIM-SM не зависит от конкретного протокола одноадресной маршрутизации, а скорее использует существующие таблицы одноадресной маршрутизации для проверок RPF (Reverse Path Forwarding).

— RPF-проверки проводятся в зависимости от типа дерева:

Для общего дерева адрес RP используется в качестве контрольного адреса.

Для исходного дерева адрес источника многоадресной рассылки используется в качестве проверочного адреса.

30.3 Механизм протокола PIM-SM

26.3.1 DR Election

После инициализации многоадресные маршрутизаторы используют приветственную сообщения для обнаружения соседей и поддержания отношений между ними. Приветственные сообещния используются для выбора назначенного маршрутизатора (DR) для общих сетей (например, Ethernet), который будет служить единственным передатчиком многоадресной информации в подсети. Будь то сеть, подключенная к источникам

многоадресной рассылки или сеть, подключенная к получателям, если сеть является общей средой, необходимо выбрать DR.

DR на стороне получателя отправляет сообщения Join до RP для присоединения к группе.

DR на стороне источника многоадресной рассылки отправляет сообщения Register до RP для регистрации.

30.3.1 RP Election

В сетях многоадресной рассылки PIM-SM узел, служащий корнем общего дерева, называется Rendezvous Point (RP). Все потоки многоадресной рассылки в общем дереве пересылаются получателям через RP, который может обрабатывать пересылку для нескольких или всех групп многоадресной рассылки. Таким образом, в сети может быть один или несколько RP.

Обнаружение RP:

Маршрутизаторы в домене, включая DR и известные маршрутизаторы, используют вручную заданные IP-адреса RP и протокол начальной загрузки (bootstrap) для динамического выбора RP с помощью механизма bootstrap.

Выбор BSR:

После инициализации сети PIM-SM загрузочный маршрутизатор BSR (Bootstrap Router) отвечает за сбор информации о RP в сети, выбор RP для каждой группы многоадресной рассылки, а затем распространение настроек RP (т. е. базы данных сопоставления групп-RP) по маршрутизаторам по всей сети PIM-SM. Домен PIM-SM имеет только один BSR и может одновременно иметь несколько маршрутизаторов-кандидатов начальной загрузки C-BSR (Candidate Bootstrap Routers).

Если в домене есть только один C-BSR, этот маршрутизатор становится BSR для домена.

Если в домене несколько C-BSR, BSR становится маршрутизатор с наивысшим приоритетом.

Если существует несколько C-BSR с одинаковым приоритетом, маршрутизатор с наивысшим IP-адресом становится BSR.

Выбор RP:

Если в домене PIM-SM есть только один кандидат-RP (C-RP), этот узел становится RP для домена.

Если существует несколько C-RP с разными приоритетами, в качестве RP для домена выбирается тот, у которого самый высокий приоритет (более низкое значение приоритета).

Если существует несколько C-RP с одинаковым приоритетом, RP определяется с использованием алгоритма хэширования на основе таких параметров, как групповой адрес, длина маски и адрес C-RP. Тот, у кого наибольшее значение хеш-функции, становится RP.

Если существует несколько C-RP с одинаковым приоритетом и значением хеш-функции, RP для домена становится тот, у которого самый высокий IP-адрес.

30.3.2 RP-BSR

— Candidate Rendezvous Points (C-RPs) отправляют объявления на Bootstrap Router (BSR).

C-RP периодически отправляют объявления через одноадресную рассылку (каждые 60 секунд).

BSR хранит все объявления C-RP в RP-set.

— BSR периодически отправляет сообщения Bootstrap Router (BSR) всем маршрутизаторам PIM (224.0.0.13).

Сообщения BSR содержат весь RP-set и адрес BSR.

Сообщение шаг за шагом рассылается из BSR по всей сети.

— Все маршрутизаторы используют полученный RP-set для определения RP.

Все маршрутизаторы используют один и тот же алгоритм выбора RP, что обеспечивает согласованный выбор RP.

30.4 Принципы работы

30.4.1 Регистрация источника многоадресной рассылки

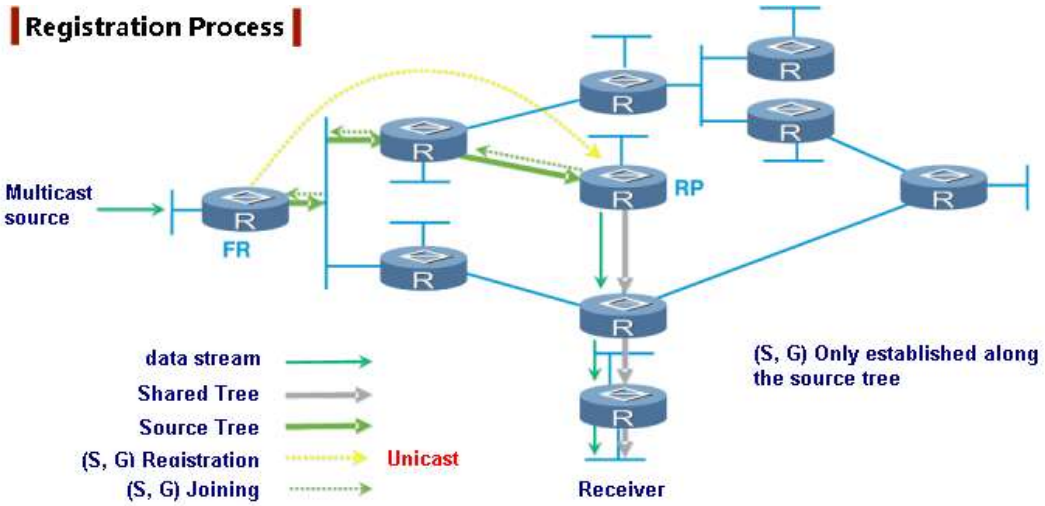

Рисунок 39 – Процесс регистрации источника многоадресной рассылки

1) Источник отправляет многоадресный трафик на первый маршрутизатор (R1).

2) R1 инкапсулирует пакеты многоадресной рассылки, полученные от источника, в register пакеты одноадресной рассылки и отправляет их RP. Адресом назначения этих пакетов является RP, а адрес многоадресной рассылки также включен в одноадресный пакет. Инкапсулированное сообщение может выглядеть так: “Отправьте регистрацию v2 на адрес 44.1.1.1 для 18.1.1.8, группа 224.1.1.1”. R1 регистрирует эту информацию с помощью RP, устанавливая флаг “F”, чтобы указать, что он напрямую подключен к источнику, а также устанавливая флаг «registering», чтобы указать, что он находится в процессе регистрации.

3) Получив пакет регистрации от R1, R4-RP предпринимает следующие действия:

1. Он декапсулирует пакет и пересылает его по общему дереву.

2. Он генерирует запись (S,G) и устанавливает проверку RPT так, чтобы она указывала на источник.

3. Он инициирует соединение (S,G) с источником.

4) R2 создает исходное дерево (S,G) и инициирует соединение (S,G) с R1. В конце концов, и R1, и R2 образуют исходное дерево (S,G) по направлению к RP.

30.4.2 Прекращение регистрации

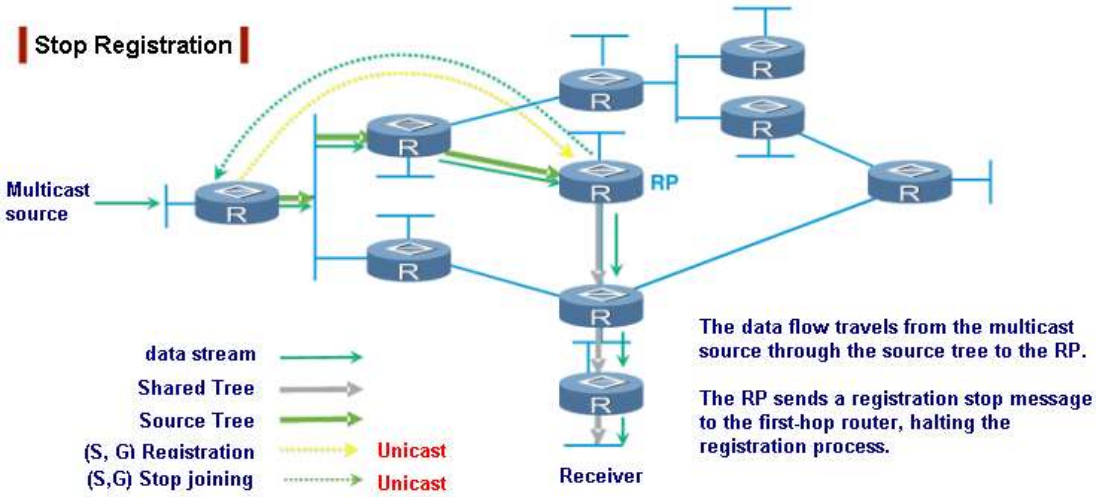

Рисунок 40 – Процесс прекращения регистрации

1) После формирования исходного дерева (S,G), когда R1 получает еще один многоадресный пакет:

1. Он пересылает многоадресный пакет по дереву источников (S,G).

2. Кроме того, он прекращает регистрацию, не инкапсулируя и не пересылая дальнейшие пакеты одноадресной регистрации.

2) Когда RP получает многоадресный пакет от (S,G), он отправляет пакет остановки регистрации на маршрутизатор первого перехода.

30.4.3 Процесс пересылки многоадресного потока

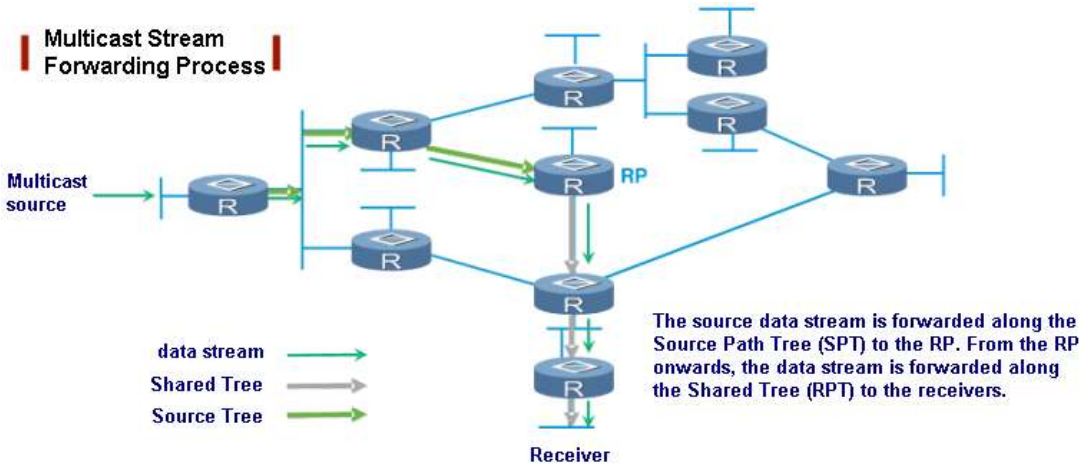

Рисунок 41 – Процесс пересылки многоадресного потока

1) После получения пакета остановки регистрации R1 прекращает одноадресную передачу пакетов регистрации.

2) Последний маршрутизатор переключается на исходное дерево и отправляет источнику сообщение о присоединении (S,G).

30.4.4 Переключение с RPT на SPT

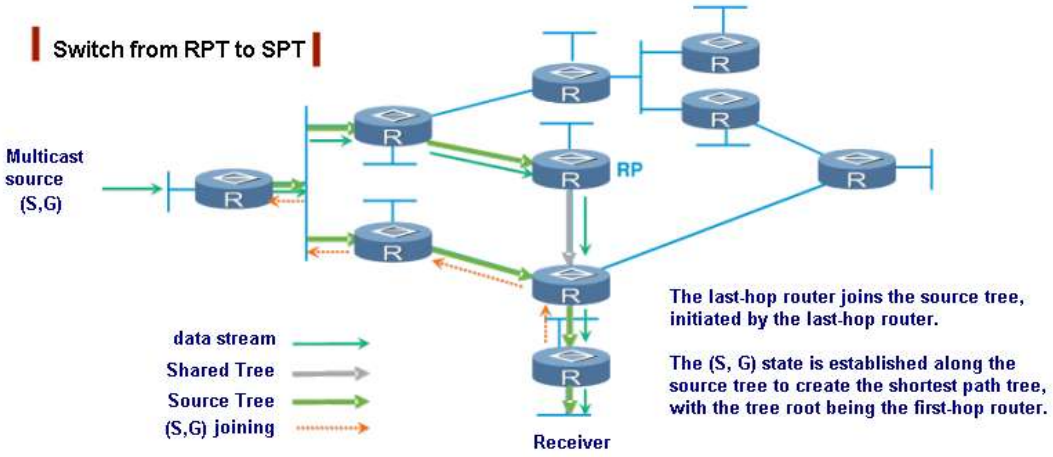

Рисунок 42 - Переключение с RPT на SPT (1)

Присоединившись к SPT (shortest path tree), информация многоадресной рассылки может быть направлена непосредственно получателю без необходимости прохождения через RP, тем самым уменьшая задержку сети и потенциальную перегрузку на RP. Это устраняет ограничение на получение многоадресной информации исключительно через общее дерево.

После получения некоторых пакетов данных, исходящих от S по RPT, маршрутизатор последнего перехода решает инициировать SPT-соединение с источником, чтобы установить дерево кратчайшего пути (SPT) с корнем в S. Пока состояние восходящего SPT полностью установлено, Маршрутизатор последнего перехода продолжает получать пакеты многоадресных данных от RPT. Когда пакеты многоадресных данных, исходящие от S, достигают маршрутизатора последнего перехода по дереву SPT, маршрутизатор знает, что восходящий SPT полностью установлен. Однако потеря пакетов может произойти во время процесса переключения.

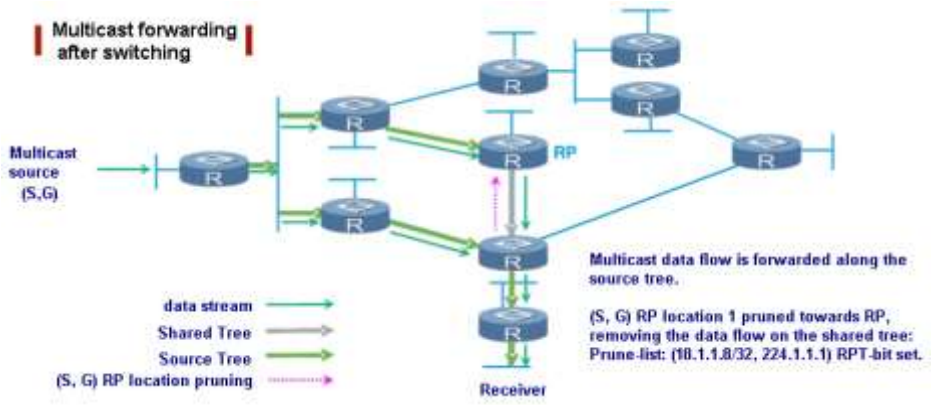

Рисунок 43 – Переключение с RPT на SPT (2)

После переключения на дерево SPT информация многоадресной рассылки будет напрямую отправляться из источника S многоадресной рассылки получателям. Путем перехода от дерева RPT к дереву SPT PIM-SM может создать дерево пересылки SPT более эффективным способом по сравнению с PIM-DM.

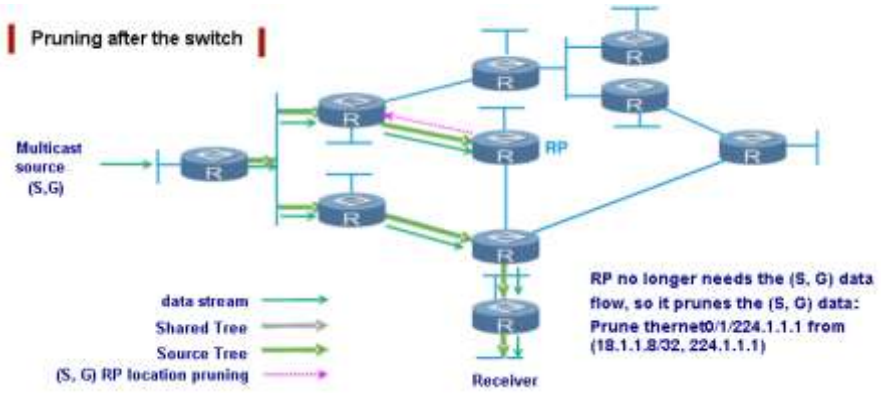

Рисунок 44 – Обрезка после переключения (1)

Маршрутизатор последнего перехода намеревается отправлять сообщения об обрезке (prune), содержащие информацию о RP, шаг за шагом к RP. После получения информации RP пересылает Prune сообщения в обратном порядке к источнику многоадресной рассылки, тем самым в конечном итоге обеспечивая переход потока многоадресной информации из дерева RPT в дерево SPT.

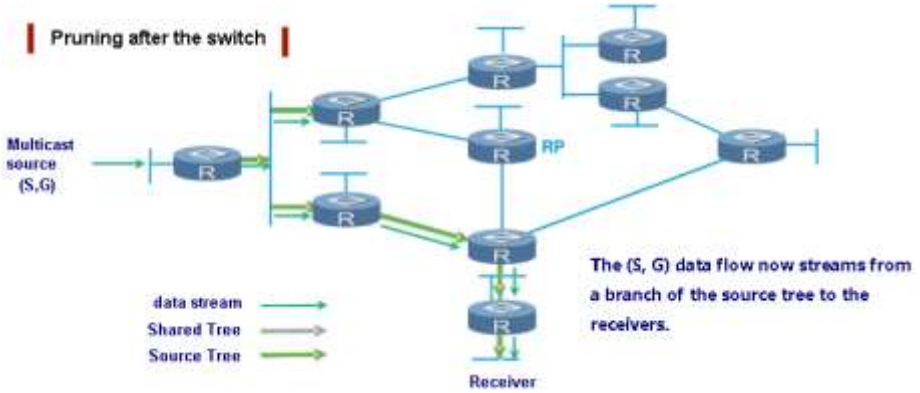

Рисунок 45 – Обрезка после переключения (2)

Когда пропускная способность информации превышает заданный порог, PIM-SM перейдет от общего дерева к пути исходного дерева.

По умолчанию маршрутизаторы, соединяющие получателей (маршрутизаторы последнего перехода), присоединяются к дереву кратчайшего пути (SPT) сразу после обнаружения источника многоадресной рассылки, то есть после получения первого пакета данных, переключаясь таким образом с RPT на SPT.

30.5 Настройка PIM

30.5.1 Общая конфигурация PIM

Таблица 110 – команды конфигурации PIM

Команда	Описание	Режим
[no] pim sm	Отключить/включить функцию PIM	“(config)#”
[no] pim dr-priority <dr-priority>	Восстановить/настроить приоритет выбора DR порта	«(Vlan-interface)#”
[no] pim hello-interval <hello-interval>	Интервал отправки приветственного сообщения	“(config)#”

30.5.2 Конфигурация RP

Таблица 111 – Команды конфигурации RP

Команда	Описание	Режим
[no] pim rp-candidate	Отключить/включить кандидатов RP	“(config)#”
[no] pim static-rp <rp-addr> (<ip-address>/<mask-len> | all)	Удалить/создать определённый статический RP	“(config)#”
pim rp-candidate priority <priority>	Настроить приоритет кандидата RP	“(config)#”
pim rp-candidate interval <time>	Настроить временный интервал кандидата RP	“(config)#”
[no] pim rp-candidate group-prefix <ip-address>/<mask-len>	Удалить/создать конфигурацию области многоадресной рассылки RP	“(config)#”
clear pim rp-candidate group-prefix	Очистить конфигурацию диапазона многоадресной рассылки RP	“(config)#”

30.5.3 Конфигурация BSR

Таблица 112 – команды конфигурации BSR

Команда	Описание	Режим
[no] pim bsr-candidate	Отключить/включить функцию кандидата BSR	“(config)#”
pim bsr-candidate priority <priority>	Настроить приоритет кандидата BSR	“(config)#”

30.5.4 Конфигурация пути маршрутизации

Таблица 113 - Конфигурация пути маршрутизации

Команда	Описание	Режим
[no] pim default route-distance <route-distance>	Восстановить/настроить путь маршрутизации по умолчанию	“(config)#”
[no] pim distance <distance>	Восстановить/настроить путь маршрутизации PIM	«(Vlan-interface)#”

30.5.5 Конфигурация затрат на маршрутизацию

Таблица 114 - Конфигурация затрат на маршрутизацию

Команда	Описание	Режим
[no] pim default route-metric <route-metric>	Восстановить/настроить издержеки маршрутизации по умолчанию	“(config)#”
[no] pim metric <metric>	Затраты на восстановление/конфигурацию PIM	«(Vlan-interface)#”

30.5.6 Конфигурация области многоадресной рассылки

Таблица 115 - Конфигурация области многоадресной рассылки

Команда	Описание	Режим
[no] pim boundary <ip-address>/<mask-len>	Отменить/настроить ограничение области многоадресной рассылки	“(config)#”

30.5.7 Показать PIM

Таблица 116 – Просмотр PIM

Команда	Описание	Режим
show pim info	Показать информацию о конфигурации PIM	“#”
show pim rp-candidate group-prefix	Показать конфигурацию диапазона многоадресной рассылки RP	“#”
show pim status	Показать информацию о статусе PIM	“#”
show pim rp-info	Показать информацию о RP	“#”
show pim rp-info <gourp-address>	Поиск RP по многоадресной группе	“#”
show pim bsr-info	Показать информацию BSR	“#”
show pim neighbor	Показать информацию о соседях	“#”
show pim routing-table	Показать информацию о многоадресной маршрутизации	“#”

30.6 Пример настройки

30.6.1 Критерий задач конфигурации

Таблица 117 - Критерий задач конфигурации

Критерий задач конфигурации	Описание
Включить функцию многоадресной маршрутизации	Необходимый
Активировать функцию IGMP	Необходимый
Включить функцию PIM	Необходимый
Включить кандидатов RP/создать определённые статические RP	Требуется (или-или)
Включить функцию кандидата BSR	Необязательный
Приоритет выборов порта DR	Эта конфигурация вступает в силу только тогда, когда включен кандидат RP.
Конфигурация таймера	Необязательный
Атрибуты, связанные с RP	Необязательный
Атрибуты, связанные с BSR	Необязательный
Путь маршрутизации/стоимость	Необязательный
Область многоадресной рассылки	Необязательный

30.6.2 Пример настройки

1. Требования к сети

— Router1, Router2 и Router3 динамически изучают и поддерживают маршрутизацию через OSPF.

— Одноадресная маршрутизация — это нормально.

— Host1 - Host4 может получать пакеты данных из источников многоадресной рассылки посредством многоадресной рассылки.

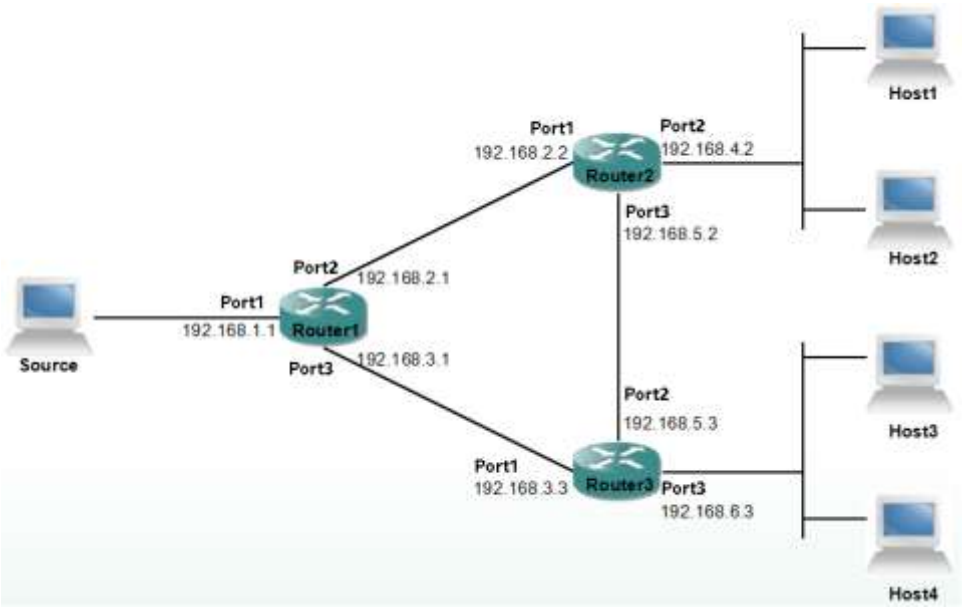

Рисунок 46 - Схема топологии сети

2. План настройки

— Настроить виртуальные интерфейсы и включить OSPF для Router1, Router2 и Router3, а также объявить сеть.

— Включить функцию многоадресной маршрутизации и IGMP

— Включить PIM и настройте статический RP.

3. Шаги настройки

（1）Настроить виртуальные интерфейсы и OSPF.

Настройка Router1

Router1(config)# vlan 2-3

Router1(config)# interface ethernet 1/0/2

Router1(config-eth1/0/2)# switchport access 2

Router1(config-eth1/0/2)#interface ethernet 1/0/3

Router1(config-eth1/0/3)# switchport access 3

Router1(config-eth1/0/3)# exit

Router1(config)# interface vlan-interface 1

Router1(Vlan-interface1)# ip address 192.168.1.1 255.255.255.0

Router1(Vlan-interface1)# interface vlan-interface 2

Router1(Vlan-interface2)# ip address 192.168.2.1 255.255.255.0

Router1(Vlan-interface2)# interface vlan-interface 3

Router1(Vlan-interface3)# ip address 192.168.3.1 255.255.255.0

Router1(Vlan-interface3)# exit

```
Router1(config)# router ospf
Router1(ospf-router)# network 192.168.1.0/24 area 0
Router1(ospf-router)# network 192.168.2.0/24 area 0
Router1(ospf-router)# network 192.168.3.0/24 area 0
# Настройка Router2
Router2(config)# vlan 2-3
Router2(config)# interface ethernet 1/0/2
Router2(config-eth1/0/2)# switchport access 2
Router2(config-eth1/0/2)#interface ethernet 1/0/3
Router2(config-eth1/0/3)# switchport access 3
Router2(config-eth1/0/3)# exit
Router2(config)# interface vlan-interface 1
Router2(Vlan-interface1)# ip address 192.168.2.2 255.255.255.0
Router2(Vlan-interface1)# interface vlan-interface 2
Router2(Vlan-interface2)# ip address 192.168.4.2 255.255.255.0
Router2(Vlan-interface2)# interface vlan-interface 3
Router2(Vlan-interface3)# ip address 192.168.5.2 255.255.255.0
Router2(Vlan-interface3)# exit
Router2(config)# router ospf
Router2(ospf-router)# network 192.168.2.0/24 area 0
Router2(ospf-router)# network 192.168.4.0/24 area 0
Router2(ospf-router)# network 192.168.5.0/24 area 0
# Настройка Router3
Router3(config)# vlan 2-3
Router3(config)# interface ethernet 1/0/2
Router3(config-eth1/0/2)# switchport access 2
Router3(config-eth1/0/2)#interface ethernet 1/0/3
Router3(config-eth1/0/3)# switchport access 3
Router3(config-eth1/0/3)# exit
Router3(config)# interface vlan-interface 1
Router3(Vlan-interface1)# ip address 192.168.3.3 255.255.255.0
Router3(Vlan-interface1)# interface vlan-interface 2
Router3(Vlan-interface2)# ip address 192.168.5.3 255.255.255.0
Router3(Vlan-interface2)# interface vlan-interface 3
Router3(Vlan-interface3)# ip address 192.168.6.3 255.255.255.0
Router3(Vlan-interface3)# exit
```

Router3(config)# router ospf
Router3(ospf-router)# network 192.168.3.0/24 area 0
Router3(ospf-router)# network 192.168.5.0/24 area 0
Router3(ospf-router)# network 192.168.6.0/24 area 0

（2）Настроить многоадресную маршрутизацию и IGMP.

Настройка Router1
Router1(config)# multicast route-enable
Router1(config)# interface vlan-interface 1
Router1(Vlan-interface1)# igmp enable
Router1(Vlan-interface1)# interface vlan-interface 2
Router1(Vlan-interface2)# igmp enable
Router1(Vlan-interface2)# interface vlan-interface 3
Router1(Vlan-interface3)# igmp enable
Настройка Router2
Router2(config)# multicast route-enable
Router2(config)# interface vlan-interface 1
Router2(Vlan-interface1)# igmp enable
SWITCH(Vlan-interface1)# interface vlan-interface 2
Router2(Vlan-interface2)# igmp enable
Router2(Vlan-interface2)# interface vlan-interface 3
Router2(Vlan-interface3)# igmp enable
Настройка Router3
Router3(config)# multicast route-enable
Router3(config)# interface vlan-interface 1
Router3(Vlan-interface1)# igmp enable
Router3(Vlan-interface1)# interface vlan-interface 2
Router3(Vlan-interface2)# igmp enable
Router3(Vlan-interface2)# interface vlan-interface 3
Router3(Vlan-interface3)# igmp enable

（3）Включить PIM и настроить статический RP.

Настройка Router1
Router1(config)# interface vlan-interface 1
Router1(Vlan-interface1)# pim sm
Router1(Vlan-interface1)# interface vlan-interface 2

```
Router1(Vlan-interface1)# pim sm
Router1(Vlan-interface2)# interface vlan-interface 3
Router1(Vlan-interface3)# pim sm
Router1(Vlan-interface3)# exit
Router1(config)# pim static-rp 192.168.2.2 all
# Настройка Router2
Router2(config)# interface vlan-interface 1
Router2(Vlan-interface1)# pim sm
Router2(Vlan-interface1)# interface vlan-interface 2
Router2(Vlan-interface1)# pim sm
Router2(Vlan-interface2)# interface vlan-interface 3
Router2(Vlan-interface3)# pim sm
Router2(Vlan-interface3)# exit
Router2(config)# pim static-rp 192.168.2.2 all
# Настройка Router3
Router3(config)# interface vlan-interface 1
Router3(Vlan-interface1)# pim sm
Router3(Vlan-interface1)# interface vlan-interface 2
Router3(Vlan-interface1)# pim sm
Router3(Vlan-interface2)# interface vlan-interface 3
Router3(Vlan-interface3)# pim sm
Router3(Vlan-interface3)# exit
Router3(config)# pim static-rp 192.168.2.2 all
```

4. Проверка конфигурации

（1）После настройки, как описано выше, проверка конфигурации показывает, что Router1, Router2 и Router3 установили отношения соседства PIM друг с другом попарно.

```
# Просмотр информацию о соседях PIM на Router1
Router1(config)# show pim neighbor
Neighbor's Address  Interface Name   Uptime
------------------  ---------------  ------
192.168.2.2         VlanIf2          75
192.168.3.3         VlanIf3          105
# Просмотр информации о соседях PIM на Router2
Router2(config)# show pim neighbor
```

```
Neighbor's Address  Interface Name   Uptime
------------------  --------------  ------
192.168.2.1         VlanIf1         90
192.168.5.3         VlanIf3         105
```

Просмотр информации о соседях PIM на Router3

```
Router3# show pim neighbor
Neighbor's Address  Interface Name   Uptime
------------------  --------------  ------
192.168.3.1         VlanIf1         95
192.168.5.2         VlanIf2         80
```

Просмотр RP информации в PIM SM domain

Просмотр информации о соседях x PIM на Router1

```
Router1(config)# show pim rp-info 225.0.0.1
RP Address: 192.168.3.1
```

Просмотр информации о соседях PIM на Router2

```
Router2(config)# show pim rp-info 225.0.0.1
RP Address: 192.168.3.1
```

Просмотр информации о соседях PIM на Router3

```
Router3(config)# show pim rp-info 225.0.0.1
RP Address: 192.168.3.1
```

Посмотреть информацию таблицы маршрутизации PIM коммутатора.

Host1 отправил сообщение о присоединении к многоадресной группе 225.0.0.1, в котором показаны конкретные записи таблицы (S, G), общее количество записей таблицы (*, G) и (S, G), а также информация о входящих и исходящих интерфейсы

Просмотр информации о соседях PIM на Router1

```
Router1(config)# show pim routing-table
    Group        Source      Type     UpLink     DownLinks
  225.0.0.1  INADDR_ANY      (*,G)       NA     VlanIf3,
  225.0.0.1      192.168.4.101       (S,G)       NA
  225.0.0.1      192.168.1.101       (S,G)    VlanIf1    VlanIf2, VlanIf3,
```

Просмотр информации о соседях PIM на Router2

```
Router2(config)# show pim routing-table
   Group      Source       Type       UpLink     DownLinks
```

```
225.0.0.1    INADDR_ANY      (*,G)    VlanIf3     VlanIf2,
    225.0.0.1 192.168.4.101      (S,G) VlanIf2
    225.0.0.1      192.168.1.101      (S,G) VlanIf1     VlanIf2,
# Просмотр информации о соседях PIM на Router3
Router3(config)# show pim routing-table
 Group    Source       Type      UpLink     DownLinks
  225.0.0.1    INADDR_ANY  (*,G)    VlanIf1     VlanIf2,
    225.0.0.1   192.168.4.101      (S,G)    VlanIf1
```

31 VRRP (VIRTUAL ROUTER REDUNDANCY PROTOCOL)/ ПРОТОКОЛ РЕЗЕРВИРОВАНИЯ ВИРТУАЛЬНОГО МАРШРУТИЗАТОРА

Протокол резервирования виртуального маршрутизатора VRRP (Virtual Router Redundancy Protocol), представляет собой протокол маршрутизации, предложенный IETF для решения проблемы единой точки отказа при настройке статических шлюзов в локальных сетях. VRRP широко используется в периферийных сетях, и цель его разработки — обеспечить аварийное переключение IP-трафика данных в определенных сценариях, не вызывая сбоев. Это позволяет хостам использовать один маршрутизатор и обеспечивает поддержание соединения между маршрутизаторами даже в тех случаях, когда фактический маршрутизатор первого перехода (first-hop) выходит из строя.

- Введение в VRRP;
- Механизм VRRP;
- Настройка VRRP;
- Пример настройки VRRP.

31.1 Введение в VRRP

VRRP — это протокол выбора, который динамически распределяет ответственность виртуального маршрутизатора между VRRP-маршрутизаторами в локальной сети. Маршрутизатор VRRP, управляющий IP-адресом виртуального маршрутизатора, называется главным маршрутизатором и отвечает за пересылку пакетов на эти виртуальные IP-

адреса. Когда главный маршрутизатор становится недоступным, этот процесс выбора обеспечивает механизм динамического переключения при сбое, позволяя IP-адресу виртуального маршрутизатора служить маршрутизатором первого перехода по умолчанию для конечных хостов. Это протокол резервирования устройства доступа к локальной сети. Все узлы в локальной сети устанавливают шлюз по умолчанию, поэтому пакеты с адресами назначения, не принадлежащими локальной подсети, отправленные узлами, пересылаются на коммутатор уровня 3 через шлюз по умолчанию, тем самым обеспечивая связь между узлами и внешними сетями.

VRRP — это протокол отказоустойчивости маршрутизации, также известный как протокол резервирования маршрутизации. Все узлы в локальной сети устанавливают маршрут по умолчанию. Когда узел в сети отправляет пакеты с адресами назначения, находящимися за пределами локальной подсети, пакеты пересылаются на внешние маршрутизаторы по маршруту по умолчанию, обеспечивая связь между узлами и внешними сетями. Когда маршрутизатор по умолчанию выходит из строя, внутренние хосты не смогут взаимодействовать с внешними сетями. Если на маршрутизаторах настроен VRRP, виртуальный маршрутизатор активирует резервный маршрутизатор, тем самым обеспечивая полную сетевую связь.

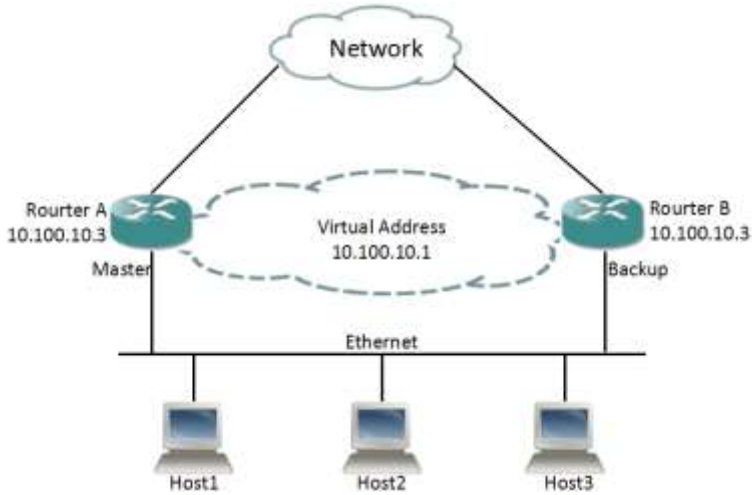

Рисунок 47 – Процесс отказоустойчивой маршрутизации

31.1.1 27.1.1 Механизм работы

1. После включения функции VRRP маршрутизаторы определяют свои роли в резервной группе на основе приоритета. Маршрутизатор с наивысшим приоритетом становится главным маршрутизатором, а маршрутизатор с более низким приоритетом становится резервным маршрутизатором. Главный

маршрутизатор периодически отправляет сообщения объявления (advertisement) VRRP, чтобы уведомить другие маршрутизаторы в резервной группе о том, что он работает правильно, в то время как резервный маршрутизатор запускает таймер и ожидает сообщений объявлений.

2. В зависимости от режима вытеснения (preemption mode) VRRP механизм замены главной роли различается:

— В режиме вытеснения, когда главный маршрутизатор получает сообщение объявление VRRP, он сравнивает свой приоритет с приоритетом в сообщении объявлении. Если его приоритет выше приоритета в сообщении, он становится главным маршрутизатором; в противном случае он остается в резервном состоянии.

— В режиме без вытеснения, пока главный маршрутизатор не выходит из строя, маршрутизаторы в резервной группе всегда сохраняют свои главные или резервные роли. Даже если маршрутизатору в резервной группе впоследствии будет присвоен более высокий приоритет, он не станет главным маршрутизатором.

3. Если таймер резервного маршрутизатора истекает без получения сообщений объявлений VRRP от главного маршрутизатора, предполагается, что главный маршрутизатор больше не работает должным образом. На этом этапе резервный маршрутизатор считает себя главным маршрутизатором и отправляет сообщения объявления VRRP наружу. Маршрутизаторы в резервной группе выбирают главный маршрутизатор на основе приоритета и берут на себя ответственность за пересылку пакетов.

31.1.2 Балансировка нагрузки

В реальных сетевых конфигурациях часто используется балансировка нагрузки VRRP. Балансировка нагрузки подразумевает одновременную работу нескольких маршрутизаторов для распределения рабочей нагрузки и предотвращения простоя устройств. Поэтому необходимо создать две или более группы резервного копирования для достижения балансировки нагрузки. Балансировка нагрузки VRRP имеет следующие характеристики:

— Каждая резервная группа состоит из одного главного маршрутизатора и нескольких резервных маршрутизаторов.

— Главные маршрутизаторы разных резервных групп могут различаться.

— Один и тот же маршрутизатор может присоединяться к нескольким резервным группам с разными приоритетами, что позволяет маршрутизатору выступать в качестве главного маршрутизатора в одной резервной группе и в качестве резервного маршрутизатора в других.

31.2 Настройка VRRP

31.2.1 Общая конфигурация VRRP

Таблица 118 - Общая конфигурация VRRP

Команда	Описание	Режим
vrrp [enable | disable]	Включить/выключить функцию VRRP	“(config)#”
vrrp method [real-mac | virtual-mac]	Настроить, использовать ли виртуальный MAC	“(config)#”
vrrp dscp <dscp-value>	Настроить dscp для сообщений VRRP	“(config)#”
[no] vrrp virtual-ip ping enable	Настроить, принимает ли виртуальный IP-адрес пакеты ICMP	“(config)#”
[no] vrrp trap enable [authfailure | newmaster]	Настроить функцию trap VRRP	“(config)#”
[no] vrrp gratuitous-arp timeout <interval>	VRRP синхронизированная отправка gratuitous-arp	“(config)#”
vrrp gratuitous-arp timeout disable	Отключить функцию запланированной gratuitous-arp	“(config)#”
[no] vrrp un-check ttl	Настроить функцию проверки TTL	“(config)#”
track <track-num> interface <interface-type> <interface-number>	Функция отслеживания статуса порта	“(config)#”
[no] track <track-num> ip route <ip-address> <mask>	Удалить/добавить таблицу маршрутизации функцию отслеживания следующего перехода	“(config)#”
[no] vrrp bind vrid <virtual-router-id>	Отменить/привязать vrrp	«(Vlan-interface)#”
[no] vrrp vrid <virtual-router-id> virtual-ip <virtual-address>	Отменить/настроить виртуальный IP-адрес	«(Vlan-interface)#”
[no] vrrp vrid <virtual-router-id> priority <priority-value>	Восстановить/настроить приоритет VRRP	«(Vlan-interface)#”
[no] vrrp vrid <virtual-router-id> preempt-mode [timer delay <delay-value>]	Восстановить/настроить режим VRRP	«(Vlan-interface)#”
[no] vrrp vrid <virtual-router-id> track <track-num> reduced <priority-reduced>	Восстановить/настроить мониторинг портов	«(Vlan-interface)#”
vrrp vrid <virtual-router-id> authentication-mode {md5 | simple | none} [cipher] <key>	Настроить режим аутентификации	«(Vlan-interface)#”

[no] vrrp vrid <virtual-router-id> timer advertise <adver-interval>	Время сообщения уведомления о восстановлении/конфигурации	«(Vlan-interface)#”

31.2.2 Показать VRRP

Таблица 119 – Просмотр VRRP

Команда	Описание	Режим
show vrrp info	Показать информацию о конфигурации VRRP	“#”
show vrrp info [interface <interface-type> <interface-number> | vrid <virtual-router-id>]	Показать информацию о статистике сообщений VRRP	“#”
clear vrrp statistics [interface <interface-type> <interface-number> | vrid <virtual-router-id>]	Очистить статистику сообщений VRRP	“#”
show vrrp status [interface <interface-type> <interface-number> | vrid <virtual-router-id>]	Показать информацию о статусе VRRP	“#”
show vrrp track {<track-num> | all}	Показать статус трека vrrp	“#”

31.3 Пример настройки

31.3.1 Критерий задач конфигурации

Таблица 120 - Критерий задач конфигурации

Критерий задач конфигурации	Описание
Глобальное включение VRRP	Необходимый
Привязать VRRP	Необходимый
Настроить виртуальный IP	Необходимый
Приоритет VRRP	Необходимый
Настроить DSCP для сообщений VRRP	Необязательный
Виртуальный IP получает сообщения ICMP	Необязательный
Функция VRRP TRAP	Необязательный
VRRP отправляет gratuitous-arp по расписанию	Необязательный
Настроить виртуальный MAC	Необязательный
TTL инспекция	Необязательный
Отслеживать статус порта	Необязательный
Режим VRRP	Необязательный
Мониторинг портов	Необязательный
Режим аутентификации	Необязательный
Время уведомления	Необязательный

31.3.2 Пример настройки

1. Требования к сети

— Router1, Router2 и Router3 динамически изучают и поддерживают маршруты через OSPF.

— Router1 — главный маршрутизатор, а Router2 — резервный маршрутизатор.

— Сбой устройства Router1, маршрутизация переключится на резервный маршрутизатор.

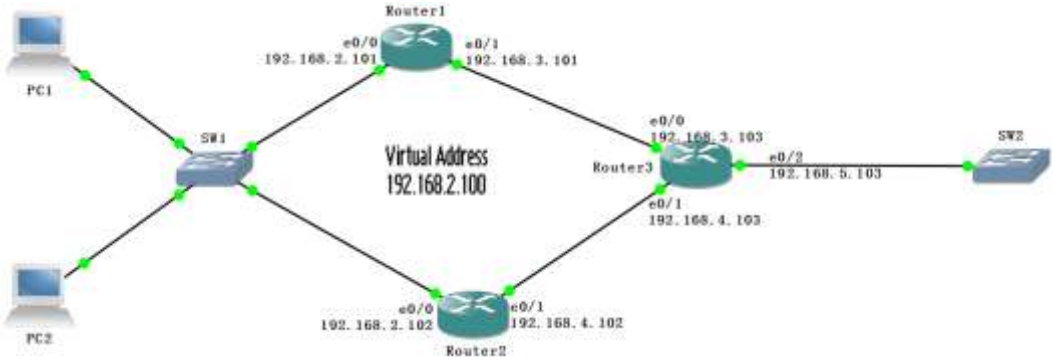

Рисунок 48 - Схема топологии сети

2. План настройки

— Настроить виртуальные интерфейсы для Router1, Router2 и Router3.

— Включить OSPF и объявить сеть.

— Настроить VRRP

3. Шаги настройки

（1）Настроить виртуальные интерфейсы

Настройка Router1

Router1# configure

Router1(config)# vlan 2

Router1(Vlan2)# exit.

Router1(config)# interface ethernet 1/2/2

Router1(config-eth1/2/2)# switchport access vlan 2

Router1(config-eth1/2/2)# exit

Router1(config)# interface vlan-interface 1

Router1(Vlan-interface1)# ip address 192.168.2.101 255.255.255.0

Router1(Vlan-interface1)# exit

Router1(config)# interface vlan-interface 2
Router1(Vlan-interface2)# ip address 192.168.3.101 255.255.255.0
Настройка Router2
Router2# configure
Router2(config)# vlan 2
Router2(Vlan2)# exit.
Router2(config)# interface ethernet 1/2/2
Router2(config-eth1/2/2)# switchport access vlan 2
Router2(config-eth1/2/2)# exit
Router2(config)# interface vlan-interface 1
Router2(Vlan-interface1)# ip address 192.168.2.102 255.255.255.0
Router2(Vlan-interface1)# exit
Router2(config)# interface vlan-interface 2
Router2(Vlan-interface2)# ip address 192.168.4.101 255.255.255.0
Настройка Router3
Router3# configure
Router3(config)# vlan 2-3
Router3(Vlan2)# exit.
Router3(config)# interface ethernet 1/2/2
Router3(config-eth1/2/2)# switchport access vlan 2
Router3(config-eth1/2/2)# exit
Router3(config)# interface ethernet 1/2/3
Router3(config-eth1/2/3)# switchport access vlan 3
Router3(config-eth1/2/3)# exit
Router3(config)# interface vlan-interface 1
Router3(Vlan-interface1)# ip address 192.168.3.103 255.255.255.0
Router3(Vlan-interface1)# exit
Router3(config)# interface vlan-interface 2
Router3(Vlan-interface2)# ip address 192.168.4.103 255.255.255.0
Router3(Vlan-interface2)# exit
Router3(config)# interface vlan-interface 3
Router3(Vlan-interface3)# ip address 192.168.5.103 255.255.255.0

（2）Настроить OSPF

Настройка Router1
Router1(config)# router ospf
Router1(ospf-router)# network 192.168.2.0/24 area 0

Router1(ospf-router)# network 192.168.3.0/24 area 0

Настройка Router2

Router2(config)# router ospf

Router2(ospf-router)# network 192.168.2.0/24 area 0

Router2(ospf-router)# network 192.168.4.0/24 area 0

Настройка Router3

Router3(config)# router ospf

Router3(ospf-router)# network 192.168.3.0/24 area 0

Router3(ospf-router)# network 192.168.4.0/24 area 0

Router3(ospf-router)# network 192.168.5.0/24 area 0

（3）Настроить VRRP

Настройка Router1

Router1(config)# interface vlan-interface 1

Router1(Vlan-interface1)# vrrp bind vrid 1

Router1(Vlan-interface1)# vrrp vrid 1 virtual-ip 192.168.2.100

Router1(Vlan-interface1)# vrrp vrid 1 priority 250

Настройка Router2

Router2(config)# interface vlan-interface 1

Router2(Vlan-interface1)# vrrp bind vrid 1

Router2(Vlan-interface1)# vrrp vrid 1 virtual-ip 192.168.2.100

4. Проверка конфигурации

Конфигурация VRRP на Router1

Router1(config)# show vrrp status

VRIDVLANIFSTATUSPRIORITYMASTER_IP

1 Vlanif1 Init 250 N/A

Конфигурация VRRP на Router2

Router1(config)# show vrrp status

VRIDVLANIFSTATUSPRIORITYMASTER_IP

1 Vlanif1 Init 250 N/A

PC1 и PC2 получают доступ к 192.168.5.103, маршрутизация осуществляется только через маршрутизатор Router1; Отключение

соединения с маршрутизатором Router1, доступ PC1 и PC2 к 192.168.5.103, связь переключается на маршрутизатор Router2.

32 BGP (BORDER GATEWAY PROTOCOL)/ ПРОТОКОЛ ПОГРАНИЧНОГО ШЛЮЗА

32.1 Обзор BGP

Протокол пограничного шлюза BGP (Border Gateway Protocol) — это протокол внутреннего шлюза для автономных систем. Основная функция системы объявлений BGP — обмен информацией о доступности с другими системами BGP в сети. Эта информация о доступности включает в себя информацию о достижимости внутри автономных систем AS (autonomous systems). Этой информации достаточно для построения подключенной AS (которая будет разорвана в случае петель маршрута), и на уровне AS применяются определенные политики.

BGP-4 предоставляет набор механизмов для поддержки бесклассовой междоменной маршрутизации CIDR (Classless Inter-Domain Routing) [RFC1518, RFC1519]. Эти механизмы включают в себя набор объявления IP-префиксов для адресов назначения и устранение понятия «класса» в BGP. BGP-4 также вводит такие концепции, как агрегирование маршрутов, включая наборы путей AS.

Информация о маршруте, которым обменивается BGP, поддерживает парадигму назначения, предполагающую, что маршрутизаторы пересылают пакеты на основе адреса назначения в заголовке IP-пакета. Это, в свою очередь, определяет, можно ли применять политики с помощью BGP, поддерживая политики, основанные на пересылке адреса назначения.

32.2 Настройка BGP

32.2.1 Общая конфигурация BGP

Таблица 121 - Общая конфигурация BGP

Команда	Описание	Режим
[no] router bgp <as-number>	Отключить/включить BGP	“(config)#”
bgp router-id <router-Id> **no bgp router-id**	Отменить/Настроить идентификатор маршрутизатора	“(bgp-router)#”

32.2.2 Конфигурация домена BGP

Таблица 122 - Конфигурация домена BGP

Команда	Описание	Режим
maximum-paths ebgp <1-255> **no maximum-paths ebgp**	Максимальное время пересылки сообщений EBGP	“(bgp-router)#”
maximum-paths ibgp <1-255> **no maximum-paths ebgp**	Максимальное количество попыток пересылки сообщений IBGP	“(bgp-router)#”
timers bgp <0-65535> <0-65535> **no timers bgp**	BGP keepalive/время удержания	“(bgp-router)#”
bgp network import-check no bgp network import-check	Обнаружить достижимость маршрутизации	“(bgp-router)#”
bgp default local-preference <0-4294967295> no bgp default local-preference	Локальный приоритет по умолчанию	“(bgp-router)#”
redistribute (connected|static|rip|ospf) no redistribute (connected|static|rip|ospf)	Ввести другие протокольные маршруты	“(bgp-router)#”
network A.B.C.D/M no network A.B.C.D/M	Ввести маршруты публикации вручную	“(bgp-router)#”
aggregate-address A.B.C.D/M no aggregate-address A.B.C.D/M	Агрегация маршрутизации	“(bgp-router)#”
neighbor (A.B.C.D|WORD) remote-as <0-4294967295>	Привязать соседа как домен	“(bgp-router)#”
neighbor WORD peer-group	Создать группу соседей	“(bgp-router)#”
no neighbor (A.B.C.D|WORD)	Удалить соседей	“(bgp-router)#”
neighbor (A.B.C.D | WORD) peer-group WORD no neighbor (A.B.C.D | WORD) peer-group WORD	Привязать группу соседей	“(bgp-router)#”
neighbor (A.B.C.D | WORD) shutdown no neighbor (A.B.C.D | WORD) shutdown	Близкие указанные соседи	“(bgp-router)#”

neighbor (A.B.C.D | WORD) port <0-65535> no neighbor (A.B.C.D | WORD) port	Установить номер TCP-порта для соседских подключений	“(bgp-router)#”
neighbor (A.B.C.D | WORD) weight <0-65535> no neighbor (A.B.C.D | WORD) weight	Установить веса соседей	“(bgp-router)#”

32.3 Пример настройки

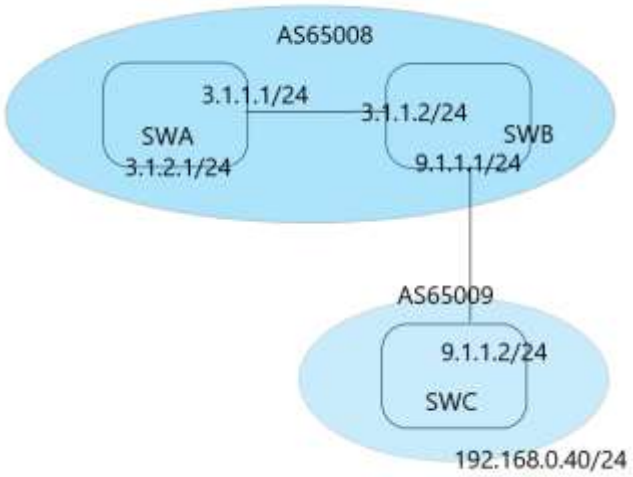

Рисунок 49 - Схема топологии сети

Конфигурация:

SWA:

```
vlan 1-4
interface vlan-interface 1
  ip address 3.1.2.1 255.255.255.0
interface vlan-interface 3
  ip address 3.1.1.1 255.255.255.0
interface ethernet 1/0/3
  switchport mode access
  switchport access vlan 3
router ospf
network 3.1.1.1/24 area 0.0.0.0
network 3.1.2.1/24 area 0.0.0.0

router bgp 65008
```

neighbor 3.1.1.2 remote-as 65008

SWB :

```
vlan 2-3
interface vlan-interface 2
  ip address 9.1.1.1 255.255.255.0
interface vlan-interface 3
  ip address 3.1.1.2 255.255.255.0
interface ethernet 1/0/7
  switchport mode access
  switchport access vlan 2

 interface ethernet 1/0/17
  switchport mode access
  switchport access vlan 3

router ospf
network 3.1.1.2/24 area 0.0.0.0
network 9.1.1.1/24 area 0.0.0.0
router bgp 65008
neighbor 3.1.1.1 remote-as 65008
neighbor 9.1.1.2 remote-as 65009
network 3.1.1.0/24
network 3.1.2.0/24
```

SWC:

```
vlan 1-2
  interface vlan-interface 1
  ip address 192.168.0.40 255.255.255.0
  interface vlan-interface 2
  ip address 9.1.1.2 255.255.255.0

 interface ethernet 1/0/7
  switchport mode access
  switchport access vlan 2
```

router bgp 65009
neighbor 9.1.1.1 remote-as 65008
network 192.168.0.40/24

```
SWITCH(config)# show ip routing-table all
Total Entry: 4
-------------------------------------------------------------
       Destination/ Mask       Proto          NextHop          Interface                       Des
           3.1.1.0/24          Bgp          9.1.1.1          Vlanif2
           3.1.2.0/24          Bgp          9.1.1.1          Vlanif2
           9.1.1.0/24        Direct         9.1.1.2          Vlanif2
       192.168.0.0/24        Direct     192.168.0.40         Vlanif1
SWITCH(config)#
```

Рисунок 50 - Просмотр маршрутизации

33 DOT1X/ ПРОТОКОЛ УПРАВЛЕНИЯ ДОСТУПОМ К СЕТИ НА ОСНОВЕ ПОРТОВ

33.1 Обзор Dot1x

При практическом развертывании сетей IEEE 802 неизбежно, что неавторизованные устройства будут физически подключаться к сети.

Протокол 802.1x обеспечивает протокол управления доступом к сети на основе портов. Управление доступом к сети на основе портов относится к аутентификации и контролю пользовательских устройств, подключенных на уровне портов устройств доступа в локальной сети. Если пользовательское устройство, подключенное к порту, проходит аутентификацию, оно может получить доступ к ресурсам в локальной сети; в противном случае он не сможет получить доступ к ресурсам локальной сети.

Системы, использующие 802.1x, следуют типичной архитектуре клиент/сервер, состоящей из трех объектов:

Клиентские устройства (ПК): запрашивают доступ к локальной сети и службам коммутатора, а также отвечают на запросы коммутаторов. На рабочих станциях должно быть установлено клиентское программное обеспечение, совместимое с протоколом 802.1X, например Linux xsupplicant.

Сервер аутентификации: выполняет фактическую аутентификацию клиентов. Сервер аутентификации проверяет личность клиента и сообщает коммутатору, имеет ли клиент разрешение на доступ к локальной сети и

службам коммутатора. Поскольку коммутаторы действуют как прокси, служба аутентификации прозрачна для клиентов. В этой версии единственным поддерживаемым сервером аутентификации является Remote Authentication Dial-In User Service (RADIUS), который поддерживает расширяемый протокол аутентификации EAP (Extensible Authentication Protocol). RADIUS работает в режиме клиент/сервер, обмениваясь информацией безопасной аутентификации между сервером и несколькими клиентами RADIUS.

Коммутаторы (граничные коммутаторы или точки беспроводного доступа): контролируют физический доступ к сетям на основе статуса аутентификации клиента. Выступая в качестве посредников (прокси) между клиентами и серверами аутентификации, коммутаторы запрашивают идентификационную информацию от клиентов, проверяют эту информацию через серверы аутентификации и возвращают результаты аутентификации клиентам. Коммутаторы включают в себя RADIUS-клиенты, отвечающие за инкапсуляцию и декапсуляцию кадров EAP и взаимодействие с серверами аутентификации. Когда коммутатор получает кадр EAPOL и передает его серверу аутентификации, заголовок Ethernet удаляется, оставляя оставшийся кадр EAP для переупаковки в формат RADIUS. Кадры EAP не изменяются и не проверяются во время инкапсуляции, а сервер аутентификации должен поддерживать собственные форматы кадров EAP. Когда коммутатор получает сообщение от сервера аутентификации, он удаляет заголовок кадра сервера, затем переупаковывает оставшийся кадр EAP в формат кадра Ethernet и отправляет его клиенту. Dot1x можно настроить на портах доступа или портах маршрутизатора уровня 3.

33.2 Конфигурация dot1x

Таблица 123 – Команды конфигурации dot1x

Команда	Описание	Режим
dot1x (enable|disable)	Глобальная активирующая конфигурация	“(config)#”
dot1x (enable|disable)	Конфигурация включения порта	“(config-eth)#”
radius authentication A.B.C.D INTEGER<1-65535>	Настроить IP-адрес радиус-сервера	“(config)#”
radius key authentication text	Настроить общий ключ для сообщений о взаимодействии устройства и сервера Radius	“(config)#”
show dot1x	Посмотреть конфигурацию dot1x	“#”

33.3 Пример настройки

Включить глобальную конфигурацию:
SWITCH(config)# dot1x enable

Настроить порт:
SWITCH(config-eth1/0/1)# dot1x enable

Настроить сервер аутентификации:
SWITCH(config)# radius authentication 192.168.1.213

Отображение информации о конфигурации:
SWITCH(config)# show dot1x
Global 802.1X protocol is : enable
Radius Auth IP =192.168.1.213 Port=1812
Auth Server Encryption Key=Trustel

eth1/0/1 802.1X protocol is : enable
eth1/0/2 802.1X protocol is : disable
eth1/0/3 802.1X protocol is : disable
eth1/0/4 802.1X protocol is : disable
eth1/0/5 802.1X protocol is : disable
eth1/0/6 802.1X protocol is : disable

34 НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

34.1 Восстановление ПО коммутатора через встроенный загрузчик

1. Перезагрузить устройство по питанию или командой.
2. Нажимайте “Esc” пока не попадём в bootloader

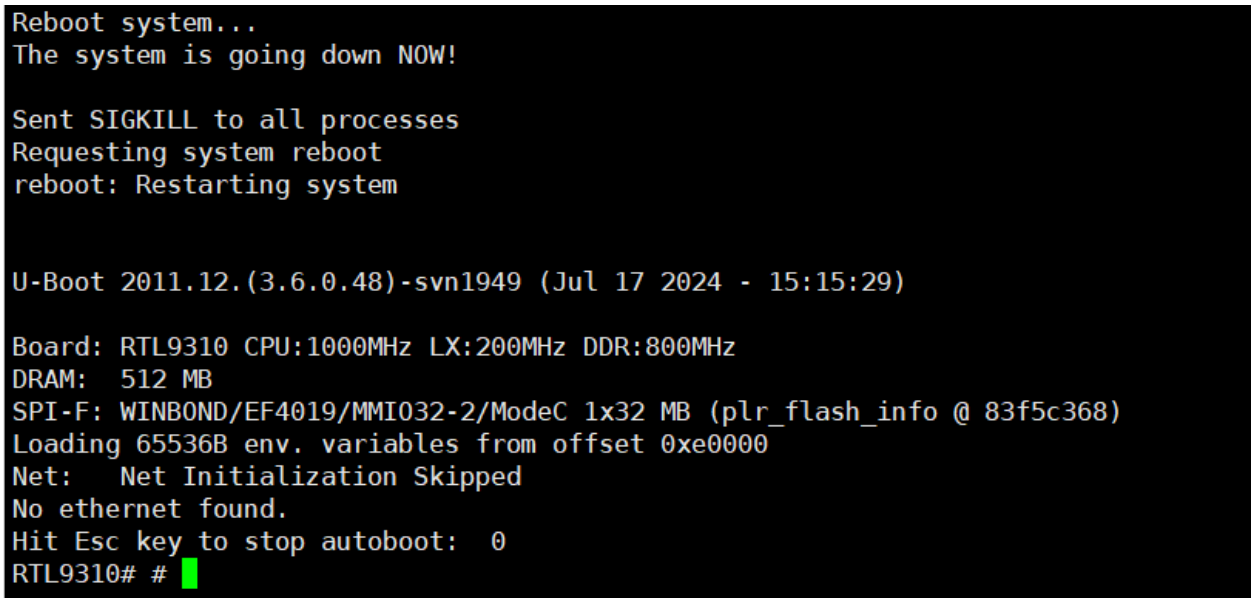

Рисунок 51 - bootloader

3.Настройте адрес tftp сервера командой **setenv serverip 10.16.0.200.**

4.Настройте адрес коммутатора командой **setenv ipaddr 10.16.0.199.**

5.Проверьте настройки командой **printenv.**

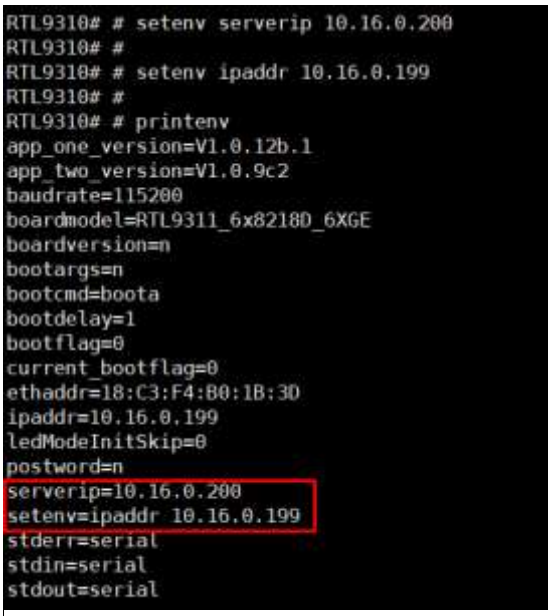

Рисунок 52 - Настройки

6.Загрузить образ на коммутатор командой: **upgrade romforce VA2200-48P-6XV1.0.2.img.**

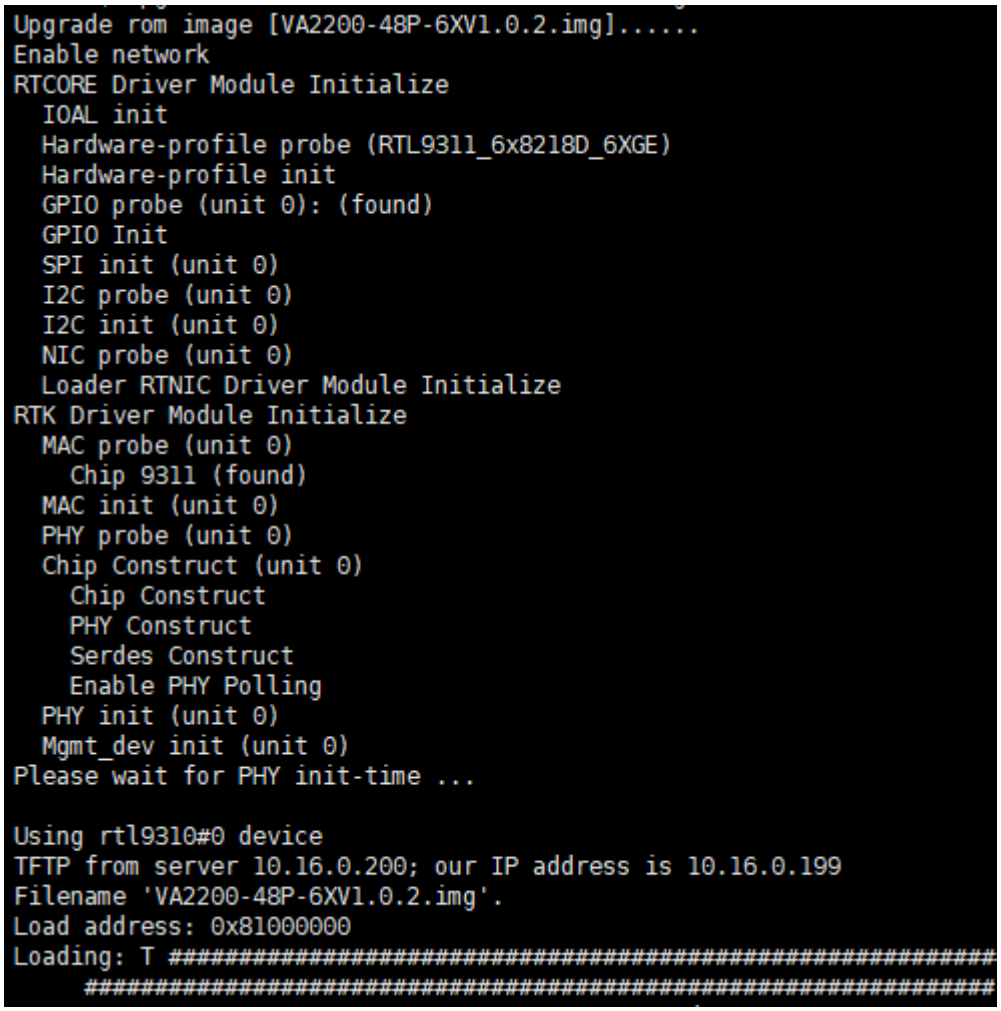

Рисунок 53 – Загрузка образа

7. После успешной загрузки образа, перезагрузить коммутатор командой reset.

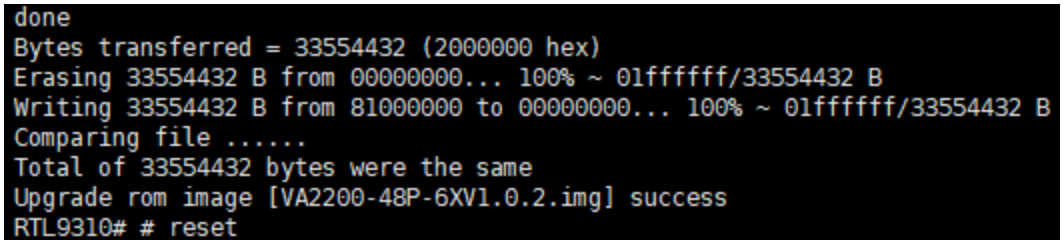

Рисунок 54 - Перезагрузка

35 Информирование о лицензиях

35.1 SNMP

Various copyrights apply to this package, listed in various separate
parts below. Please make sure that you read all the parts.

---- Part 1: Sparta, Inc (BSD) -----

Copyright (c) 2003-2010, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may
  be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 2: ScienceLogic, LLC (BSD) ----

Copyright (c) 2006, ScienceLogic, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its
  contributors may be used to endorse or promote products derived
  from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS
OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

35.2 PIMD

Copyright (C) 1998-2001 University of Southern California/Information Sciences Institute
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.