ФАКЕЛ

Руководство по эксплуатации программы для ЭВМ "Программное обеспечение коммутатора «Факел»"

ФАКЕЛ

Содержание

1 Введение

1.1 О программном обеспечении

Программа для ЭВМ для ЭВМ "Программное обеспечение коммутатора «Факел»" — встроенное прикладное программное обеспечение для выполнения функций управления, коммутации и маршрутизации сетевых соединений внутри локальных сетей и сетей связи общего пользования.

Программа для ЭВМ "Программное обеспечение коммутатора «Факел»" предназначена для работы на аппаратных платформах коммутаторов «Факел» серий FS100, FS200, FS400 (далее — Устройства). Программа инициализирует аппаратные средства коммутатора, выполняет коммутацию и маршрутизацию сетевого трафика, предоставляет интерфейсы управления конфигурацией и состоянием устройства, обеспечивает мониторинг, диагностику.

1.2 Описание функциональных характеристик

Программа для ЭВМ для ЭВМ "Программное обеспечение коммутатора «Факел»" обладает следующими возможностями:

- коммутация Ethernet-трафика в сетях передачи данных, настройка режимов и скоростей работы портов, поддержка кадров увеличенного размера (Jumbo Frame);
- создание и управление виртуальными локальными сетями (VLAN), туннелирование и преобразование VLAN-тегов (QinQ, VLAN Mapping);
- агрегация каналов связи (статическая и по протоколу LACP), в том числе межшассийная (MLAG), для повышения производительности и отказоустойчивости;
- предотвращение сетевых петель и защита топологии средствами протоколов связующего дерева (RSTP, MSTP) и защиты кольца Ethernet (ERPS);
- обработка многоадресного трафика канального уровня (IGMP Snooping);
- поддержка стека протоколов IPv4, статическая и динамическая (RIP) маршрутизация трафика;
- виртуальная маршрутизация и переадресация (VRF), маршрутизация на основе политик (PBR) и по нескольким равным путям (ECMP);
- предоставление сетевых служб: DHCP (сервер, ретранслятор, Snooping), клиент службы доменных имён (DNS), синхронизация времени (NTP);

- предотвращение сетевых петель и обеспечение резервирования соединений, резервирование шлюза по умолчанию (VRRP) и контроль состояния каналов;
- управление качеством обслуживания и приоритезация трафика: классификация по классу обслуживания (CoS) и кодовой точке (DSCP), ограничение и формирование полосы пропускания;
- управление доступом к сетевым ресурсам средствами списков управления доступом (ACL);
- аутентификация, авторизация и учёт (AAA) с поддержкой протоколов RADIUS, TACACS+ и стандарта IEEE 802.1X;
- защита от широковещательных штормов (Storm Control), изоляция трафика (Private VLAN), контроль обучения MAC-адресов на портах (Port Security);
- защита трафика управления (SSHv2) и разграничение полномочий по уровням привилегий;
- мониторинг состояния сетевых интерфейсов и аппаратных компонентов (датчиков, источников питания, вентиляторов);
- обнаружение соседних устройств (LLDP), измерение параметров сети (IP SLA), диагностика кабельных линий (VCT), зеркалирование портов;
- подача электропитания подключаемым устройствам по технологии Power over Ethernet (PoE);
- управление через интерфейс командной строки (CLI), протокол SNMP (v1/v2c/v3);
- резервное копирование, восстановление и хранение конфигурации в энергонезависимой памяти.

Если у вас возникнут какие-либо вопросы при использовании нашего продукта или чтении этого документа, пожалуйста, свяжитесь с нами

2 Руководство по базовой настройке

2.1 Настройка Управления системой

2.1.1 Обзор

2.1.1.1 Функции начального оповещения

Функция «Баннер» используется для настройки сообщений на устройствах. Пользователь может указать любые сообщения для уведомления других пользователей. Неправильные действия могут привести к критическим ситуациям, таким как прерывание работы сервиса; в этом случае необходимо предварительное уведомление (например, для уведомления пользователей «Не перезагружайте устройство»).

В настоящее время поддерживаются три типа сообщений:

- MOTD (message of the day). Сообщения будут отображаться на терминале, когда пользователь подключится к устройству.
- баннер входа в систему. Сообщения будут отображаться на терминале, когда пользователь войдет в систему. Для отображения этого сообщения требуется «Режим входа в систему». См. раздел «Настройка управления пользователями».
- баннер EXEC. Сообщения будут отображаться на терминале, когда пользователь войдет в режим EXEC.

2.1.1.2 Принцип работы

Эта функция отображает уведомление на терминале для предотвращения ошибок при работе.

2.1.1.3 Настройка баннера MOTD

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте уведомление.

Пользователь может создать уведомление (однострочное или многострочное) для отображения на всех подключенных терминалах. В следующем примере разделительным символом является #. Все символы между двумя разделительными символами будут отображаться на терминалах при подключении устройства пользователем.

Длина сообщения составляет максимум 99 строк, по 1023 символа в каждой строке.

```
Switch(config)# banner motd # This is a switch #
```

Шаг 3. Выход из режима настройки.

```
Switch(config)# exit
```

Шаг 4. Проверка.

Для отображения внесенной конфигурации используйте следующую команду:

```
switch# show running
banner motd ^C
 This is a switch
^C
```

Настройка баннера входа в систему

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте уведомление.

Пользователь может создать уведомление (однострочное или многострочное), которое будет отображаться на всех подключенных терминалах. Для отображения этого сообщения требуется «Режим входа в систему». См. раздел «Настройка управления пользователями».

В следующем примере разделительным символом является #. Все символы между двумя разделительными символами будут отображаться на терминале при подключении устройства пользователем.

Длина сообщения составляет максимум 99 строк, по 1023 символа в каждой строке.

```
Switch(config)# banner login # admin login #
```

Шаг 3. Выход из режима настройки.

```
Switch(config)# exit
```

Шаг 4. Проверка.

Для отображения внесенной конфигурации используйте следующую команду:

```
switch# show running
banner login ^C
 admin login
^C
```

2.1.1.4 Настройка информирующего Exec баннера

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте уведомление.

Пользователь может создать уведомление (однострочное или многострочное) для отображения на всех подключенных терминалах. В следующем примере разделительным символом является #. Все символы между двумя разделительными символами будут отображаться на терминалах, когда пользователь перейдет в режим EXEC.

Длина сообщения составляет максимум 99 строк, по 1023 символа в каждой строке.

```
Switch(config)# banner exec # do not reboot! #
```

Шаг 3. Выход из режима настройки.

```
Switch(config)# exit
```

Шаг 4. Проверка.

Для отображения внесенной конфигурации используйте следующую команду:

```
switch# show running
banner exec ^C
 do not reboot!
^C
```

2.1.2 Сценарии применения

2.1.2.1 Сценарий 1: Промаркируйте нужное устройство

Установите сообщение MOTD как «Это коммутатор определенного отдела/подразделения», и пользователь увидит сообщение при подключении к устройству. Если пользователю потребуется управлять коммутатором другого отдела, он сможет понять, что подключился не к тому устройству.

Шаги при настройке

```
Switch# configure terminal
Switch(config)# banner motd # This is a switch of IT OTDEL! ! ! #
Switch(config)# exit
```

Проверка внесенной конфигурации

```
switch# show running
banner motd ^C
 This is a switch of IT OTDEL ! ! !
^C
```

2.2 Настройка подсистемы управления пользователями

2.2.1 Общие положения

2.2.1.1 Описание

Подсистема управления пользователями повышает безопасность, предотвращая подбор пароля неавторизованными пользователями. Пользователь ограничен определенным количеством попыток успешного входа в коммутатор.

Существуют три режима загрузки коммутатора:

- в режиме «без авторизации» любой может подключиться к коммутатору без аутентификации;
- в режиме «с авторизацией» существует один пользователь по умолчанию;
- в режиме «локальной авторизации» для подключения к коммутатору требуется учетная запись пользователя. Локальная аутентификация пользователей использует созданные заранее локальные учетные записи и пароли для проверки попыток входа локальных пользователей. Каждый коммутатор может иметь максимум 32 локальные учетные записи пользователей. Прежде чем включить локальную аутентификацию пользователей, необходимо создать как минимум одну локальную учетную запись. Вы можете настроить локальные учетные записи пользователей, создав уникальную комбинацию имени пользователя и пароля для каждого локального пользователя. Каждое имя пользователя должно содержать менее 32 символов. Вы можете настроить каждую локальную учетную запись пользователя с уровнем привилегий; допустимые уровни привилегий — 1 или 4. После авторизации локального пользователя в систему отображаются только те команды, которые доступны для этого уровня привилегий;

В режим настройки может одновременно войти только один пользователь.

2.2.2 Настройка подсистемы управления пользователями

2.2.2.1 Настройка пользователей в режиме «локальной авторизации»

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Введите имя пользователя и пароль.

```
Switch(config)# username testname privilege 4 password 123abc<>
```

Шаг 3. Перейдите в режим настройки и установите тип режима авторизации.

```
Switch(config)# line vty 0 7
Switch(config-line)# login local
Switch(config-line)# exit
```

Шаг 4. Выход из режима настройки.

```
Switch(config)# exit
```

Шаг 5. Проверка внесенной конфигурации.

После выполнения указанных выше настроек для входа в коммутатор потребуется имя пользователя и пароль, и пользователь сможет войти, используя ранее созданные имя пользователя и пароль. Это пример вывода приглашения ко входу в систему.

```
Username:
```

После ввода имени пользователя потребуется ввести пароль

```
Username: testname
Password:
```

Успешная авторизация

```
Password:

Switch#
```

2.2.2.2 Настройка пользователей в режиме «с авторизацией»

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки и задайте пароль.

```
Switch(config)# line vty 0 7
Switch(config-line)# line-password abc
Switch(config-line)# login
```

Шаг 3. Выход из режима настройки.

```
Switch(config)# exit
```

Шаг 4. Проверка внесенной конфигурации.

После выполнения указанных выше настроек для входа в коммутатор потребуется ранее созданный пароль. Это пример вывода приглашения к входу в систему.

```
Password:
```

Настройка процедуры восстановления пароля

Если пароль утерян, его можно восстановить, выполнив следующие шаги.

Шаг 1. Включите систему. Начнётся работа загрузчика. На консоли будет выведена следующая информация.

```
CPU:   MPC8247 (HiP7 Rev 14, Mask 1.0 1K50M) at 350 MHz
Board: 8247 (PCI Agent Mode)
I2C:   ready
DRAM:  256 MB
In:    serial
Out:   serial
Err:   serial
Net:   FCC1 ETHERNET, FCC2 ETHERNET [PRIME]
Press ctrl+b to stop autoboot: 3
```

Шаг 2. Нажмите Ctrl+B. Остановите автоматическую загрузку.

```
Bootrom#
```

Шаг 3. В интерфейсе загрузчика следуйте приведенным ниже инструкциям.

```
Bootrom# boot_flash_nopass
Bootrom# Do you want to  revert  to the default config file ? [Y|N|E]:
```

 Пожалуйста, запомните ваше имя пользователя и пароль.

Утеря пароля может привести к потере конфигурации или прерыванию работы сервиса.

2.3 Настройка TFTP

2.3.1 Общие положения

2.3.1.1 Описание функции

Вы можете загрузить файл конфигурации коммутатора с TFTP-сервера или загрузить файл с коммутатора на TFTP-сервер. Загрузка файла конфигурации коммутатора с сервера необходима для обновления конфигурации коммутатора. Вы можете перезаписать текущий файл новым. Загрузка файла конфигурации коммутатора на сервер необходима для резервного копирования; этот загруженный файл можно использовать для будущих загрузок на тот же или на другой коммутатор того же типа.

2.3.2 Настройка

Перед началом загрузки или выгрузки файла конфигурации с помощью TFTP выполните следующие действия:

Убедитесь, что рабочая станция, выступающая в качестве TFTP-сервера, правильно настроена.

Убедитесь, что на коммутаторе прописан сетевой маршрут к TFTP-серверу. Если маршрутизация между подсетями не прописана, то коммутатор и TFTP сервер должны находиться в одной подсети. Проверьте подключение к TFTP-серверу с помощью команды ping.

Убедитесь, что загружаемый файл конфигурации находится в правильном каталоге на TFTP-сервере.

При операциях загрузки/выгрузки убедитесь, что права доступа к файлу установлены правильно.

При операциях выгрузки, если вы перезаписываете существующий файл (включая пустой файл, если вам пришлось создать такой) на сервере, убедитесь, что права доступа к файлу установлены правильно.

2.3.2.1 Загрузка файла конфигурации с помощью TFTP

```
Switch# copy mgmt-if tftp://10.10.10.163/startup-config.conf flash:/startup-config.conf
```

2.3.2.2 Загрузка файла конфигурации с использованием TFTP

```
Switch# copy flash:/startup-config.conf mgmt-if tftp://10.10.10.163/startup-config.conf
```

2.4 Настройка Telnet

2.4.1 Общие положения

2.4.1.1 Описание функции

Telnet — это сетевой протокол, используемый в Интернете и локальных сетях для обеспечения двунаправленной интерактивной связи с использованием виртуального терминального соединения для передачи текстовых команд. Данные пользователя передаются в полосе пропускания вместе с управляющей информацией Telnet в 8-битном канале передачи данных по протоколу TCP (Transmission Control Protocol). Telnet был разработан в 1969 году, описан в RFC 15, расширен в RFC 854 и стандартизирован как стандарт Internet Engineering Task Force (IETF) STD 8. Исторически Telnet обеспечивал доступ к интерфейсу командной строки (обычно операционной системы) на удаленном хосте. Большинство сетевого оборудования и операционных систем со стеком TCP/IP поддерживают службу Telnet для удаленной настройки (включая системы на базе Windows NT). Из-за проблем с безопасностью Telnet, его использование сократилось в пользу протокола SSH.

2.4.2 Настройка

2.4.2.1 Telnet подключение к внутреннему порту коммутатора

```
Switch# telnet 10.10.29.247
Entering character mode
Escape character is '^]'.
Switch #
```

2.4.2.2 Telnet подключение к порту управления коммутатора

```
Switch# telnet mgmt-if 10.10.29.247
Entering character mode
Escape character is '^]'.
Switch #
```

2.4.2.3 Настройка сервера Telnet

Шаг 1. Вход в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включение службы Telnet.

```
Switch(config)# service telnet enable
```

Шаг 3. Выход из режима настройки.

```
Switch(config)# exit
```

2.5 Настройка SSH

2.5.1 Общие положения

2.5.1.1 Описание функции

Протокол Secure Shell (SSH) обеспечивает безопасное удаленное соединение с устройством. SSH обеспечивает более высокий уровень безопасности удаленных соединений, чем Telnet, благодаря надежному шифрованию при аутентификации. SSH поддерживает алгоритмы шифрования DES (Data Encryption Standard), 3DES (Triple DES) и аутентификацию пользователей на основе паролей. Функция SSH включает в себя SSH-сервер и интегрированный SSH-клиент, которые представляют собой дополнительные приложения, работающие на коммутаторе. Вы можете использовать SSH-клиент для подключения к коммутатору, на котором запущен SSH-сервер. Встроенный SSH-клиент также работает с SSH-сервером, поддерживаемым в этой аппаратной версии, и с другими SSH-серверами.

2.5.2 Настройка

Рисунок 1 – Топология SSH сессии

2.5.2.1 Создание ключа для SSH

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте ключ.

```
Switch(config)# rsa key a generate
```

Шаг 3. Создайте закрытый ключ с именем a.pri содержащий ключ A, затем сохраните его в ПЗУ.

```
Switch(config)# rsa key a export url flash:/a.pri private ssh2
```

Шаг 4. Создайте закрытый ключ с именем a.pub, содержащий ключ A, и сохраните его в ПЗУ.

```
Switch(config)# rsa key a export url flash:/a.pub public ssh2
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# exit
```

2.5.2.2 Импортирование ключа

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Импортируйте созданный нами ключ a.pub, указав его как importKey.

```
Switch(config)# rsa key importKey import url flash:/a.pub public ssh2
```

Шаг 3. Создайте имя пользователя и пароль.

```
Switch(config)# username aaa privilege 4 password abc
```

Шаг 4. Назначьте ключ пользователю aaa.

```
Switch(config)# username aaa assign rsa key importKey
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# exit
```

2.5.2.3 Использование SSH для подключения

Шаг 1. Загрузка ключа a.pri в SSH-клиента.

Шаг 2. Подключение к клиенту.

```
[root@test1 tftpboot]# ssh -i a.pri aaa@10.10.39.101
aaa@10.10.39.101's password:
Switch#
```

2.6 Настройка времени и часового пояса

2.6.1 Общие положения

2.6.1.1 Описание функции

Допускается ручная настройка времени и даты после перезагрузки системы. Время останется точным до следующей перезагрузки системы. Мы рекомендуем использовать ручную настройку только в крайнем случае. Если у вас есть внешний источник, с которым коммутатор может синхронизироваться, вам не нужно вручную устанавливать системные часы.

2.6.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка времени и часового пояса.

```
Switch(config)# clock set datetime 11:30:00 10 26 2013
Switch(config)# clock set summer-time dst date 6 1 2013 02:00:00 10 31 2013
02:00:00 120
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# exit
```

Шаг 4. Проверка.

Используйте следующую команду для отображения времени и даты:

```
Switch# show clock detail
13:31:10 dst Sat Oct 26 2013
Time zone: (GMT + 08:00:00)  beijing
Summer time starts at beijing 02:00:00  06/01/2013
Summer time ends at dst 02:00:00  10/31/2013
Summer time offset:  120 minutes
```

2.7 Конфигурирование RPC API

2.7.1 Общие положения

2.7.1.1 Описание функции

Служба RPC API позволяет пользователю настраивать и отслеживать работу системы коммутатора посредством удаленного вызова процедур (RPC) из своей локальной программы.

В настоящее время сервис поддерживает JSON-RPC поверх протокола HTTP, с базовой аутентификацией HTTP.

2.7.1.2 Описание работы

Служба RPC API использует стандартный протокол JSON-RPC по HTTP для связи между коммутатором и вашей локальной программой. Пользователь может отправлять команды CLI коммутатора используя метод JSON-RPC: ‘executeCmds’. По умолчанию режим CLI находится в привилегированном режиме EXEC (#).

Пользователь может отправить запрос JSON-RPC через HTTP POST-запрос по URL: http://:/command-api. Структура запроса и ответа JSON-RPC показаны ниже:

JSON-RPC запрос

```
{
    "params":[                                          Parameters for
command
        {
            "format":"text",                            Expected response
format, can be ‘text’ or ‘json’,
the default format is ‘text’
            "version":1,                                The API version
            "cmds":[                                    List of CLI commands
                "show run",                             CLI command 1
                "config t",                             CLI command 2
                "vlan database",                        CLI command 3
                "vlan 1-8",                             CLI command 4
                "interface eth-0-1",                    CLI command 5
                "switchport mode trunk",                CLI command 6
                "switchport trunk allowed vlan add 2",  CLI command 7
                "shutdown",                             CLI command 8
                "end",                                  CLI command 9
                "show interface switchport"             CLI command 10
            ]
        }
    ],
    "jsonrpc":"2.0",                                    JSON RPC protocol
version. Always 2.0.
    "method":"executeCmds",                             Method to run the
switch CLI commands
    "id":"70853aff-af77-420e-8f3c-fa9430733a19"         JSON RPC unique
identifier
}
```

JSON-RPC ответ

```
{
    "jsonrpc":"2.0",                                    JSON RPC protocol
version. Always 2.0.
    "id":"70853aff-af77-420e-8f3c-fa9430733a19",        JSON RPC unique
identifier
    "result":[                                          Result list of
objects from each CLI command executed.
        {
            "sourceDetails":"version 5.1.6.fcs\n!\n …",  Output information
of CLI Command 1.
                                                        The Original ASCII
output information returned from CLI command if this command is successfully
executed.
            "errorCode":-1003,                          Error code if it is
available.
            "errorDesc":"unsupported command…",         Error description if
it is available.
            "warnings":"% Invalid…",                    Warnings if it is
available.
                                                        Formatted JSON
object will also be returned if it is available.
        },
        { },                                            Output information
of CLI Command 2.
        { },                                            Output information
of CLI Command 3.
        { },                                            Output information
of CLI Command 4.
        { },                                            Output information
of CLI Command 5.
        { },                                            Output information
of CLI Command 6.
        { },                                            Output information
of CLI Command 7.
        { },                                            Output information
of CLI Command 8.
        { },                                            Output information
of CLI Command 9.
        {
            "sourceDetails":" Interface name          : eth-0-1\n Switchport
mode          : trunk\n …\n"
        }                                               Output information
of CLI Command 10.
    ]
}
```

Пример кода клиента на Python

Пример кода, использующего библиотеку ‘pyjsonrpc’:

```
import pyjsonrpc
import json

http_client = pyjsonrpc.HttpClient(
    url = "http://10.10.39.64:80/command-api",
    username = "username",
    password = "password"
)

cmds = {}
cmd_list = ["show run", "config t", "vlan database", "vlan 1-8", "interface
eth-0-1", "switchport mode trunk", "switchport trunk allowed vlan add 2",
"shutdown", "end", "show interface switchport"]

cmds['cmds'] = cmd_list
cmds['format'] = 'text'
cmds['version'] = 1

try:
    response = http_client.call("executeCmds", cmds)
    print("json response:");
    json_result = json.dumps(response, indent=4)
    print(json_result)
except Exception, e:
    if e.code == 401:
        print "Unauthorized user"
    else:
        print e.message
        print e.data
```

Коды ошибок

Таблица 1 – Список кодов ошибок JSON-RPC 2.0

Код ошибки	Описание
32700	Ошибка синтаксического анализа
32600	Неверный запрос
32601	Метод не найден
32602	Неверный параметр
32603	Внутренняя ошибка

Таблица 2 – Список кодов ошибок RPC-API

Код ошибки	Описание
1000	Общая ошибка
2001	JSON RPC API ошибка: версия API не поддерживается
2002	Ошибка API JSON RPC: необходимо указать ‘params’ вместе с ‘cmds’ в JSON RPC
2003	Ошибка API JSON RPC: неподдерживаемый формат ответа команды
3001	Сбой выполнения команды: истекло время ожидания
3002	Сбой выполнения команды: неподдерживаемая команда
3003	Сбой выполнения команды: несанкционированная команда
3004	Сбой выполнения команды: строка не соответствует ни одной команде в текущем режиме
3005	Сбой выполнения команды: невозможно преобразовать в формат JSON
3006	Сбой выполнения команды: слишком короткий список команд
3007	Сбой выполнения команды: слишком длинный список команд

2.7.2 Настройка

2.7.2.1 Настройка службы RPC API

Пользователь может включить службу RPC API, выполнив следующие шаги.

Номер пота по умолчанию - 80.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите службу RPC API.

```
Switch(config)# service rpc-api enable
```

NOTE Используйте следующую команду для отключения службы rpc-api:

```
Switch(config)# service rpc-api disable
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

2.7.2.2 Настройка службы RPC API с HTTP-аутентификацией

Пользователь может настроить режим HTTP-аутентификации для сервиса RPC API.

В настоящее время поддерживается только базовая HTTP-аутентификация. Пользователь получит код состояния 401 (Несанкционированный доступ), если укажет неверное имя пользователя или пароль.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Укажите имя пользователя и пароль, затем включите аутентификацию RPC-API.

```
Switch(config)# username myuser password mypass privilege 4
Switch(config)# service rpc-api auth-mode basic
```

NOTE Используйте следующую команду для отключения аутентификации:

```
Switch(config)# no service rpc-api auth-mode
```

NOTE Настройки HTTP-аутентификации службы RPC API вступят в силу после перезапуска этой службы или перезагрузки системы.

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show services rpc-api
RPC API service configuration:
 Server State         : enable
 Port                 : 80
 Authentication Mode  : basic
 VRF                  : default
```

3 Руководство по настройке Ethernet

3.1 Настройка интерфейса

3.1.1 Общие положения

3.1.1.1 Описание функции

Состояние интерфейса, скорость и режим дуплекса можно настроить. Если интерфейс настроен как «no shutdown», он может нормально работать после подключения кабеля. Если интерфейс настроен как «shutdown», он не будет работать независимо от того, подключен кабель или нет.

Если устройство поддерживает комбинированные порты, пользователь может выбрать режим работы (медный или оптоволоконный). Два режима работы одного порта не могут работать одновременно. Настройка скорости или режима дуплекса на комбинированных портах не будет эффективной, если комбинированный порт работает в оптоволоконном режиме.

Правила именования физических портов следующие: формат имени интерфейса — eth-[слот]-[порт]; [слот] равен 0 для одно-юнитового коммутатора; при включении стекирования номер [слота] определяется в соответствии с конфигурацией. Номер [порта] начинается с 1 и увеличивается сверху вниз, слева направо. На следующем рисунке показано имя интерфейса устройства:

NOTE Для получения более подробной информации о типах и количестве интерфейсов, пожалуйста, обратитесь к техническим характеристикам продукта.

3.1.2 Настройка

3.1.2.1 Настройка состояния интерфейса

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включение интерфейса.

```
Switch#(config)# interface eth-0-1
Switch(config-if)# no shutdown
```

Шаг 3. Выключение интерфейса.

```
Switch(config-if)# interface eth-0-2
Switch(config-if)# shutdown
```

Шаг 4. Выйти из режима настройки.

```
Switch(config-if)# end
```

Шаг 5. Проверка.

Для отображения состояния интерфейсов используйте следующую команду:

```
Switch# show interface status
Port       Status     Duplex   Speed    Mode     Type
------------------------------------------------------------
eth-0-1    up         a-full   a-1000   access   1000BASE_T
eth-0-2    admin down auto     auto     access   1000BASE_T
```

3.1.2.2 Настройка скорости интерфейса

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и установите скорость.

Установите скорость интерфейса eth-0-1 на 100 Мбит/с.

```
Switch(config)# interface eth-0-1
Switch(config-if)# speed 100
Switch(config-if)# no shutdown
```

Установите скорость интерфейса eth-0-2 на 1000 Мбит/с.

```
Switch(config-if)# interface eth-0-2
Switch(config-if)# no shutdown
Switch(config-if)# speed 1000
```

Установите скорость интерфейса eth-0-3 в режим авто

```
Switch(config-if)# interface eth-0-3
Switch(config-if)# no shutdown
Switch(config-if)# speed auto
```

Шаг 3. Выйти из режима настройки.

```
Switch(config-if)# end
```

Шаг 4. Проверка.

Для отображения состояния интерфейсов используйте следующую команду:

```
Switch# show interface status
Port       Status     Duplex   Speed    Mode     Type
------------------------------------------------------------
```

```
eth-0-1    up          a-full   100       access   1000BASE_T
eth-0-2    up          a-full   1000      access   1000BASE_T
eth-0-3    up          a-full   a-1000    access   1000BASE_T
```

3.1.2.3 Настройка режима дуплекса для интерфейса

Устройство поддерживает 3 режима дуплекса:

- дуплекс: интерфейс может одновременно передавать и принимать пакеты;

- полудуплекс: интерфейс может одновременно или передавать или принимать пакеты;

- автосогласование: интерфейс должен согласовать со встречным интерфейсом режим дуплекса.

Пользователь может выбрать подходящий режим дуплекса в зависимости от состояния и нужд сети.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и установите режим дуплекса.

Установите режим полного дуплекса для интерфейса eth-0-1

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# duplex full
```

Установите режим полудуплекса для интерфейса eth-0-2

```
Switch(config-if)# interface eth-0-2
Switch(config-if)# no shutdown
Switch(config-if)# duplex half
```

Установите режим дуплекса для интерфейса eth-0-3 в значение auto

```
Switch(config)# interface eth-0-3
Switch(config-if)# no shutdown
Switch(config-if)# duplex auto
```

Шаг 3. Проверка.

Для отображения состояния интерфейсов используйте следующую команду:

```
Switch# show interface status
Port       Status     Duplex   Speed    Mode     Type
------------------------------------------------------------
eth-0-1    up         full     a-1000   access   1000BASE_T
eth-0-2    up         half     a-100    access   1000BASE_T
eth-0-3    up         a-full   a-1000   access   1000BASE_T
```

3.2 Настройка скорости группы интерфейсов

3.2.1 Общие положения

3.2.1.1 Описание функции

Интерфейсы в одной группе используют одинаковую скорость, которая называется «групповой скоростью» или «скоростью группы»; использование команды «групповой скорости» для любого интерфейса повлияет на все остальные интерфейсы в этой группе.

3.2.2 Настройка

3.2.2.1 Просмотр информации об идентификаторе группы интерфейса

Перед настройкой скорости интерфейса пользователям необходимо знать, какие интерфейсы принадлежат к одной группе интерфейсов; для интерфейсов, не входящих в группу, используется команда speed для установки режима скорости, а для интерфейсов, входящих в группу, используется команда group-speed для установки режима скорости.

Если group-id интерфейса равен 0, это означает, что интерфейс не принадлежит ни к одной группе интерфейсов. Если group-id интерфейса отличен от 0, то интерфейс принадлежит к группе интерфейсов; интерфейсы с одинаковым group-id принадлежат к одной группе интерфейсов..

Шаг 1. Отобразить информацию об идентификаторах групп интерфейсов.

Для отображения информации о группах интерфейсов используйте следующую команду:

```
Switch# show group-id info
Group Id Member Ports
-----------+--------------------
0            eth-0-1   eth-0-2
             eth-0-3   eth-0-4
             eth-0-5   eth-0-6
             eth-0-7   eth-0-8
             eth-0-9   eth-0-10
             eth-0-11  eth-0-12
             eth-0-13  eth-0-14
             eth-0-15  eth-0-16
             eth-0-17  eth-0-18
             eth-0-19  eth-0-20
             eth-0-21  eth-0-22
             eth-0-23  eth-0-24
             eth-0-25  eth-0-26
             eth-0-27  eth-0-28
             eth-0-29  eth-0-30
             eth-0-31  eth-0-32
```

```
            eth-0-33  eth-0-34
            eth-0-35  eth-0-36
            eth-0-37  eth-0-38
            eth-0-39  eth-0-40
            eth-0-41  eth-0-42
            eth-0-43  eth-0-44
            eth-0-45  eth-0-46
            eth-0-47  eth-0-48
--------------------------------
1           eth-0-49  eth-0-50
            eth-0-51  eth-0-52
Switch#
```

Шаг 2. Задайте скорость группы.

```
Switch# configure terminal
Switch(config)# interface eth-0-49
Switch(config-if)# group-speed 1000
% Warning: Speed of Port eth-0-49, eth-0-50, eth-0-51, eth-0-52 will all be
switched to 1000M after entering this CLI
```

3.3 Настройка интерфейсов уровня 3

3.3.1 Общие положения

3.3.1.1 Описание функции

Поддерживаются 3 типа интерфейсов Уровня 3:

- интерфейсы VLAN: Логический интерфейс с функциями уровня 3. Соединяет различные VLAN через IP-адрес на интерфейсе VLAN. Интерфейсы VLAN можно создавать и удалять;
- маршрутизируемые порты: это физические порты, настроенные в режиме уровня 3 с помощью команды no switchport в режиме конфигурации интерфейса;
- порты агрегации каналов уровня 3: Интерфейсы агрегации каналов, состоящие из маршрутизируемых портов.

Коммутатор третьего уровня может назначать IP-адрес каждому маршрутизируемому порту и интерфейсу VLAN. Всем интерфейсам третьего уровня требуется IP-адрес для маршрутизации трафика. В этом разделе показано, как настроить интерфейс третьего уровня и назначить ему IP-адрес.

3.3.2 Настройка

3.3.2.1 Настройка маршрутизируемого порта

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте IP-адрес.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 4. Проверка.

Используйте следующую команду для краткого отображения состояния интерфейсов:

```
Switch# show ip interface brief
Interface              IP-Address      Status                Protocol
eth-0-1                 1.1.1.1         up                      up
Switch# show ip interface
Interface eth-0-1
  Interface current state: UP
  Internet address(es):
    1.1.1.1/24 broadcast 1.1.1.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 01:00:00,  ARP retry interval 1s
  VRRP master of:  VRRP is not configured on this interface
```

3.3.2.2 Настройка интерфейсов VLAN

В этой главе описывается настройка и использование интерфейсов VLAN. На одном интерфейсе Ethernet можно настроить несколько виртуальных интерфейсов LAN (VLAN). После создания VLAN-интерфейса он функционирует так же, как и любой физический интерфейс, и его можно настраивать и отображать так же, как и любой физический интерфейс. Протоколы

маршрутизации, такие как RIP, OSPF и BGP, могут работать в сетях с использованием интерфейсов VLAN.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и задайте необходимые атрибуты порта.

```
Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 4. Войдите в режим настройки интерфейса VLAN и задайте IP-адрес.

```
Switch(config)# interface vlan10
Switch(config-if)# ip address 2.2.2.2/24
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 6. Проверка.

Используйте следующую команду для отображения краткого состояния интерфейсов:

```
Switch# show ip interface brief
Interface              IP-Address      Status                Protocol
vlan10                 2.2.2.2         up                    up

Switch# show ip interface
Interface vlan10
  Interface current state: UP
  Internet address(es):
    2.2.2.2/24 broadcast 2.2.2.255
  Joined group address(es):
    224.0.0.1
```

```
The maximum transmit unit is 1500 bytes
ICMP error messages limited to one every 1000 milliseconds
ICMP redirects are always sent
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are always sent
ARP timeout 01:00:00,  ARP retry interval 1s
VRRP master of :  VRRP is not configured on this interface
```

3.4 Настройка состояния Errdisable для интерфейсов

3.4.1 Общие положения

3.4.1.1 Описание функции

Errdisable — это механизм защиты системы путем отключения неисправного интерфейса. Если интерфейс переходит в состояние Errdisable, существует два способа его восстановления. Первый — настроить таймер восстановления интерфейса после перехода в Errdisable (настроить нужно до обнаружения ошибки); интерфейс будет восстановлен автоматически по истечении заданного времени. Но если ошибка Errdisable произошла раньше, а затем включено восстановление после Errdisable - автоматическое восстановление не произойдет. Второй способ — задать команду «no shutdown» для интерфейса, находящегося в состоянии Errdisable.

Кратковременное падение линка интерфейса — это потенциальная ошибка, вызванная аппаратными проблемами или проблемами канала связи. Администратор может настроить условия обнаружения изменения состояния канала связи интерфейса, чтобы исключить возникновение таких ложных ошибок.

3.4.1.2 Основные принципы

Терминология и определение

Статус Errdisable: Интерфейс, который отключается функцией Errdisable из-за нештатного события. В этом документе мы называем этот статус «статусом Errdisable».

Причина Errdisable: Нештатное событие называется «причиной Errdisable». Возможные причины перечислены в следующей таблице:

Таблица 3 – Причины возникновения состояния Errdisable

Name	Explanation
bpduguard	Система получила пакет BPDU на граничном порту STP.
bpduloop	Система получила пакет BPDU, отправленный локальным устройством.
link-monitor-failure	Обнаружено превышение порогового значения EFM.

oam-remote-failure	Обнаружена ошибка EFM.
port-security	Система получила пакет с недоверенным MAC-адресом
link-flap	Нестабильность соединения
monitor-link	Вышестоящий (встречный) порт отключен, связанный с ним порт переходит в состояние errdisable.
udld	Обнаружена однонаправленность соединения
fdb-loop	Петля и хаотичное переключение MAC-адреса
loopback-detection	Обнаружена петля сети
reload-delay	Интерфейс находится в режиме ожидания перезагрузки. Период задержки перезагрузки это интервал, в течение которого каналы перезагружаются после перезагрузки MLAG-соединения.
dual-active-conflict	Обнаружен конфликт в среде стекирования

3.4.2 Настройка

3.4.2.1 Настройка перехода в состояние Errdisable

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включить обнаружение сбоя соединения.

```
Switch(config)# errdisable detect reason link-flap
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Используйте следующую команду для отображения настройки errordisable：

```
Switch# show errdisable detect
ErrDisable Reason          Detection status
-----------------          ----------------
bpduguard                  Enabled
bpduloop                   Enabled
link-monitor-failure       Enabled
oam-remote-failure         Enabled
```

```
port-security             Enabled
link-flap                 Enabled
monitor-link              Enabled
udld                      Disabled
fdb-loop                  Disabled
loopback-detection        Enabled
reload-delay              Enabled
```

3.4.2.2 Настройка восстановления после перехода в Errdisable

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите параметр errdisable и установите интервал восстановления.

```
Switch(config)# errdisable recovery reason link-flap
Switch(config)# errdisable recovery interval 30
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Используйте следующую команду для отображения конфигурации восстановления при переходе в error disable：

```
Switch# show errdisable recovery
ErrDisable Reason         Timer Status
-----------------         --------------
bpduguard                 Disabled
bpduloop                  Disabled
link-monitor-failure      Disabled
oam-remote-failure        Disabled
port-security             Disabled
link-flap                 Enabled
udld                      Disabled
fdb-loop                  Disabled
loopback-detection        Disabled
Timer interval: 30 seconds
```

3.4.2.3 Настройка таймера перехода в Errdisable при падении линка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Опишите условия обнаружения падения линка.

```
Switch(config)# errdisable flap reason link-flap 20 60
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения конфигурации используйте следующую команду:

```
Switch# show errdisable flap
ErrDisable Reason         Flaps     Time (sec)
-----------------         ------    ----------
link-flap                 20        60
```

3.4.2.4 Проверка состояния Errdisable для интерфейсов

Администратор может проверить статус errdisable интерфейса с помощью трех команд.

Команда 1. Включение восстановление после перехода в errdisable.

При включении опции, команда отобразит остаток времени до восстановления. Если опция не включена, статус будет “unrecovery”.

```
Switch# show errdisable recovery
ErrDisable Reason         Timer Status
-----------------         --------------
bpduguard                 Disabled
bpduloop                  Disabled
link-monitor-failure      Disabled
oam-remote-failure        Disabled
port-security             Disabled
link-flap                 Enabled
udld                      Disabled
fdb-loop                  Disabled
loopback-detection        Disabled
Timer interval: 300 seconds
Interfaces that will be enabled at the next timeout:
Interface Errdisable Reason Time Left(sec)
--------- ----------------- --------------
eth-0-3   link-flap         25
```

Команда 2. Выключение восстановления после перехода в errdisable.

```
Switch# show errdisable recovery
ErrDisable Reason         Timer Status
```

```
-----------------       -------------
bpduguard               Disabled
bpduloop                Disabled
link-monitor-failure    Disabled
oam-remote-failure      Disabled
port-security           Disabled
link-flap               Disabled
udld                    Disabled
fdb-loop                Disabled
loopback-detection      Disabled
Timer interval: 300 seconds
```

Команда 3. Отображение краткой информации интерфейса для проверки состояния errdisable.

```
Switch# show interface status
Port       Status      Duplex   Speed    Mode    Type          Description
-------------------------------------------------------------------------------
eth-0-1    up          a-full   a-1000   TRUNK   1000BASE_SX
eth-0-2    down        auto     auto     TRUNK   Unknown
eth-0-3    errdisable a-full    a-1000   TRUNK   1000BASE_SX
eth-0-4    down        auto     auto     ACCESS  Unknown
```

3.4.3 FAQ

В следующем примере показано, как анализировать нештатное событие fdb-loop и link-flap.

3.4.3.1 fdb-loop

FDB-петля вызвана нестабильностью записей MAC-адресов. Коммутатор записывает исходный MAC-адрес, VLAN и принимающий интерфейс в таблицу MAC-адресов при обучении MAC-таблицы. Если пакеты с одним и тем же VLAN и одним и тем же MAC-адресом постоянно поступают с разных интерфейсов, таблица MAC-адресов будет постоянно обновляться. Это явление называется FDB-петлей (или нестабильностью MAC-адресов). FDB-петля может привести к ошибке пересылки трафика и сетевому шторму - зацикливанию трафика и петли в сети. Система контролирует частоту перезаписи MAC-адресов и, если она превышает определенный порог, срабатывает обнаружение FDB-петли. В случае включения перехода в Errdisable по причине FDB-петли, система случайным образом устанавливает один из интерфейсов, участников FDB-петли, в состояние Errdisable. В обратном случае, система просто записывает лог и больше ничего не делает.

Возможные причины появления петли:

- неправильное подключение сетевых кабелей приводит к образованию кольцевой сети, что вызывает частое переключение MAC-адресов;

- в сети присутствует множество виртуальных машин, которые мигрируют и часто переключаются, вызывая переключение MAC-адресов;

- в сети присутствует несанкционированный трафик, например, атаки с использованием MAC-адресов, осуществляемые неавторизованными пользователями и т.д;

- в сети присутствуют различные физические устройства, такие как тестеры, отправляющие трафик с одинаковым исходным MAC-адресом и VLAN.

Функция защиты от fdb-loop с помощью Errdisable по умолчанию отключена, чтобы предотвратить отключение встречного порта и потере соединения. Если необходимо исключить автоиспользование защиты на определенных каналах, можно использовать команду «errdisable fdb-loop trust». В этом случае, такой интерфейс не будет отключаться функциями Errdisable.

3.4.3.2 link-flap

«Нестабильность соединения» - это постоянное переключение интерфейса из состояния «включено» в состояние «выключено». Нестабильность соединения может привести к прерыванию работы сервиса. Типичная ситуация — отключение основного канала связи и переключение трафика на резервный. Если нестабилен основной канал, то основной и резервный каналы будут слишком часто переключаться. Для предотвращения нестабильности система проверяет частоту таких колебаний. Если частота колебаний превышает определенный порог, соединение помечается как нестабильное. Если команда «Errdisable reason link-flap enable» была использована, система устанавливает интерфейс в состояние Errdisable. В противном случае, система только записывает лог и ничего больше не делает.

Нестабильность соединения в основном вызвана физическими причинами, такими как проблемы с кабелем/ЦАП/оптическим волокном/модулем и т. д.

Защита соединений путем перевода в состояние Errdisable включена по умолчанию. Мы не рекомендуем пользователям отключать эту функцию.

3.5 Настройка таблицы MAC-адресов

3.5.1 Общие положения

3.5.1.1 Описание функции

Таблица MAC-адресов содержит информацию об адресах, которую использует коммутатор для переадресации трафика между портами. Таблица адресов включает следующие типы адресов:

- динамический адрес: мак адрес источника, распознанный коммутатором, который будет устаревать по истечении определенного времени, если он не будет заново обновлен. Поддерживается только режим обучения IVL;

- статический адрес: адрес источника, добавленный администраторами вручную.

Ниже приведено краткое описание терминов и понятий, используемых для описания таблицы MAC-адресов:

- IVL: (Independent VLAN Learning) независимое обучение VLAN. Если для заданного набора VLAN определенный MAC-адрес изучен в одном VLAN, он не может быть использован в любой другой VLAN в заданном наборе;

- SVL: (Shared VLAN Learning) общее обучение VLAN. Если для заданного набора VLAN в одном VLAN изучен отдельный MAC-адрес, он может быть использован при принятии решений о пересылке трафика в других VLAN в заданном наборе.

3.5.2 Настройка

3.5.2.1 Настройка времени устаревания адреса

Время устаревания не является точным. Если время устаревания установлено на N, то динамический адрес будет устаревать в течение интервала N~2N. Время устаревания по умолчанию составляет 300 секунд.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите время устаревания динамического адреса.

```
Switch(config)# mac-address-table ageing-time 10
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения времени устаревания используйте следующую команду:

```
Switch# show mac address-table ageing-time
MAC address table ageing time is 10 seconds
```

3.5.2.2 Настройка статического Unicast адреса

Unicast адрес может быть привязан только к одному порту. Согласно изображению, Mac-Da 0000.1234.5678 должен перенаправлять трафик через eth-0-1.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка статической таблицы MAC-адресов.

```
Switch(config)# mac-address-table 0000.1234.5678 forward eth-0-1 vlan 1
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения таблицы MAC-адресов используйте следующую команду:

```
Switch# show mac address-table
Mac Address Table
------------------------------------------
(*) - Security Entry
Vlan    Mac Address       Type       Ports
----   --------------   -------   --------
1       0000.1234.5678   static    eth-0-1
```

3.5.2.3 Настройка статического Multicast адреса

Multicast адрес может быть привязан к нескольким портам. Согласно изображению, Mac-Da 0100.0000.0000 может перенаправлять запросы через eth-0-1 и eth-0-2.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка статической таблицы MAC-адресов для многоадресной рассылки.

```
Switch(config)# mac-address-table 0100.0000.0000 forward eth-0-1 vlan 1
Switch(config)# mac-address-table 0100.0000.0000 forward eth-0-2 vlan 1
```

Шаг 3. Выходим из настроек режима.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения таблицы MAC-адресов используйте следующую команду:

```
Switch# show mac address-table
   Mac Address Table
------------------------------------------
(*) - Security Entry
Vlan    Mac Address       Type        Ports
----   --------------    -------     -------
```

```
1       0100.0000.0000    static      eth-0-1
                                      eth-0-2
```

3.5.2.4 Настройка фильтра по MAC-адресу

MAC-фильтр отбрасывает кадры, мак-адрес источника или назначения которых, прописаны в фильтре (их следует отбрасывать). MAC-фильтр имеет более высокий приоритет, чем MAC-адрес.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Добавьте unicast адрес, который необходимо удалить.

```
Switch(config)# mac-address-table 0000.1234.5678 discard
```

Шаг 3. Выход из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения фильтра MAC-адресов используйте следующую команду:

```
Switch# show mac-filter address-table
     MAC Filter Address Table
---------------------------------
 Current count       : 1
 Max count           : 128
 Left count          : 127
 Filter address list :
---------------------------------
 0000.1234.5678
```

3.5.2.5 Настройка фильтра по MAC-адресу для конкретной VLAN

MAC-фильтр отбрасывает кадры, для которых адрес источника или назначения прописаны в фильтре и при совпадении VLAN кадра с указанной VLAN в фильтре.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте VLAN.

```
Switch(config)# vlan 2
```

Шаг 3. Выход из режима просмотра VLAN.

```
Switch(config-vlan)# exit
```

Шаг 4. Добавьте unicast адрес, который необходимо удалить.

```
Switch(config)# mac-address-table 0000.1234.5678 discard vlan 2
```

Шаг 5. Выход из режима настроек.

```
Switch(config)# end
```

Шаг 6. Проверка.

Для отображения фильтра MAC-адресов со специальными VLAN используйте следующую команду:

```
Switch# show mac address-table blackhole
          Mac Address Table
------------------------------------------
(*)   - Security Entry      (M)   - MLAG Entry
(MO)  - MLAG Output Entry   (MI)  - MLAG Input Entry
(E)   - EVPN Entry          (EO)  - EVPN Output Entry
(EI)  - EVPN Input Entry
Vlan    Mac Address        Type         Ports
----    -----------        --------     -----
2       0000.1234.5678     blackhole    drop
```

3.6 Настройка VLAN

3.6.1 Общие положения

3.6.1.1 Описание функции

VLAN (виртуальная локальная сеть) — это коммутируемая сеть, которая логически сегментирует сеть на различные широковещательные домены, так что пакеты коммутируются только между портами, предназначенными для одной и той же VLAN. Каждый VLAN рассматривается как логическая сеть, и пакеты, отправляемые станциям, не принадлежащим к той же VLAN, должны перенаправляться только через маршрутизатор.

Ссылка на стандарт: IEEE 802.1Q

3.6.1.2 Основные принципы

Ниже приведено краткое описание терминов и понятий, используемых для описания VLAN:

- VID: Идентификатор VLAN;
- локальная сеть: Local Area Network;

- VLAN: Виртуальная локальная сеть;

- PVID: Port VID (идентификатор порта). Кадры без меток или с метками приоритета будут назначаться этому VID.

Помеченный кадр: тегированный кадр – Ethernet-кадр в заголовке которого указан 4-байтовый идентификатор VLAN, как показано на рисунке ниже:

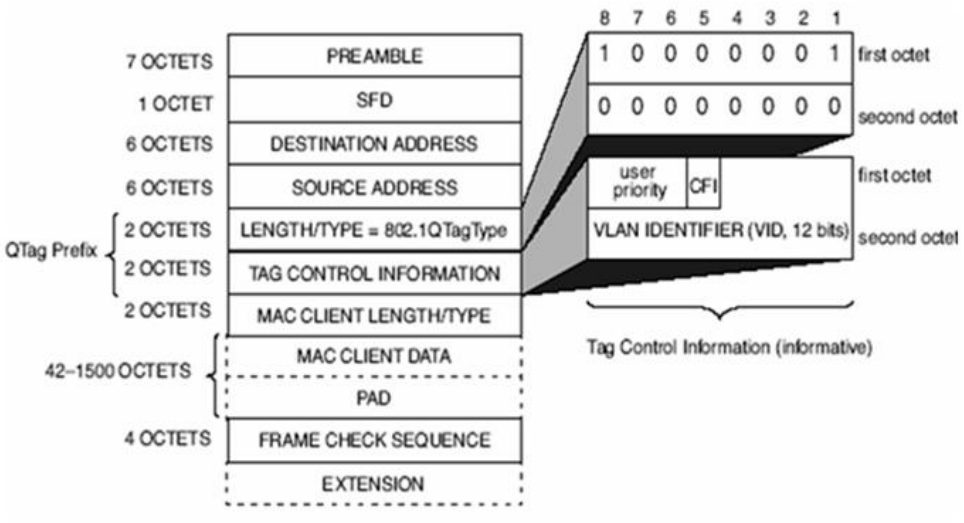


Рисунок 2 – Тэгированный кадр

Транковое порт: По этому каналу могут передаваться как тегированные и нетегированные кадры кадры. Транковый порт позволяет нескольким VLAN-сетям проходить через него, как показано на рисунке ниже:

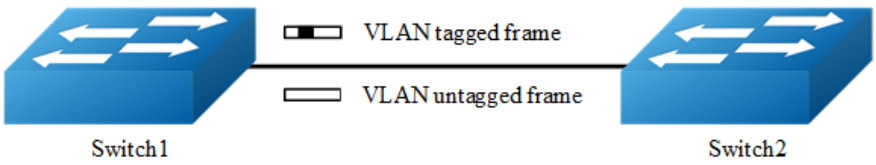


Рисунок 3 – Транковое соединение

Порт доступа: По этому порту можно передавать только нетегированные кадры. Порт доступа находится на границе сети, где подключаются конечные станции (см. рисунок ниже):

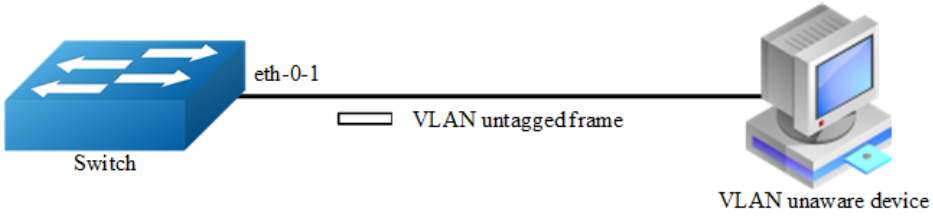


Рисунок 4 – Канал доступа

3.6.2 Конфигурация

3.6.2.1 Настройка порта доступа

Порт доступа принимает только кадры без влан-меток.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса, установите режим порта коммутатора и пропишите нужный VLAN.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
```

Шаг 4. Выход из настроек режима.

```
Switch(config-if)# end
```

Шаг 5. Проверка.

Для отображения информации об VLAN порта коммутатора используйте следующую команду:

```
Switch# show vlan brief
VLAN ID  Name            State   STP ID      Member ports
                                             (u)-Untagged, (t)-Tagged
======= ================ ======= =======  ========================
1       default          ACTIVE  0       eth-0-2(u) eth-0-3(u)
                                             eth-0-4(u) eth-0-5(u)
                                             eth-0-6(u) eth-0-7(u)
                                             eth-0-8(u) eth-0-9(u)
                                             eth-0-10(u) eth-0-11(u)
                                             eth-0-12(u) eth-0-13(u)
                                             eth-0-14(u) eth-0-15(u)
                                             eth-0-16(u) eth-0-17(u)
                                             eth-0-18(u) eth-0-19(u)
                                             eth-0-20(u) eth-0-21(u)
```

```
                                                    eth-0-22(u) eth-0-23(u)
2       VLAN0002          ACTIVE  0       eth-0-1(u)
```

3.6.2.2 Настройка транкового порта

Транковый порт принимает тегированные и нетегированные приоритетом кадры, а также передает как тегированные и нетегированные кадры. Если транковый порт получает нетегированные кадр, этому кадру присваивается VLAN, соответствующий PVID транкового порта; если кадр, отправленный с транкового порта, и VID кадра равен PVID транкового порта, этот кадр отправляется без метки VLAN.

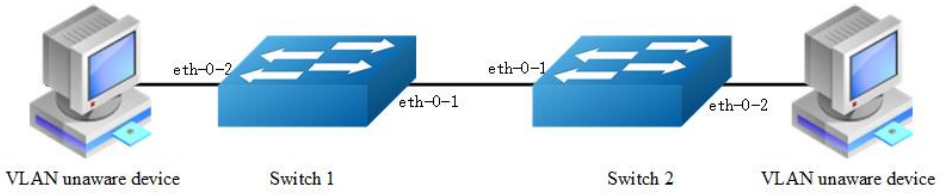


Рисунок 5 – Транковый линк (канал)

На рисунке выше показана топология сети. Следующие шаги по настройке одинаковы для коммутаторов Switch1 и Switch2.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10,20
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса, установите режим порта коммутатора и пропишите нужный VLAN.

Установите для интерфейса eth-0-1 режим работы интерфейса как транк, задайте собственный PVID равным 10 и разрешите все теги VLAN на этом интерфейсе:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# exit
```

Установите для интерфейса eth-0-2 режим работы коммутатора как «доступ» и назначьте VLAN ID интерфейсу eth-0-2:

```
Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

Шаг 4. Выход из режима настроек.

```
Switch(config-if)# end
```

Шаг 5. Проверка.

Для отображения информации об интерфейсе порта коммутатора используйте следующую команду:

```
Switch# show interface switchport
 Interface name           : eth-0-1
 Switchport mode          : trunk
 Ingress filter           : enable
 Acceptable frame types   : all
 Default Vlan             : 10
 Configured Vlans         :    1   10   20
 Interface name           : eth-0-2
 Switchport mode          : access
 Ingress filter           : enable
 Acceptable frame types   : vlan-untagged only
 Default Vlan             : 10
 Configured Vlans         :   10
```

Для отображения краткой информации о VLAN используйте следующую команду:

```
Switch# show vlan brief
VLAN ID  Name            State   STP ID      Member ports
                                             (u)-Untagged, (t)-Tagged
======= ================ ======= =======  ========================
1       default          ACTIVE  0       eth-0-1(t) eth-0-3(u)
                                         eth-0-4(u) eth-0-5(u)
                                         eth-0-6(u) eth-0-7(u)
                                         eth-0-8(u) eth-0-9(u)
                                         eth-0-10(u) eth-0-11(u)
                                         eth-0-12(u) eth-0-13(u)
                                         eth-0-14(u) eth-0-15(u)
                                         eth-0-16(u) eth-0-17(u)
                                         eth-0-18(u) eth-0-19(u)
                                         eth-0-20(u) eth-0-21(u)
                                         eth-0-22(u) eth-0-23(u)
10      VLAN0010         ACTIVE  0       eth-0-1(t) eth-0-2(u)
20      VLAN0020         ACTIVE  0       eth-0-1(t)
```

3.7 Настройка VLAN для передачи голоса

3.7.1 Общие положения

3.7.1.1 Описание функции

С развитием голосовых технологий использование IP-телефонов/интегрированных устройств доступа (IAD) становится все более распространенным в широкополосной сети. Голосовой и информационный трафик обычно присутствует в сети одновременно, тогда как голосовому трафику требуется более высокий приоритет для повышения производительности и снижения уровня потери пакетов.

Традиционный метод повышения качества голосового трафика заключается в использовании списков контроля доступа (ACL) для разделения голосовых пакетов и использовании QoS для обеспечения качества передачи.

Функция Voice VLAN позволяет идентифицировать голосовые пакеты по MAC-адресу источника, что делает настройку более удобной.

3.7.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# exit
```

Шаг 3. Настройка COS голосовой VLAN (необязательно).

Значение cos по умолчанию равно 5.

```
Switch(config)# voice vlan set cos to 7
```

Шаг 4. Настройте VLAN для передачи голоса и создайте для нее запись MAC-адреса.

```
Switch(config)# voice vlan 2
Switch(config)# voice vlan mac-address 0055.0000.0000 ffff.ff00.0000
description test
```

Шаг 5. Войдите в режим настройки интерфейса и включите VLAN для передачи голоса.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# voice vlan enable
Switch(config-if)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
```

Шаг 6. Проверка.

Отправьте пакет на eth-0-1, формат пакета следующий (приоритет в метке VLAN равен 0):

```
0x0000: 0000 0a02 0001 0055 0000 0011 8100 0002 ........k.......
0x0010: 0800 aadd aadd aadd aadd aadd aadd aadd .............. 0x0020: aadd
aadd aadd aadd aadd aadd aadd aadd .................. 0x0020: aadd aadd aadd
aadd aadd aadd aadd aadd ................ 0x0030: aadd aadd aadd aadd aadd
aadd ............
```

Получен пакет от eth-0-2, формат полученного пакета следующий (приоритет в метке VLAN равен 5):

```
    0x0000:  0000 0a02 0001 0055 0000 0011 8100 a002  ........k.......
    0x0010:  0800 aadd aadd aadd aadd aadd aadd aadd  ................
    0x0020:  aadd aadd aadd aadd aadd aadd aadd aadd  ................
    0x0030:  aadd aadd aadd aadd aadd aadd            ............
```

3.8 Настройка классификации VLAN

3.8.1 Общие положения

3.8.1.1 Описание функции

Классификация VLAN используется для определения конкретных правил направления пакетов в выбранные VLAN на основе критериев протокола или подсети. Наборы правил могут быть сгруппированы (одна группа на каждый интерфейс).

Правила классификации VLAN бывают трех типов: на основе MAC-адресов, на основе IP-адресов и на основе протоколов. Правило классификации VLAN на основе MAC-адресов классифицирует пакеты в указанную VLAN в соответствии с MAC-адресом источника входящих пакетов; правило классификации VLAN на основе IP-адресов классифицирует пакеты в соответствии с IP-адресом источника входящих пакетов; а правило классификации VLAN на основе протоколов классифицирует пакеты в соответствии с типом входящих пакетов на уровне 3. Поддерживаются следующие типы на уровне 3: ARP, IP (v4), MPLS, Mcast MPLS, PPPoE, RARP.

В одну и ту же группу классификации VLAN можно добавить правила классификации VLAN разных типов. Группа классификации VLAN может применяться только к одному порту коммутатора. На одном порту коммутатора может действовать только один тип правил классификации VLAN.

3.8.2 Настройка

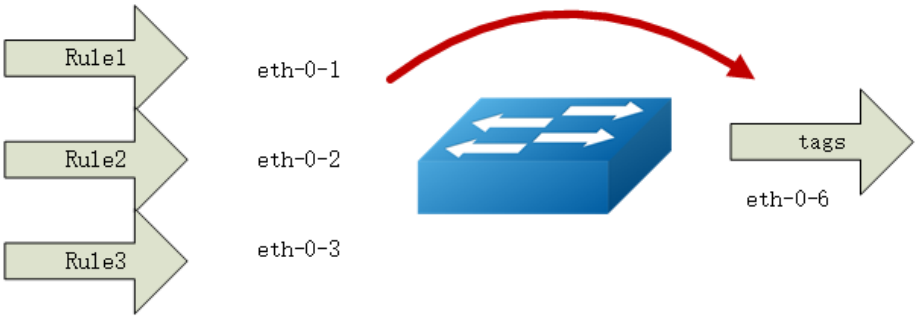


Рисунок 6 – Классификация VLAN

В этом примере конфигурации создаются три правила классификатора VLAN:

Правило 1 основано на MAC-адресах и классифицирует пакеты с MACSA 2222.2222.2222 во VLAN 5;

Правило 2 основано на IP-адресах и классифицирует пакеты, исходящие с IP-адреса 1.1.1.1/24, во VLAN 5;

Правило 3 основано на протоколе и классифицирует все ARP-пакеты во VLAN 5.

Добавьте правило 1, правило 2, правило 3 в группу 31. Затем примените группу 31 к трем интерфейсам: eth-0-1, eth-0-2, eth-0-3. Эти три интерфейса имеют разные типы классификации VLAN. eth-0-1 настроен по классификации VLAN на основе IP-адресов, это означает, что на этом интерфейсе могут действовать только правила на основе IP-адресов. eth-0-2 настроен по классификации VLAN на основе MAC-адресов, это означает, что на этом интерфейсе могут действовать только правила на основе MAC-адресов. eth-0-3 настроен по классификации VLAN на основе протоколов, это означает, что на этом интерфейсе могут действовать только правила на основе протоколов.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 5
Switch(config-vlan)# vlan 6
Switch(config-vlan)# exit
```

Шаг 3. Создайте правило классификатора VLAN и добавьте правила в группу.

```
Switch(config)# vlan classifier rule 1 mac 2222.2222.2222 vlan 5
Switch(config)# vlan classifier rule 2 ip 1.1.1.1 vlan 5
Switch(config)# vlan classifier rule 3 protocol arp vlan 5

Switch(config)# vlan classifier group 31 add rule 1
Switch(config)# vlan classifier group 31 add rule 2
Switch(config)# vlan classifier group 31 add rule 3
Switch(config)# arp as-layer-3 enable
```

Шаг 4. Примените группу классификаторов VLAN к интерфейсу.

интерфейс eth-0-1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 6
Switch(config-if)# switchport access allowed vlan add 5
Switch(config-if)# vlan classifier activate 31 based ip
Switch(config-if)# exit
```

интерфейс eth-0-2:

```
Switch(config)# interface eth-0-2
Switch(config-if)# switchport access vlan 6
Switch(config-if)# switchport access allowed vlan add 5
Switch(config-if)# vlan classifier activate 31 based mac
Switch(config-if)# exit
```

интерфейс eth-0-3:

```
Switch(config)# interface eth-0-3
Switch(config-if)# switchport access vlan 6
Switch(config-if)# switchport access allowed vlan add 5
Switch(config-if)# vlan classifier activate 31 based protocol
Switch(config-if)# exit
```

интерфейс eth-0-6:

```
Switch(config)# interface eth-0-6
Switch(config)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 5
Switch(config-if)# exit
```

Шаг 5. Выход из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Проверьте правила классификатора VLAN:

```
Switch# show vlan classifier rule
vlan classifier rule 1 mac 2222.2222.2222
vlan 5vlan classifier rule 2 ip 1.1.1.1 vlan 5
vlan classifier rule 3 protocol arp vlan 5
```

Проверьте группу классификатора VLAN:

```
Switch# show vlan classifier group
vlan classifier group 31 add rule 1
vlan classifier group 31 add rule 2
vlan classifier group 31 add rule 3
```

Проверьте интерфейс классификатора VLAN:

```
Switch# show vlan classifier interface grou
vlan classifier group 31 on interface eth-0-2, based mac
vlan classifier group 31 on interface eth-0-1, based ip
vlan classifier group 31 on interface eth-0-3, based protocol
```

3.9 Настройка VLAN Mapping (преобразование VLAN ID)

3.9.1 Общие положения

3.9.1.1 Описание функции

У клиентов интернет-провайдеров часто возникают специфические требования к идентификаторам VLAN. Требуемые разными клиентами VLAN в одной и той же сети могут пересекаться, и трафик клиентов через инфраструктуру может быть смешанным. VLAN Mapping предназначен для преобразования идентификаторов VLAN (VID). Это может быть необходимо для предотвращения их совпадения с VID других сетей при прохождении трафика через общие узлы. После преобразования идентификация трафика из разных VLAN с идентичными VID будет различаться.

При помощи данной функции поставщики услуг могут предоставлять услуги клиентам, у которых уже есть свои собственные VLAN или использовать одну VLAN для обслуживания клиентов, имеющих несколько VLAN.

Туннелирование 802.1Q расширяет пространство VLAN за счет использования иерархии VLAN-in-VLAN и повторной маркировки пакетов. Функция “VLAN Mapping” увеличивает возможное количество VLAN за счет использования иерархии “VLAN-in-VLAN” - повторного тегирования поверх тегов VLAN, записанных ранее. Таким образом, количество передаваемых через коммутатор VLAN может достигать 4096 × 4096. При использовании функции “VLAN Mapping” VLAN-тег первичной VLAN инкапсулируется в тег общедоступной VLAN, и пакеты с двумя тегами будут передаваться по магистральной сети. Инкапсулированный VLAN-тег будет скрыт, для передачи будет использоваться только тег общедоступной VLAN. Благодаря разделению потока

данных, VLAN-тег первичной сети передается прозрачно, и различные теги VLAN могут быть использованы повторно.

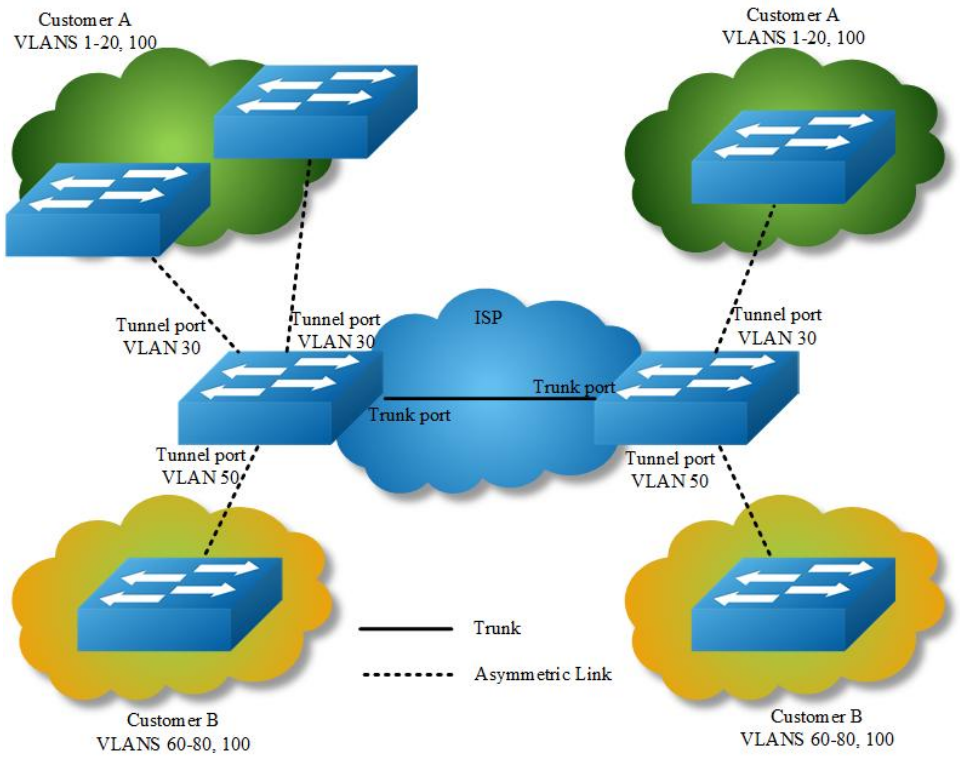


Рисунок 7 – QinQ туннелирование

Использование туннелирования 802.1Q расширяет доступное количество тегов VLAN. Поддерживаются два типа туннелирования 802.1Q: базовое туннелирование 802.1Q и селективное туннелирование 802.1Q. Базовое туннелирование 802.1Q основано на маркировке портов, и все данные будут инкапсулированы в общий тег VLAN одного и того же порта, поэтому этот тип имеет большие ограничения на практике. В то время как селективное туннелирование 802.1Q позволяет разделять потоки данных и инкапсулировать разные теги VLAN на основе разных данных.

3.9.2 Настройка

3.9.2.1 Настройка трансляции VLAN

Рисунок 8 – Преобразование VLAN

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 2,3
Switch(config-vlan)# exit
```

Шаг 3. Создайте EVC и настройте dot1q сопоставление VLAN.

```
Switch(config)# ethernet evc evc_c1
Switch(config-evc)# dot1q mapped-vlan 2
Switch(config)# ethernet evc evc_c2
Switch(config-evc)# dot1q mapped-vlan 3
```

Шаг 4. Создайте таблицу сопоставления VLAN и свяжите VLAN и EVC.

```
Switch(config)# vlan mapping table vm
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1
Switch(config-vlan-mapping)# raw-vlan 20 evc evc_c2
Switch(config-vlan-mapping)# exit
```

Шаг 5. Включите трансляцию VLAN на интерфейсе и примените таблицу сопоставления VLAN.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk vlan-translation
Switch(config-if)# switchport trunk vlan-translation mapping table vm
Switch(config-if)# switchport trunk allowed vlan add 2,3

Switch(config-if)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2,3
Switch(config-if)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Для отображения информации об интерфейсе порта коммутатора используйте следующую команду:

```
Switch# show interface switchport interface eth-0-1
Interface name           : eth-0-1
 Switchport mode          : trunk
 VLAN traslation          : enable
 VLAN mapping table       : vm
 Ingress filter           : enable
 Acceptable frame types   : all
 Default Vlan             : 1
 Configured Vlans         : 1    2    3
```

Для отображения информации из таблицы сопоставления VLAN используйте следующую команду:

```
Switch# show vlan mapping table
Table Name         EVC Name           Mapped VLAN Raw VLAN
 ================ ================  =========== ======================
vm                 evc_c1             2           10
                   evc_c2             3           20
```

3.9.2.2 Настройка туннелирования 802.1q (базовое туннелирование 802.1Q)

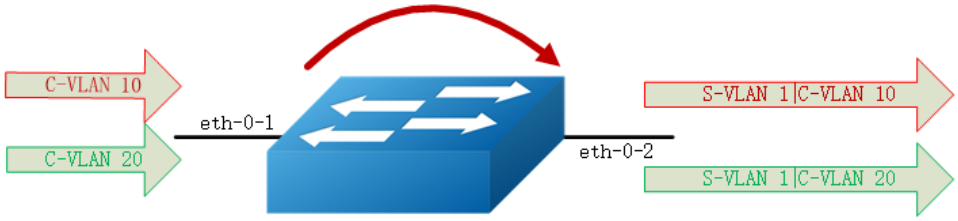


Рисунок 9 – QinQ Туннель

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и установите режим порта коммутатора.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode dot1q-tunnel
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 4. Проверка.

В этом примере показано, как настроить порт коммутатора для работы с базовым туннелем dot1q. Вы можете использовать команду «show the configuration on the switchport»:

```
Switch# show interface switchport interface eth-0-1
Interface name            : eth-0-1
 Switchport mode          : dot1q-tunnel(basic)
 Ingress filter           : enable
 Acceptable frame types   : all
 Default Vlan             : 1
 Configured Vlans         : 1
```

3.10 Настройка агрегации каналов

3.10.1 Общие положения

3.10.1.1 Описание функции

3.10.1.2 Аббревиатуры

Сокращение	Описание
LACP	Протокол управления агрегацией каналов
AGG Group	Группа агрегации
AGG IF	Интерфейс агрегации
Member IF	Интерфейс участника группы

3.10.1.3 Описание

Технология агрегации каналов (Link Aggregation) заключается в объединении нескольких физических интерфейсов Ethernet в один логический интерфейс, образующий группу агрегации; несколько физических интерфейсов в одной группе агрегации логически рассматриваются как один интерфейс. Использование технологии агрегации каналов позволяет увеличить пропускную способность канала за счет объединения нескольких физических интерфейсов в один логический интерфейс без модернизации оборудования. При этом, помимо увеличения пропускной способности, агрегация каналов использует механизм резервирования канала, что эффективно повышает надежность взаимодействия между устройствами.

Несколько интерфейсов Ethernet образуют группу агрегации. Интерфейсы Ethernet являются членами группы. Каждая группа агрегации соответствует логическому интерфейсу, который называется интерфейсом агрегации. Группа агрегации и интерфейс агрегации должны

использовать один и тот же индекс, например: группа агрегации 1 соответствует интерфейсу агрегации 1.

Типы агрегации групп/интерфейсов:

- группа/интерфейс агрегации уровня 2: Все интерфейсы- участники являются интерфейсами уровня 2;
- группа/интерфейс агрегации уровня 3: Все интерфейсы-участники являются интерфейсами уровня 3.

Режимы агрегации каналов.

Существует два режима агрегации каналов. Преимущества каждого режима следующие:

- статический режим агрегации: после настройки, если статус участника активен, интерфейс агрегации может перейти в активный режим;
- Iинамический режим агрегации: использование протокола LACP для динамического включения или исключения интерфейса в зависимости от обстоятельств.

NOTE Группы агрегации со статическим режимом называются статическими группами агрегации; группы агрегации с динамическим режимом называются динамическими группами агрегации.

Состояние интерфейса пользователя:

- W (ожидание): в режиме динамической агрегации этот участник не может пересылать трафик данных;
- S (приостановка): в режиме динамической агрегации этот участник не может пересылать трафик данных;
- B (активен): этот участник может пересылать трафик данных;
- D (выключен): интерфейс находится в состоянии "down".

NOTE Интерфейс агрегации активен, когда хотя бы один участник находится в статусе «активен» (bundle).

3.10.1.4 Предыстория

Существующая проблема

По мере постоянного роста сетей пользователи предъявляют все более высокие требования к пропускной способности и надежности каналов связи. В традиционных технологиях всегда происходит замена интерфейсных плат на платы с более высокой скоростью или устройств на другие, поддерживающих более высокие скорости работы интерфейсных плат; однако такой подход обходится дороже и не отличается гибкостью.

Преимущества агрегации каналов

Технология агрегации каналов (Link Aggregation) заключается в объединении нескольких физических интерфейсов Ethernet в один логический интерфейс, образующий группу агрегации;

несколько физических интерфейсов в одной группе агрегации логически рассматриваются как один интерфейс. Использование технологии агрегации каналов позволяет увеличить пропускную способность канала за счет объединения нескольких физических интерфейсов в один логический интерфейс без модернизации оборудования. При этом, помимо увеличения пропускной способности, агрегация каналов использует механизм резервирования, что эффективно повышает надежность сети.

Преимущества агрегации ссылок:

- увеличение пропускной способности: несколько физических интерфейсов логически объединяются в один интерфейс; пропускная способность агрегированного интерфейса равна сумме пропускных способностей каждого из входящих в него интерфейсов;
- резервирование каналов: при отказе одного из каналов трафик может быть перенаправлен на другие работоспособные каналы, что повышает общую надежность интерфейса агрегации каналов;
- балансировка нагрузки: внутри одной группы агрегации можно обеспечить балансировку нагрузки между отдельными каналами.

3.10.1.5 Описание принципа

3.10.1.6 Протокол LACP

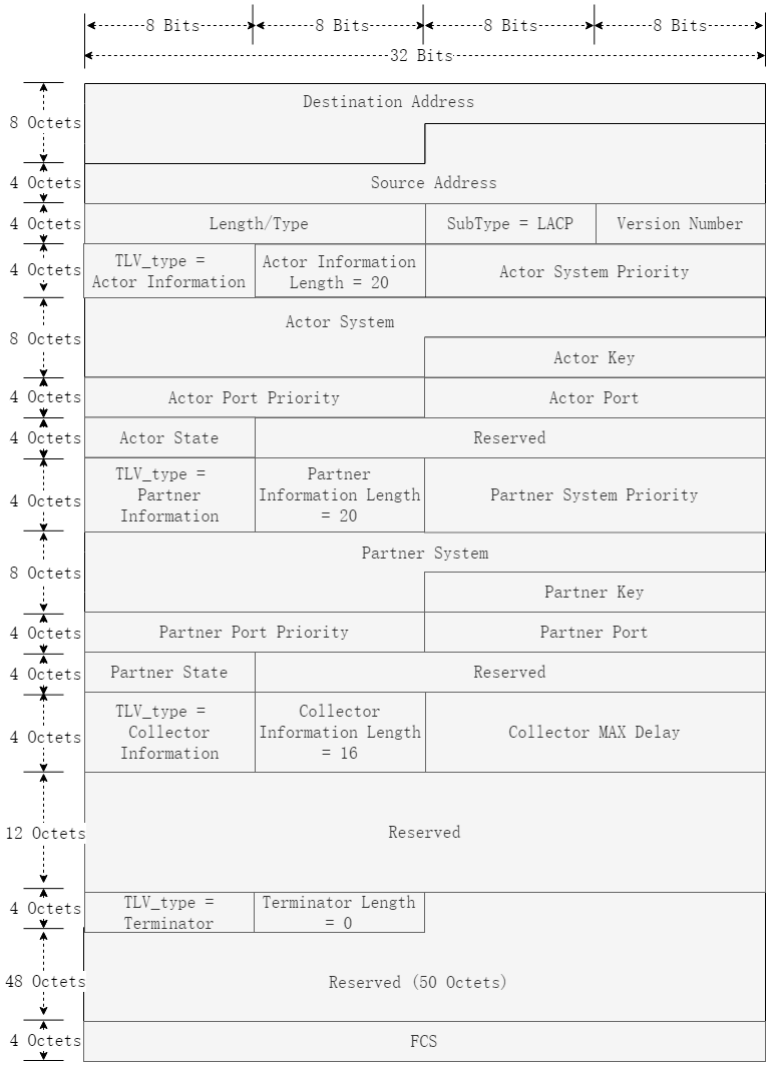


Рисунок 10 – Структура LACPDU пакета

Таблица 4 – Поля и разделы пакета

Поле	Длина	Описание
Destination Address	6 Байт	Адрес назначения, многоадресный адрес (01-80-C2-00-00-02)
Source Address	6 Байт	Исходный адрес, MAC-адрес передающего интерфейса.
Length/Type	2 Байта	Тип протокола 0x8809
Subtype	1 Байт	Подтип. 0x01 - LACP пакет
Version Number	1 Байт	Версия протокола 0x01

Поле	Длина	Описание
TLV_type	1 Байт	0x00: Terminator 0x01: Actor 0x02: Partner 0x03: Collector
Actor_Information_Length	1 Байт	Длинна поля «actor». 20 Байт
Actor_System_Priority	2 Байта	Локальный приоритет системы. Настраиваемый. По умолчанию 32768 (0x8000).
Actor_System	6 Байт	ID системы, совпадает с локальным MAC-address
Actor_key	2 Байта	Ключевое значение, генерируемое при конфигурации интерфейса. Необходим для присоединения участника к группе агрегации. Конфигурация интерфейса содержит индекс группы агрегации для присоединения к MLAG.
Actor_Port_Priority	2 Байта	Системный приоритет интерфейса. Настраиваемый. По умолчанию 2048 (0x800).
Actor_Port	2 Байта	Индекс интерфейса, в соответствии с выбранным интерфейсом коммутатора.
Actor_State	1 Байт	Информация о локальных состояниях, допустимый диапазон значений 0-7. 0 (LACP_Activity): пассивное/активное состояние управления каналом интерфейса. 0 - пассивное, 1 - активное. 1 (LACP_Timeout): значение таймаута. 0 - длительный таймаут, 1 - короткий таймаут. 2 (Агрегация): пропускная способность интерфейса для агрегации. 1 -интерфейс интегрируем. 0 - независимый канал, не интегрируемый. 3 (Синхронизация): агрегируется ли интерфейс. 1 - канал находится в состоянии IN_SYNC, интерфейс находится в правильной группе агрегации. 0 - канал находится в состоянии OUT_OF_SYNC, интерфейс не находится в правильной группе агрегации. 4 (Передача данных): 1 - прием данных разрешен на текущем интерфейсе. 0 - прием отключен на текущем интерфейсе. 5 (пересылка данных): 1 - передача разрешена на текущем интерфейсе. 0 - передача отключена на текущем интерфейсе. 6: По умолчанию: 1 - информация о партнере, используемая Actor, взята из настроенного значения по умолчанию. 0 - информация о партнере, используемая Actor, взята из пакетов LACPDU. 7 (Истек срок действия): 1 - время приема от Actor истекло. 0 - время приема от Actor не истекло.
Reserved	3 Байта	Зарезервировано для отладки

Поле	Длина	Описание
Partner_Information_Length	1 Байт	Размер информации о партнере. Информация об удаленной системе/интерфейсе, полученная интерфейсом, которая соответствует полю "участник". При инициализации системы поле "партнер" заполняется "0". После получения удаленной информации поле "партнер" обновляется.
Partner_System_Priority	2 Байта	Приоритет удаленной системы
Partner_System	6 Байт	Системный индекс удаленной системы, совпадающий с MAC-адресом удаленного устройства.
Partner_key	2 Байта	Код-значение удаленного интерфейса
Partner_Port_Priority	2 Байта	Приоритет удаленного интерфейса
Partner_Port	2 Байта	Индекс удаленного интерфейса
Partner_State	1 Байт	Статус Партнера
Reserved	2 Байта	Зарезервированное поле
Collector_Information_Length	1 Байт	Длина информации о сборщике: 0x10
CollectorMaxDelay	2 Байта	Максимальная задержка. По умолчанию 0xffff.
Reserved	12 Байт	Зарезервированное поле
Reserved	50 Байт	Зарезервированное поле, заполненное «0».
FCS	4 Байта	Поле проверки избыточности

Динамический режим агрегации реализуется с помощью протокола LACP. Содержание протокола LACP и механизм работы динамического режима агрегации описаны ниже:

Протокол LACP, основанный на стандарте IEEE802.3ad, предназначен для реализации динамической агрегации каналов. Устройства, работающие с протоколом LACP, используют LACPDU для обмена информацией об агрегации каналов.

Интерфейс участника группы агрегации может отправлять/получать LACPDU (блок данных протокола управления агрегацией каналов) для передачи локальной информации удаленному устройству. После получения LACPDU удаленное устройство сравнивает информацию с данными других участников и в соответствии устанавливает статус участника.

Режим работы LACP: активный и пассивный режимы.

По крайней мере одно устройство должно находиться в режиме ACTIVE. Только устройство в режиме ACTIVE может отправлять LACPDU. Устройство в режиме PASSIVE может отвечать на LACPDU. Если оба устройства находятся в режиме PASSIVE, отправка LACPDU невозможна.

Протокол LACP задает приоритет. Приоритет включает в себя системный приоритет (устройства) и приоритет интерфейса. Чем меньше число, тем выше приоритет.

- системный приоритет: Устройство с более высоким приоритетом может принимать решения о включении/исключении интерфейса.

- приоритет интерфейса: интерфейс с более высоким приоритетом может быть выбран в первую очередь.

3.10.1.7 Агрегация каналов

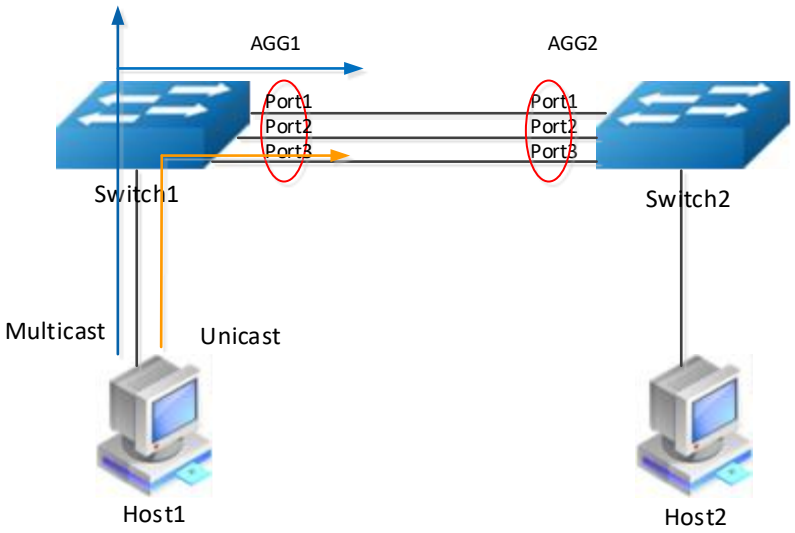


Рисунок 11 – Агрегация каналов

Следующее пояснение описывает процесс пересылки данных при агрегации каналов:

- агрегационный интерфейс agg1 коммутатора Switch1 соединяется с агрегационным интерфейсом agg2 коммутатора Switch2, образуя агрегационный канал между двумя коммутаторами;

- интерфейс агрегации рассматривается логически как интерфейс; при пересылке широковещательного сообщения на agg1 отправляется только одно широковещательное сообщение, после чего стратегия балансировки нагрузки определяет, через какой физический интерфейс будет осуществлена пересылка;

- после того, как сообщение достигает agg2, Switch2 узнает MAC-адрес, и соответствующий логический интерфейс становится agg2 (не только физический интерфейс, принимающий сообщение);

- агрегационный канал, показанный на рисунке, состоит из трех физических каналов. При оптимальной нагрузке пропускная способность каналов Switch1 и Switch2 будет равна сумме пропускных способностей всех трех физических каналов.

3.10.1.8 Резервирование каналов

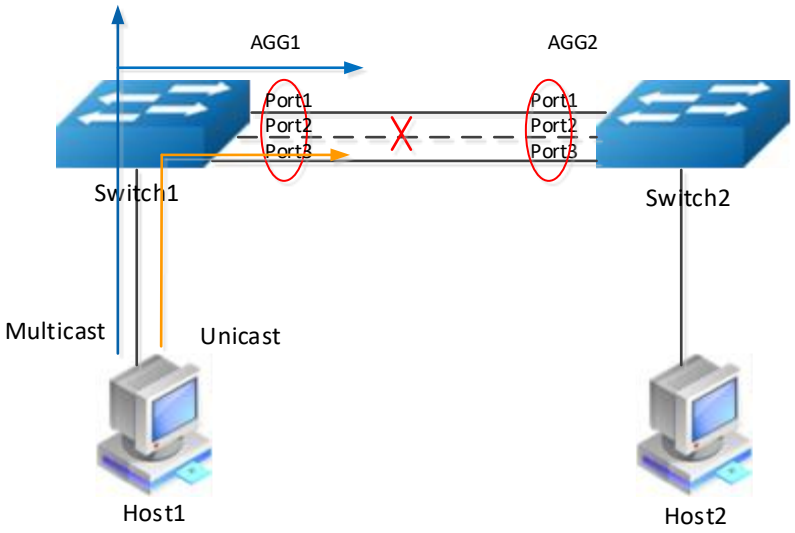


Рисунок 12 – Резервирование каналов

Как показано на рисунке, при выходе из строя одного из каналов связи между коммутаторами Switch1 и Switch2, если остальные каналы работают нормально, агрегированный канал продолжает нормально передавать сетевой трафик; просто пропускная способность агрегированного канала снижается.

3.10.1.9 Балансировка нагрузки

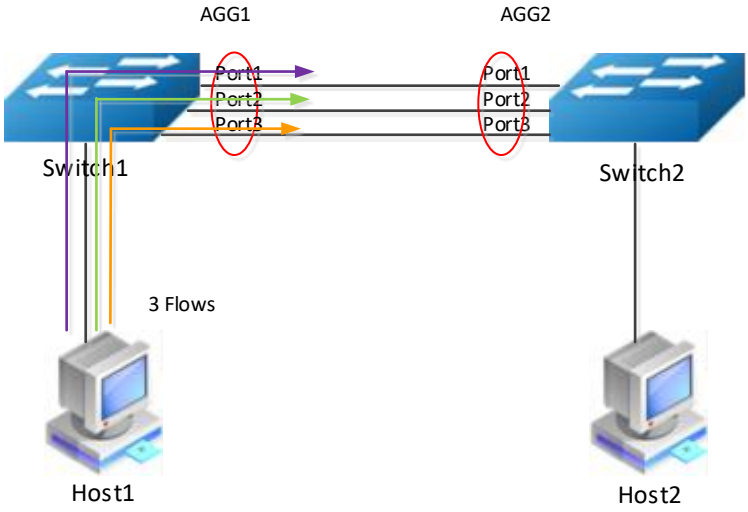


Рисунок 13 – Балансировка нагрузки

Как показано на рисунке, трафик, перенаправляемый на agg1, будет проходить через различные физические интерфейсы для обеспечения балансировки нагрузки трафика.

Существует четыре режима балансировки нагрузки: статический (по умолчанию), динамический, поочередный и отказоустойчивый.

Статический режим: режим балансировки нагрузки (на основе хэша) вычисляет значение хэша в соответствии с хэш-ключом сообщения (по умолчанию хэш-ключ — это IP-адрес получателя, IP-адрес источника, MAC-адрес получателя, MAC-адрес источника и IP-протокол); разные значения хэша соответствуют разным каналам связи, что обеспечивает балансировку нагрузки. Если хэш-ключи тестируемого трафика одинаковы, то в этом случае балансировка нагрузки не достигается.

Динамический режим: балансировка нагрузки по потокам. Если на порту 1 трафик меньше, чем на портах 2 и 3, новый поток будет распределен на порт 1. Но если на устройство одновременно поступает несколько потоков, они могут быть распределены на один и тот же порт, что приведет к дисбалансу.

Поочередный: балансировка нагрузки в режиме распределения. Если первый пакет перенаправляется на порт 1, второй пакет перенаправляется на порт 2, третий — на порт 3 и так далее. Проблема в том, что, если задержка для каждого канала разная, пакеты на приеме могут оказаться в неправильном порядке.

Устойчивый режим: балансировка нагрузки по хешу. Отличие от статического режима заключается в следующем: в устойчивом режиме при сбое канала система пересчитывает значение хеша для трафика на неисправном канале и перенаправляет трафик на рабочий канал.

3.10.1.10 Основные функции

Взвешенная агрегация каналов

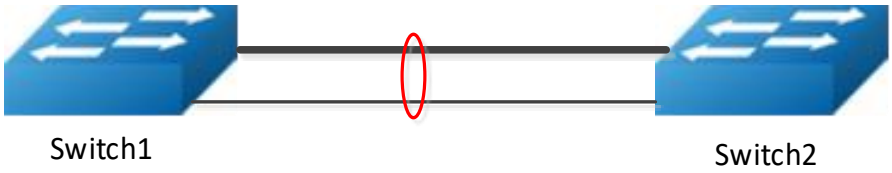


Рисунок 14 – Взвешенное агрегирование каналов

Коммутаторы Switch1 и Switch2 соединены двумя физическими каналами связи. Эти два физических канала образуют агрегирующий канал.

В некоторых случаях пропускная способность двух каналов различается, поэтому для обеспечения рационального использования полосы пропускания необходимы разные весовые коэффициенты.

В отличие от традиционной агрегации каналов, взвешенная агрегация каналов устраняет ограничения, связанные с типом интерфейса участника, и поддерживает агрегацию интерфейсов с разной скоростью. Использование весовых параметров обеспечивает рациональное распределение трафика между участниками.

Настройка весовых коэффициентов интерфейса действительна для статических AGG и LACP.

Агрегация каналов в режиме "ведущий-ведомый"

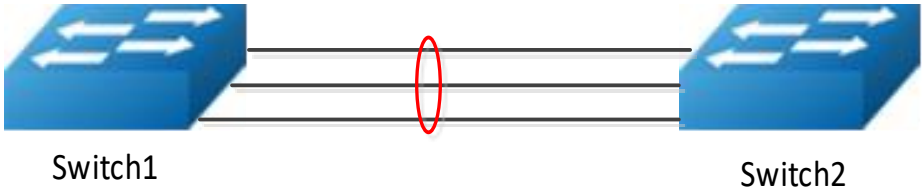


Рисунок 15 – Агрегация каналов в режиме "ведущий-ведомый"

Коммутаторы Switch1 и Switch2 соединены агрегирующим каналом. Для предотвращения обрыва сети или перегрузки из-за отказа одного канала, системе необходим резервный канал.

Как показано на рисунке, между коммутаторами Switch1 и Switch2 имеется три физических канала связи. Два из них являются рабочими, а один — резервным. В случае отказа какого-либо из рабочих каналов, пакеты могут передаваться через резервный канал.

По сравнению с традиционной агрегацией каналов, агрегация каналов в режиме «ведущий-ведомый» имеет следующие преимущества: в традиционной агрегации каналов каналы являются резервными, и при возникновении сбоя трафик неисправного канала должен быть распределен на другие работающие каналы. При высокой загрузке сети предотвратить потерю пакетов невозможно.

Администратор может настроить M рабочих каналов и N резервных каналов, чтобы обеспечить разумное соотношение M:N.

Агрегация каналов в режиме "ведущий-ведомый" допустима только для протокола LACP.

3.10.2 Ограничения и меры предосторожности

3.10.2.1 Свойство интерфейса

Агрегационный интерфейс — это логический интерфейс, часть атрибутов которого должна быть одинаковой для всех интерфейсов. Поэтому, когда участник присоединяется к агрегационному интерфейсу, он должен следовать следующим правилам:

Таблица 5 – Правила агрегации

Атрибут	Описание
Интерфейс	Все типы интерфейсов участников (уровень 2 / уровень 3) должны быть одинаковыми. Смешивание уровней 2 и 3 не допускается. Идентификатор VLAN интерфейса уровня 2 должен быть одинаковым
DHCP	Интерфейс с включенными функциями DHCP relay/DHCP snooping/DHCP server не может быть подключен к интерфейсу агрегации
Конфигурация порта	Конфигурация портов должна быть одинаковой для каждого интерфейса-участника
Private VLAN	Тип (частной VLAN / публичной VLAN) должен быть одинаковым для каждого интерфейса-члена группы

Атрибут	Описание
Error disable	Настройки Error disable должна быть одинаковой для каждого интерфейса участника
MTU	Значение MTU должно быть одинаковым для каждого интерфейса-участника и интерфейса агрегации
EFD	Статус EFD (включено/выключено) должен быть одинаковым для каждого интерфейса участника и интерфейса агрегации
MAC Learning	Статус обучения MAC-адресов (включено/выключено) должен быть одинаковым для каждого интерфейса-члена и интерфейса агрегации
Port Block	Конфигурация блокировки портов должна быть одинаковой для каждого интерфейса-участника и интерфейса агрегации

3.10.2.2 Функции не поддерживаемые одновременно с использованием агрегации каналов

Часть функций не поддерживается в интерфейсе агрегации или интерфейсе участников (см. таблицу ниже).

Таблица 6 – Не поддерживыемый функционал

Функция	Описание
IP Source guard	Не поддерживается на интерфейсе агрегации или интерфейсе участнике
IVI	Не поддерживается на интерфейсе агрегации или интерфейсе участнике
Loop back detection	Не поддерживается на интерфейсе агрегации или интерфейсе участнике
Monitor link	Интерфейс с включенной функцией НЕ может присоединиться к агрегации
G.8031/G.8032/ERPS	Интерфейс с включенными протоколами G.8031/G.8032/ERPS не может быть подключен к агрегации. Протоколы G.8031/G.8032/ERPS могут быть включены на интерфейсе агрегации
PBR	Интерфейс с включенной функцией не может присоединиться к агрегации. Функция PBR может быть включена на интерфейсе агрегации
QOS policy map	Интерфейс с включенной картой политик QoS НЕ может присоединиться к агрегации. Карту политик QoS можно включить на интерфейсе агрегации
Port security	Интерфейс с включенной опцией не может присоединиться к агрегации. Опцию можно включить на интерфейсе агрегации
Voice VLAN	Интерфейс с включенной опцией не может присоединиться к агрегации. Опцию можно включить на интерфейсе агрегации

3.10.2.3 Ограничение по техническим характеристикам

Максимальное количество групп/интерфейсов агрегации и максимальное количество интерфейсов-участников в каждой группе ограничены в соответствии с системными ресурсами.

Система поддерживает 5 режимов масштабирования агрегации (максимальное количество групп/интерфейсов агрегации и количество интерфейсов-участников в каждой группе). После изменения режима он вступит в силу после перезагрузки устройства.

Пять режимов описаны следующим образом.

Таблица 7 – Режимы масштабирования агрегации

Режим	Описание
group-mode flexible	Режим по умолчанию. Поддерживается до 64 групп агрегации (группа 0 зарезервирована). Максимальное количество интерфейсов-членов в группе настраивается. По умолчанию поддерживается до 16 интерфейсов-участников.
group-mode 56	Поддерживается до 56 групп агрегации (группа 0 зарезервирована). Поддерживается до 16 интерфейсов участников.
group-mode 32	Поддерживается до 32 групп агрегации (группа 0 зарезервирована). Поддерживается до 32 интерфейсов участников.
group-mode 16	Поддерживается до 16 групп агрегации (группа 0 зарезервирована). Поддерживается до 64 интерфейсов участников.
group-mode 8	Поддерживается до 8 групп агрегации (группа 0 зарезервирована). Поддерживается до 128 интерфейсов участников.

Фактические технические характеристики, зависят от аппаратных условий, см. в соответствующем разделе.

3.10.3 Конфигурация

3.10.3.1 Настройка статической группы каналов

3.10.3.2 Топология

3.10.3.3 Этапы настройки

Конфигурации коммутаторов Switch1 и Switch2 приведены ниже:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и добавьте интерфейс в группу каналов.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# static-channel-group 1
Switch(config-if)# exit
Switch(config)# interface eth-0-2
Switch(config-if)# static-channel-group 1
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface eth-0-3
Switch(config-if)# static-channel-group 1
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения информации о группе каналов используйте следующую команду:

```
Switch1# show channel-group summary
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
     macsa
Flags:  s - suspend           T - standby
        D - down/admin down   B - in Bundle
        R - Layer3            S - Layer2
        w - wait              U - in use
Mode:   SLB  - static load balance
        DLB  - dynamic load balance
        SHLB - self-healing load balance
        RR   - round robin load balance
Aggregator Name  Mode      Protocol     Ports
----------------+---------+------------+-------------------------------------
----------
agg1(SU)         SLB       Static         eth-0-1(B) eth-0-2(B) eth-0-3(B)
```

Для отображения информации об интерфейсе agg используйте следующую команду:

```
Switch1# show interface agg 1
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia a876.6b2c.9c01)
  Bandwidth 3000000 kbits
```

```
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00,  ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 140 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    1080 packets output, 60614 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output
```

3.10.3.4 Настройка динамического LACP

Конфигурации коммутаторов Switch1 и Switch2 приведены ниже:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите глобальные атрибуты LACP.

Настройте динамический режим LACP для групп агрегации.

Конфигурация Switch1:

```
Switch(config)# port-channel 1 lacp-mode dynamic
```

Конфигурация Switch2:

```
Switch(config)# port-channel 1 lacp-mode dynamic
```

Шаг 3. Войдите в режим настройки интерфейса и добавьте интерфейс в группу каналов.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# exit
Switch(config)# interface eth-0-2
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# no shutdown
```

```
Switch(config-if)# exit
Switch(config)# interface eth-0-3
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

Для отображения информации о группе каналов используйте следующую команду:

```
Switch# show channel-group summary
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
     macsa
Flags:  s - suspend           T - standby
        D - down/admin down   B - in Bundle
        R - Layer3            S - Layer2
        w - wait              U - in use
Mode:   SLB  - static load balance
        DLB  - dynamic load balance
        SHLB - self-healing load balance
        RR   - round robin load balance
Aggregator Name  Mode      Protocol     Ports
----------------+---------+-------------+-----------------------------------
----------
agg1(SU)         SLB       LACP(Dynamic)  eth-0-1(B) eth-0-2(B) eth-0-3(B)
```

Для отображения информации об интерфейсе agg используйте следующую команду:

```
Switch1# show interface agg1
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia cce3.33fc.330b)
  Bandwidth 3000000 kbits
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00,  ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 2 bits/sec, 0 packets/sec
```

```
    13 packets input, 1184 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    20 packets output, 2526 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
    0 underruns, 0 output errors, 0 pause output
```

3.10.3.5 Настройка группы каналов

Конфигурации коммутаторов Switch1 и Switch2 приведены ниже:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите глобальные атрибуты LACP.

Установите системный приоритет этого коммутатора. Этот приоритет используется для определения системы, ответственной за разрешение конфликтов при выборе групп агрегации. Чем ниже числовое значение, тем выше приоритет. Установите режим балансировки нагрузки. В данном случае для балансировки нагрузки выбирается MAC-адрес источника.

Настройка Switch1:

```
Switch(config)# lacp system-priority 2000
Switch(config)# hash-field port-channel
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip disable
```

Настройка Switch2:

```
Switch(config)# lacp system-priority 1000
Switch(config)# hash-field port-channel
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip disable
```

Шаг 3. Войдите в режим настройки интерфейса и добавьте интерфейс в группу каналов.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# exit
Switch(config)# interface eth-0-2
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

```
Switch(config)# interface eth-0-3
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

Для отображения информации о группе каналов используйте следующую команду:

```
Switch# show channel-group summary
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
     macsa
Flags:  s - suspend           T - standby
        D - down/admin down   B - in Bundle
        R - Layer3            S - Layer2
        w - wait              U - in use
Mode:   SLB  - static load balance
        DLB  - dynamic load balance
        SHLB - self-healing load balance
        RR   - round robin load balance
Aggregator Name  Mode      Protocol     Ports
---------------+---------+------------+-------------------------------------
----------
agg1(SU)         SLB       LACP         eth-0-1(B) eth-0-2(B) eth-0-3(B)
```

Для отображения информации об интерфейсе agg используйте следующую команду:

```
Switch1# show interface agg1
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia cce3.33fc.330b)
  Bandwidth 3000000 kbits
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00,  ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 2 bits/sec, 0 packets/sec
    13 packets input, 1184 bytes
```

```
Received 0 unicast, 0 broadcast, 0 multicast
0 runts, 0 giants, 0 input errors, 0 CRC
0 frame, 0 overrun, 0 pause input
0 input packets with dribble condition detected
20 packets output, 2526 bytes
Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output
```

3.10.3.6 Настройка взвешенной агрегации каналов

3.10.3.7 Топология

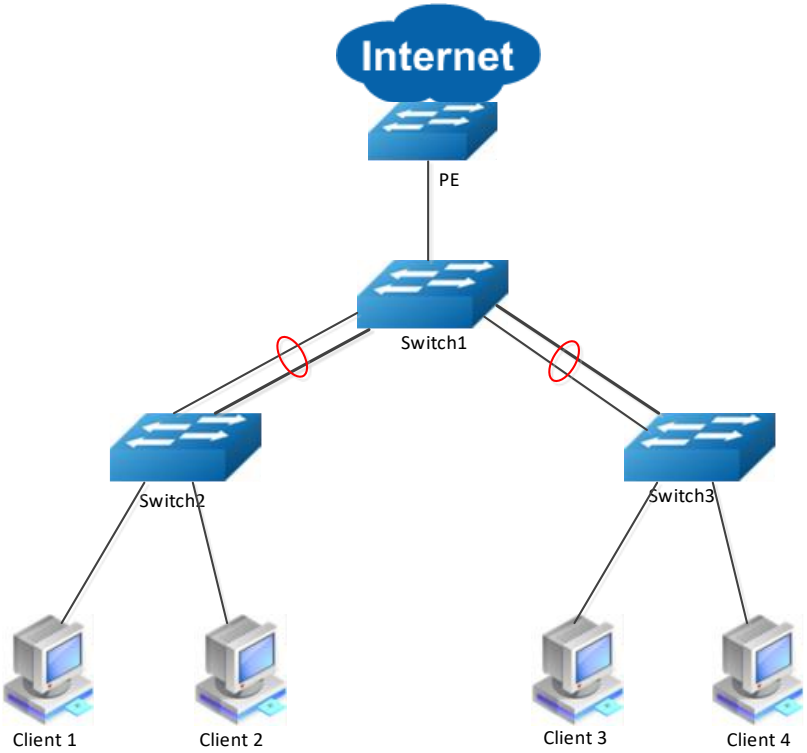


Рисунок 16 – Взвешенная агрегация каналов

3.10.3.8 Примеры конфигурации

Как показано на рисунке, Switch2 и Switch3 являются устройствами доступа. Устройством вышестоящей связи является коммутатор агрегации уровня Switch1. Между устройствами доступа и агрегации существуют два канала с разной пропускной способностью, которые образуют канал агрегации с коэффициентами веса. Конфигурация весов интерфейса действительна как для статической AGG, так и для LACP. В следующем примере показано, как включить агрегацию каналов с весами в LACP.

NOTE В этом примере мы предполагаем, что физическая пропускная способность интерфейса eth-0-1 составляет 1 Гбит/с, а физическая пропускная способность интерфейса

eth-0-25 — 10 Гбит/с. Таким образом, мы можем установить вес интерфейса eth-0-25 равным весу 10-ти интерфейсов eth-0-1. Фактические типы интерфейсов и пропускная способность зависят от модели оборудования; пожалуйста, обратитесь к техническим характеристикам продукта.

Соотношение веса и пропускной способности не является обязательным. Пользователи могут выбрать значение веса в соответствии с требованиями сети.

3.10.3.9 Этапы настройки

В этой главе показано, как настроить коммутаторы Switch1 и Switch2.

Switch3 идентичен Switch1.

Конфигурации коммутаторов Switch1 и Switch2 приведены ниже:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка интерфейса.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# exit
Switch(config)# interface eth-0-25
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# distribute-weight 10
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

NOTE По умолчанию вес интерфейсов участников равен 1.

Система поддерживает учет веса элементов только в режиме статической балансировки нагрузки и без функции самовосстановления. Общий вес всех элементов не должен превышать максимально допустимое количество элементов.

3.10.3.10 Шаг 3. Проверка.

Показать сводную информацию по группам каналов:

```
Switch# show channel-group summary
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
     macsa
Flags:   s - suspend           T - standby
         D - down/admin down   B - in Bundle
         R - Layer3            S - Layer2
         w - wait              U - in use
Mode:    SLB  - static load balance
```

```
        DLB  - dynamic load balance
        SHLB - self-healing load balance
        RR   - round robin load balance
Aggregator Name  Mode       Protocol      Ports
----------------+----------+--------------+-----------------------------------
----------
agg1(SU)         SLB        LACP(Dynamic)  eth-0-1(B) eth-0-25(B)
```

Показать информацию об интерфейсе agg1:

```
Switch# show interface agg1
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia cce3.33fc.330b)
  Bandwidth 11000000 kbits
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00,  ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 2 bits/sec, 0 packets/sec
    13 packets input, 1184 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    20 packets output, 2526 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
    0 underruns, 0 output errors, 0 pause output
```

3.10.3.11 Настройка агрегации каналов в режиме "ведущий-ведомый".

3.10.3.12 Топология

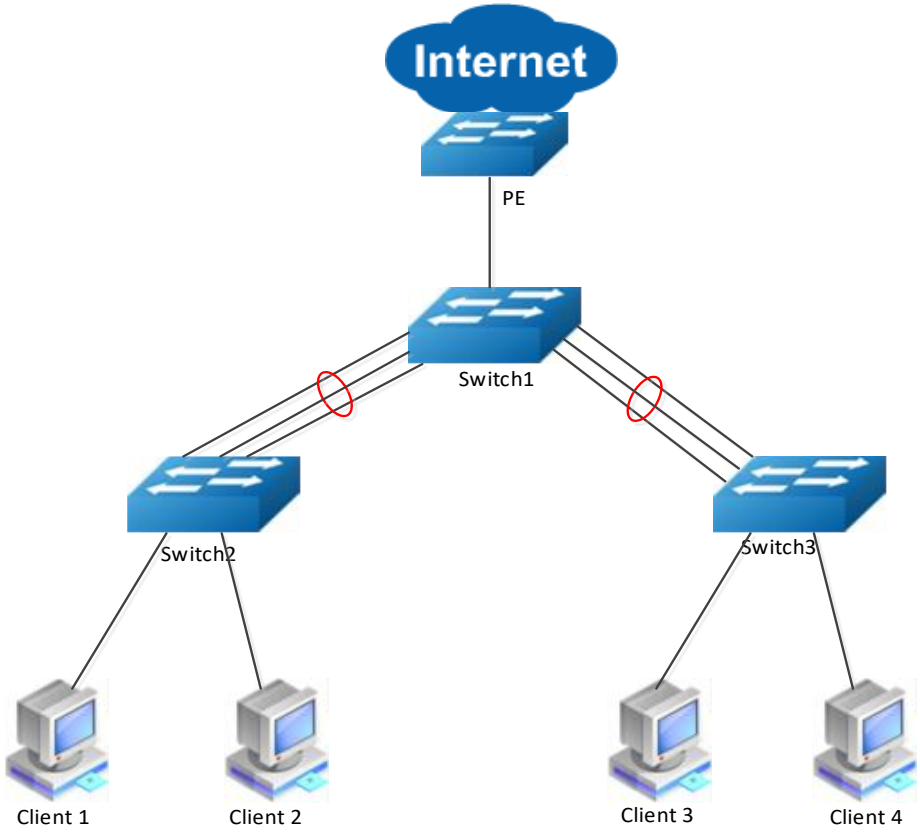


Рисунок 17 – Агрегация каналов в режиме "ведущий-ведомый"

3.10.3.13 Идеи конфигурации

Как показано на рисунке, коммутаторы Switch2 и Switch3 являются устройствами доступа. Устройством восходящего канала является коммутатор Switch1 уровня агрегации. Для обеспечения работы с несколькими клиентами восходящий канал устройства доступа должен обладать большой пропускной способностью. Также ему необходим резервный канал для предотвращения сбоев восходящего канала, которые могут привести к отключению всех клиентов нижнего сегмента.

В этом примере настроено резервное копирование в соотношении 2:1, что означает наличие двух рабочих каналов и одного резервного канала в сети.

3.10.3.14 Этапы настройки

В этой главе показано, как настроить коммутаторы Switch1 и Switch2.

Switch3 идентичен Switch1.

Конфигурации коммутаторов Switch1 и Switch2 приведены ниже:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка интерфейса.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# exit
Switch(config)# interface eth-0-2
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface eth-0-3
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 3. Настройка интерфейса.

```
Switch(config)# interface agg 1
Switch(config-if)# lacp max-active-linknumber 2
Switch(config-if)# lacp preempt enable
Switch(config-if)# lacp preempt delay 20
Switch(config-if)# end
```

NOTE Параметр “lacp max-active-linknumber 2” указывает, что в рабочем состоянии должно быть не более двух каналов связи. В резервном состоянии находится один канал, поскольку у нас три участника. Если какой-либо из рабочих каналов выйдет из строя, резервный канал может стать рабочим.

Параметр “lacp preempt enable” включает функцию вытеснения. Параметр “lacp preempt delay 20” означает, что канал связи начнет вытеснять работающий канал через 20 секунд. В этом случае, после восстановления предыдущего работающего канала, он будет ждать 20 секунд, прежде чем снова стать работающим каналом. Параметр “preempt delay” предотвращает слишком частое переключение каналов связи при их нестабильности. Значение задержки вытеснения по умолчанию равно 30. Если все каналы имеют одинаковые параметры, функцию вытеснения можно отключить. По умолчанию функция вытеснения отключена.

Шаг 4. Проверка.

Показать сводную информацию по группам каналов:

```
Switch# show channel-group summary
port-channel group-mode: flexible

Flags:  s - Suspend           T - Standby
        D - Down/Admin down   B - In bundle
        R - Layer3            S - Layer2
        w - Wait              U - In use

Mode:   SLB  - Static load balance
        DLB  - Dynamic load balance
        RR   - Round robin load balance
        RLB  - Resilient load balance
Aggregator Name  Mode      Protocol     Ports
---------------+---------+-------------+-----------------------------------
---
-------
agg1(SU)          SLB       LACP           eth-0-9(B)      eth-0-10(B)
eth-0-11(T)
```

Показать информацию об интерфейсе agg 1:

```
Switch# show interface agg 1
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is 845b.cf07.8009 (bia 845b.cf07.8009)
  Bandwidth 80000000 kbits
  Index 2049 , Metric 1 , Encapsulation ARPA
  Speed - 80.00Gb/s , Duplex - Full  , Media type is Aggregation
  Link type is autonegotiation
  FEC config: DEFAULT
  FEC ability: NONE
  FEC status: OFF
  The Maximum Frame Size is 9600 bytes
  VRF binding: not bound
  ARP timeout 01:00:00,  ARP retry interval 1s
  ARP Proxy is disabled, Local ARP Proxy is disabled
    5 minute input rate 71 bits/sec, 0 packets/sec
    5 minute output rate 68 bits/sec, 0 packets/sec
    73 packets input, 10804 bytes
    Received 0 unicast, 0 broadcast, 73 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    72 packets output, 10656 bytes
    Transmitted 0 unicast, 0 broadcast, 72 multicast
    0 underruns, 0 output errors, 0 pause output
    0 output discard
```

Взаимодействие двух сетевых карт сервера и коммутаторов

Режим привязки двух сетевых карт сервера	Соответствующая конфигурация для стороны коммутатора
Bond0	Используйте статическую агрегацию
Bond1	Конфигурация агрегации каналов не требуется.
Bond2	Используйте статическую агрегацию
Bond3	Различные интерфейсы коммутаторов настроены с разными VLAN.
Bond4	Используйте динамическую агрегацию
Bond5	Конфигурация агрегации каналов не требуется.
Bond6	Конфигурация агрегации каналов не требуется.

NOTE На практике Bond4 пользуется большей популярностью, поэтому рекомендуется использовать Bond4.

3.10.4 Сценарии применения

3.10.4.1 Топология

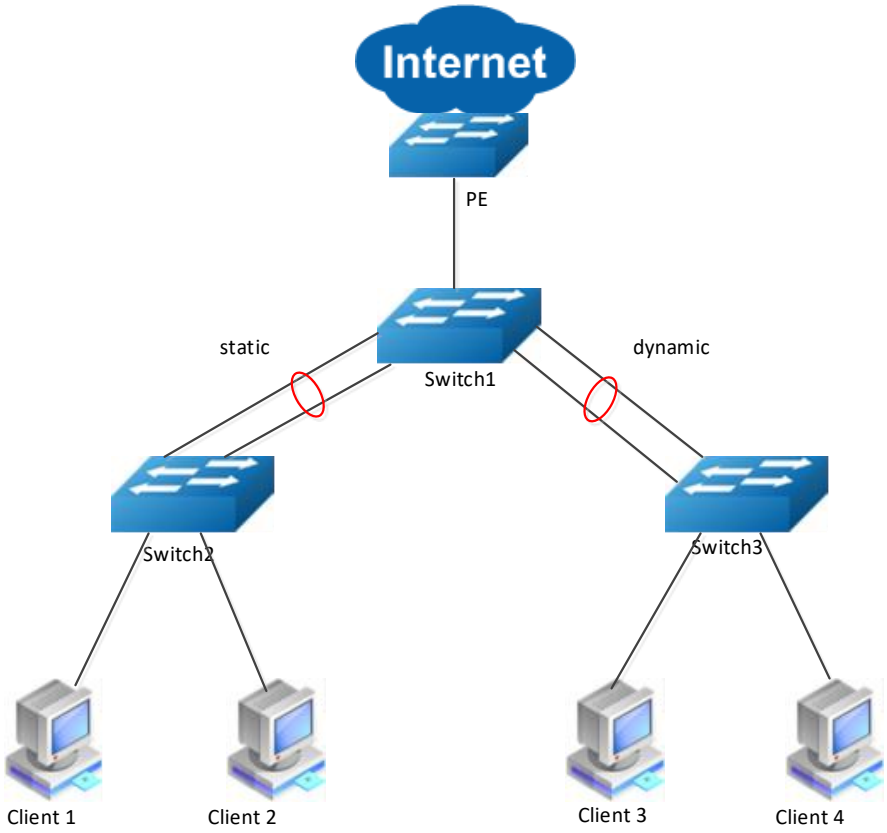


Рисунок 18 – Применение агрегации каналов

3.10.4.2 Сценарий применения и конфигурация

Как показано на рисунке, Switch2 и Switch3 — это устройства доступа. Устройство восходящего канала — это коммутатор агрегирующего уровня Switch1. Для обеспечения работы с несколькими клиентами восходящий канал устройства доступа должен обладать большой пропускной способностью. Также ему необходима резервная линия связи для предотвращения сбоев восходящего канала, которые могут привести к отключению всех клиентов нижнего сегмента сети.

В данном случае для удовлетворения таких требований мы используем агрегацию каналов.

- Если оба устройства поддерживают динамический LACP, рекомендуется использовать именно динамическую агрегацию.
- Если какое-либо из устройств не поддерживает динамический LACP, единственным выходом остается статическая агрегация.

В этом примере показано, как настроить статическую агрегацию между коммутаторами Switch1 и Switch2; также показано, как настроить протокол LACP между коммутаторами Switch1 и Switch3.

3.10.4.3 Этапы настройки статической агрегации между коммутаторами Switch1 и Switch2:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и добавьте интерфейс-участник в статический интерфейс агрегации.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# static-channel-group 1
Switch(config-if)# exit
Switch(config)# interface eth-0-2
Switch(config-if)# static-channel-group 1
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

NOTE Перед добавлением первого участника к агрегации необходимо подтвердить тип интерфейса уровня 2/уровня 3. Тип агрегации наследуется от первого участника.

Если тип Уровень 2/Уровень 3 различается, новый участник не сможет подключиться к интерфейсу агрегации.

Шаг 3. Войдите в режим настройки интерфейса агрегации, чтобы задать атрибуты.

```
Switch(config)# interface agg 1
Switch(config-if)# ip address 10.10.10.1/24
```

NOTE Следующие параметры изменить нельзя: switch-port/no switch-port, дуплекс, скорость.

Идентификатор VLAN можно изменить для агрегации на уровне 2.

3.10.4.4 Этапы настройки протокола LACP между коммутаторами Switch1 и Switch3：

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите LACP глобально.

Метод 1: Динамический LACP

NOTE Если согласование по LACP не удалось, каждый интерфейс-участник может наследовать атрибуты VLAN и независимо пересылать трафик уровня 2. Динамический LACP в основном используется в среде PXE (Preboot Execution Environment). Не рекомендуется использовать динамический LACP для подключения коммутаторов, поскольку сбой согласования может привести к зацикливанию сети.

```
Switch(config)# port-channel 2 lacp-mode dynamic
```

Метод 2: Статический LACP

NOTE По умолчанию используется статический режим LACP. Для восстановления статического режима используйте следующую команду：

```
Switch(config)# no port-channel 2 lacp-mode
```

Шаг 3. Войдите в режим настройки интерфейса и добавьте интерфейс-участник в интерфейс агрегации.

```
Switch(config)# interface eth-0-3
Switch(config-if)# no shutdown
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# exit
Switch(config)# interface eth-0-4
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 4. Проверка.

Информация о коммутаторах Switch1 и Switch2:

Показать сводную информацию по группам каналов:

```
Switch1# show channel-group summary
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
     macsa
Flags:  s - suspend           T - standby
        D - down/admin down   B - in Bundle
        R - Layer3            S - Layer2
        w - wait              U - in use
Mode:   SLB  - static load balance
        DLB  - dynamic load balance
        SHLB - self-healing load balance
        RR   - round robin load balance
Aggregator Name  Mode      Protocol     Ports
---------------+---------+------------+-------------------------------------
----------
agg1(SU)         SLB       Static         eth-0-1(B) eth-0-2(B)
```

Показать информацию об интерфейсе agg 1:

```
Switch1# show interface agg 1
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia a876.6b2c.9c01)
  Bandwidth 2000000 kbits
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00,  ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 140 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    1080 packets output, 60614 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output
```

Информация о коммутаторах Switch1 и Switch3:

Показать сводную информацию по группам каналов:

```
Switch# show channel-group summary
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
     macsa
Flags:  s - suspend           T - standby
        D - down/admin down   B - in Bundle
        R - Layer3            S - Layer2
        w - wait              U - in use
Mode:   SLB  - static load balance
        DLB  - dynamic load balance
        SHLB - self-healing load balance
        RR   - round robin load balance
Aggregator Name  Mode      Protocol     Ports
---------------+---------+-------------+-----------------------------------
----------
agg2(SU)         SLB       LACP(Dynamic)  eth-0-3(B) eth-0-4(B)
```

Показать информацию об интерфейсе agg2:

```
Switch# show interface agg2
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia cce3.33fc.330b)
  Bandwidth 2000000 kbits
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00,  ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 2 bits/sec, 0 packets/sec
    13 packets input, 1184 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    20 packets output, 2526 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
    0 underruns, 0 output errors, 0 pause output
```

3.11 Настройка управления потоком

3.11.1 Общие положения

3.11.1.1 Описание функции

Управление потоком позволяет подключенным портам Ethernet контролировать скорость трафика во время перегрузки, позволяя перегруженным узлам приостанавливать работу канала на другом конце. Если один порт испытывает перегрузку и не может принимать трафик, он уведомляет другой порт о необходимости прекратить отправку до тех пор, пока ситуация не разрешится. Когда локальное устройство обнаруживает перегрузку на своем конце, оно может уведомить партнера по каналу или удаленное устройство о перегрузке, отправив кадр-команду паузы. Вы можете использовать команду конфигурации интерфейса flowcontrol для установки возможности интерфейса принимать и отправлять кадры паузы. По умолчанию для портов задано состояние «прием выключен» и «отправка выключена».

NOTE Функция управления потоком (передача/приём) работает только в полнодуплексном режиме.

3.11.2 Настройка

3.11.2.1 Настройка инициации управления потоком

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и включите управление потоком.

```
Switch(config)# interface eth-0-1
Switch(config-if)# flowcontrol send on
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 4. Проверка.

Для отображения информации о регулировании потока используйте следующую команду:

```
Switch# show flowcontrol
Port       Receive FlowControl  Send FlowControl   RxPause      TxPause
           admin    oper        admin    oper
---------  -------- --------    -------- --------  -----------  -----------
eth-0-1    off      off         on       on        0            0
```

```
eth-0-2    off       off          off       off       0              0
eth-0-3    off       off          off       off       0              0
```

Для отображения информации об управлении потоком на указанном интерфейсе используйте следующую команду:

```
Switch# show flowcontrol eth-0-1
Port       Receive FlowControl  Send FlowControl   RxPause      TxPause
           admin    oper        admin    oper
---------  -------- --------    -------- --------  -----------  -----------
eth-0-1    off      off         on       on        0            0
```

3.11.2.2 Настройка приема команд управления потоком

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и включите управление потоком.

```
Switch(config)# interface eth-0-1
Switch1(config-if)# flowcontrol receive on
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 4. Проверка.

Для отображения информации о регулировании потока используйте следующую команду:

```
Switch1# show flowcontrol
Port       Receive FlowControl  Send FlowControl   RxPause      TxPause
           admin    oper        admin    oper
---------  -------- --------    -------- --------  -----------  -----------
eth-0-1    on       on           off      off       0            0
eth-0-2    off      off         off      off       0            0
eth-0-3    off      off         off      off       0            0
```

Для отображения информации об управлении потоком на указанном интерфейсе используйте следующую команду:

```
Switch1# show flowcontrol eth-0-1
Port       Receive FlowControl  Send FlowControl   RxPause      TxPause
           admin    oper        admin    oper
---------  -------- --------    -------- --------  -----------  -----------
eth-0-1    on       on           off      off       0            0
```

3.12 Настройка контроля сетевого шторма

3.12.1 Общие положения

3.12.1.1 Описание функции

Функция контроля шторма предотвращает прерывание трафика в локальной сети широковещательным, многоадресным или одноадресным штормом на одном из физических интерфейсов. Шторм в локальной сети возникает, когда пакеты переполняют сеть, создавая чрезмерный трафик и ухудшая производительность сети.

Для измерения интенсивности трафика в контролируемых зонах, используется один из следующих методов:

- пропускная способность в процентах от общей доступной пропускной способности порта;
- скорость передачи данных в пакетах в секунду через порт.

3.12.2 Настройка

3.12.2.1 Настройка контроля шторма по загрузке в процентах от общей полосы пропускания

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и установите уровень контроля шторма.

Пользователь может установить разные уровни для неизвестных одноадресных/многоадресных/широковещательных пакетов:

```
Switch(config)# interface eth-0-1
Switch(config-if)# storm-control unicast level 0.1
Switch(config-if)# storm-control multicast level 1
Switch(config-if)# storm-control broadcast level 10
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 4. Проверка.

```
Switch# show storm-control interface eth-0-1
Port      ucastMode ucastlevel   bcastMode bcastLevel   mcastMode mcastLevel
-------------------------------------------------------------------------------
```

```
--
eth-0-1    Level      0.10          Level      10.00         Level      1.00
```

3.12.2.2 Настройка контроля шторма по количеству пакетов в секунду

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и установите параметр Storm Control PPS.

Пользователь может установить разные значения pps для неизвестных одноадресных/многоадресных/широковещательных пакетов:

```
Switch(config)# interface eth-0-1
Switch(config-if)# storm-control unicast pps 1000
Switch(config-if)# storm-control multicast pps 10000
Switch(config-if)# storm-control broadcast pps 100000
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 4. Проверка.

```
Switch# show storm-control interface eth-0-1
Port       ucastMode ucastlevel   bcastMode bcastLevel   mcastMode mcastLevel
-------------------------------------------------------------------------------
--
eth-0-1    PPS       1000         PPS       100000       PPS       10000
```

3.13 Настройка обнаружения петель

3.13.1 Общие положения

3.13.1.1 Описание функции

Зацикливание в сети приводит к тому, что устройство продолжает отправлять широковещательные, многоадресные и неизвестные одноадресные пакеты. Это приводит к нерациональному использованию сетевых ресурсов и может парализовать всю сеть. Для быстрого обнаружения зацикливания на втором уровне сети и предотвращения его влияния на всю сеть, система должна предоставлять функцию обнаружения, которая будет уведомлять пользователя о

проверке сетевого соединения, а также управлять интерфейсом при возникновении зацикливания в сети.

Функция обнаружения петель позволяет определить, существует ли зацикливание на интерфейсе устройства. При включении обнаружения зацикливания на интерфейсе устройство будет периодически отправлять служебные пакеты обнаружения с этого интерфейса. Если устройство получает пакеты обнаружения, отправленные с этого же интерфейса, считается, что на этом интерфейсе существует петля, и устройство может отправить оповещение в систему управления сетью. Администраторы обнаруживают проблему зацикливания по таким оповещениям и устраняют проблему, чтобы избежать длительных сбоев в сети. Кроме того, устройство может управлять конкретным интерфейсом с петлей и отключать его, чтобы быстро свести к минимуму влияние зацикливания на сеть.

3.13.2 Настройка

3.13.2.1 Включить обнаружение петель

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и включите функцию обнаружения петли (Loopback Detect).

```
Switch(config)# interface eth-0-1
Switch(config-if)# loopback-detect enable
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 4. Проверка.

По умолчанию обнаружение петель отключено. Когда интерфейс включает обнаружение зацикливания, система отправляет пакеты обнаружения. Интервал передачи пакетов обнаружения по умолчанию составляет 5 секунд.

Для отображения настройки функции обнаружения петель используйте следующую команду:

```
Switch# show loopback-detect
Loopback detection packet interval(second): 5
Loopback detection recovery time(second):   15
```

```
Interface        Action          Status
eth-0-2          shutdown        NORMAL
```

3.13.2.2 Настройка интервала отправки пакетов обнаружения

Сеть постоянно меняется, поэтому обнаружение петель — это непрерывный процесс. Интерфейс отправляет пакеты обнаружения с определенным интервалом времени; время передачи пакетов называется периодом отправки пакетов обнаружения.

Интервал времени, в течение которого устройство отправляет пакеты обнаружения, составляет от 1 до 300 секунд. Период восстановления интерфейса по умолчанию в 3 раза превышает интервал отправки пакетов интерфейсом.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2: установите интервал между пакетами для функции Loopback Detect.

```
Switch(config)# loopback-detect packet-interval 10
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения интервала между пакетами в функции Loopback Detect используйте следующую команду:

```
Switch# show loopback-detect packet-interval
Loopback detection packet interval(second): 10
```

3.13.2.3 Настройка действия механизма Loopback Detect при обнаружении петли

Если на интерфейсе обнаружена петля, система может настроить действие для отправки оповещения, отключения интерфейса, блокировки интерфейса или другого действия.

После включения функции обнаружения петли на интерфейсе, такой интерфейс периодически отправляет служебные пакеты обнаружения. При обнаружении петли на интерфейсе система выполняет преднастроенное действие.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и установите действие для параметра «Обнаружение петли».

```
Switch(config)# interface eth-0-1
Switch(config-if)# loopback-detect action shutdown
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения информации о функции Loopback Detect на интерфейсе используйте следующую команду:

```
Switch# show loopback-detect interface eth-0-1
Interface         Action             Status
eth-0-1           shutdown           NORMAL
```

3.13.2.4 Настройка обнаружения петли внутри VLAN.

Укажите идентификаторы VLAN для отправки пакетов обнаружения петли на интерфейсе. После включения на интерфейсе система по умолчанию отправляет пакеты обнаружения петли без тегов. Когда интерфейс настроен в режиме тегирования в VLAN, пакеты обнаружения петли, отправляемые этим интерфейсом, будут отброшены на канале связи, и интерфейс не будет получать пакеты обнаружения, отправленные им же самим. Поэтому необходимо указать идентификаторы VLAN для пакетов обнаружения на интерфейсе.

После выполнения команды «loopback-detect packet vlan» на интерфейсе, интерфейс отправляет пакет обнаружения как без тегов, так и с указанными тегами VLAN. Можно указать максимум восемь идентификаторов VLAN.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте конкретный VLAN для параметра Loopback Detect.

```
Switch(config)# interface eth-0-1
Switch(config-if)# loopback-detect packet vlan 20
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 4. Проверка.

Для отображения конфигурации Loopback Detect используйте следующую команду:

```
Switch# show running-config interface eth-0-1
Building configuration...
!
interface eth-0-1
 loopback-detect enable
 loopback-detect packet vlan 20
!
```

3.14 Настройка туннелирования протоколов уровня 2

3.14.1 Общие положения

3.14.1.1 Описание функции

Клиентам на разных удаленных площадках, подключенных к сети провайдера, необходимо использовать различные протоколы уровня 2 для масштабирования своей топологии. Протокол STP должен работать корректно, и каждая VLAN должна охватить всю корректную топологию – и локальную площадку и все удаленные площадки в инфраструктуре клиента/провайдера.

При включении туннелирования протокола уровня 2, коммутаторы инкапсулируют пакеты протокола уровня 2 с новым заголовком уровня 2 и отправляют их по сети провайдера. Основные коммутаторы сети не обрабатывают эти пакеты, а пересылают их как обычные пакеты. Пакеты протокола уровня 2 проходят через инфраструктуру поставщика услуг насквозь и достигают коммутаторов клиентов на удаленной стороне сети. Туннелирование протокола уровня 2 может использоваться независимо или дополнять туннелирование 802.1Q.

3.14.2 Настройка

3.14.2.1 Туннелирование пакетов уровня Layer2

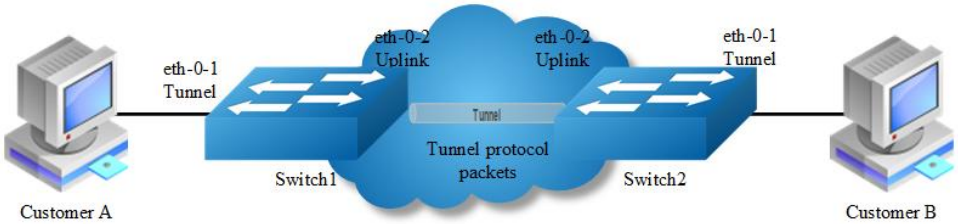


Рисунок 19 – Туннель протокола L2

В этом примере соединение установлено между коммутаторами Switch1 и Switch2. Порты eth-0-1 коммутатора Switch1 и eth-0-1 коммутатора Switch2 настроены как туннельные порты. Порты eth-0-2 коммутатора Switch1 и eth-0-2 коммутатора Switch2 настроены как аплинк порты. Если на порт eth-0-1 коммутатора Switch1 поступают пакеты протокола, к ним следует добавить

новый заголовок уровня 2 и отправить их через аплинк порт. Новый заголовок уровня 2 будет выглядеть следующим образом: MAC DA должен быть tunnel dmac; MAC SA должен быть switch route-mac; VLAN ID должен быть tunnel vid; VLAN priority (cos) должен быть Layer 2 Protocol cos; Ethertype должен быть 0xFFEE. Когда пакеты с новым заголовком уровня 2 поступают на порт eth-0-2 коммутатора Switch2, новый заголовок уровня 2 удаляется, и пакеты отправляются на порт eth-0-1 коммутатора Switch2.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 2-4
Switch(config-vlan)# exit
```

Шаг 3. Создайте EVC и настройте dot1q сопоставление VLAN.

```
Switch(config)# ethernet evc evc_c1
Switch(config-evc)# dot1q mapped-vlan 2
Switch(config-evc)# exit

Switch(config)# ethernet evc evc_c2
Switch(config-evc)# dot1q mapped-vlan 3
Switch(config-evc)# exit

Switch(config)# ethernet evc evc_c3
Switch(config-evc)# dot1q mapped-vlan 4
Switch(config-evc)# exit
```

Шаг 4. Включите протокол L2, задайте MAC-адрес назначения для туннеля и добавьте MAC-адреса протокола L2.

```
Switch(config)# l2protocol enable
Switch(config)# l2protocol tunnel-dmac 0100.0CCD.CDD2
Switch(config)# l2protocol mac 3 0180.C200.0008
Switch(config)# l2protocol mac 4 0180.C200.0009
Switch(config)# l2protocol full-mac 0100.0CCC.CCCC
```

Шаг 5. Войдите в режим настройки интерфейса и задайте атрибуты интерфейсов. Привяжите MAC-адреса протокола L2 к EVC.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-4
Switch(config-if)# spanning-tree port disable
Switch(config-if)# l2protocol mac 3 tunnel evc evc_c1
Switch(config-if)# l2protocol mac 4 tunnel evc evc_c2
Switch(config-if)# l2protocol full-mac tunnel evc evc_c3
Switch(config)# interface eth-0-2
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-4
Switch(config-if)# l2protocol uplink enable
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 7. Проверка.

Для отображения информации об интерфейсе и функции туннелирования на нем, используйте следующую команду:

```
switch1# show l2protocol interface eth-0-1
Interface  PDU Address         MASK             Status    EVC
           (u)-Untagged
           (t)-Tagged
=========  ==================  ===============  ========  ================
eth-0-1    0180.c200.0008(u)   ffff.ffff.ffff   Tunnel    evc_c1
eth-0-1    0180.c200.0008(t)   ffff.ffff.ffff   Tunnel    evc_c1
eth-0-1    0180.c200.0009(u)   ffff.ffff.ffff   Tunnel    evc_c2
eth-0-1    0180.c200.0009(t)   ffff.ffff.ffff   Tunnel    evc_c2
eth-0-1    0100.0ccc.cccc(u)   ffff.ffff.ffff   Tunnel    evc_c3
eth-0-1    0100.0ccc.cccc(t)   ffff.ffff.ffff   Tunnel    evc_c3
eth-0-1    stp(u)              ffff.ffff.ffff   Peer      N/A
eth-0-1    stp(t)              ffff.ffff.ffff   Peer      N/A
eth-0-1    slow-proto(u)       ffff.ffff.ffff   Peer      N/A
eth-0-1    slow-proto(t)       ffff.ffff.ffff   Peer      N/A
eth-0-1    dot1x(u)            ffff.ffff.ffff   Peer      N/A
eth-0-1    dot1x(t)            ffff.ffff.ffff   Peer      N/A
eth-0-1    cfm(u)              ffff.ffff.ffff   Peer      N/A
eth-0-1    cfm(t)              ffff.ffff.ffff   Peer      N/A
eth-0-1    lldp(u)             ffff.ffff.ffff   Peer      N/A
eth-0-1    lldp(t)             ffff.ffff.ffff   Peer      N/A
```

```
eth-0-1    cdp(u)              ffff.ffff.ffff  Peer      N/A
eth-0-1    cdp(t)              ffff.ffff.ffff  Peer      N/A
eth-0-1    vtp(u)              ffff.ffff.ffff  Peer      N/A
eth-0-1    vtp(t)              ffff.ffff.ffff  Peer      N/A
```

Для отображения информации об аплинк интерфейсе используйте следующую команду:

```
switch1# show l2protocol interface eth-0-2
Interface  PDU Address         MASK            Status    EVC
           (u)-Untagged
           (t)-Tagged
=========  ==================  ==============  ========  ================
eth-0-2    0180.c200.0008(u)   ffff.ffff.ffff  Peer      N/A
eth-0-2    0180.c200.0008(t)   ffff.ffff.ffff  Peer      N/A
eth-0-2    0180.c200.0009(u)   ffff.ffff.ffff  Peer      N/A
eth-0-2    0180.c200.0009(t)   ffff.ffff.ffff  Peer      N/A
eth-0-2    0100.0ccc.cccc(u)   ffff.ffff.ffff  Peer      N/A
eth-0-2    0100.0ccc.cccc(t)   ffff.ffff.ffff  Peer      N/A
eth-0-2    stp(u)              ffff.ffff.ffff  Peer      N/A
eth-0-2    stp(t)              ffff.ffff.ffff  Peer      N/A
eth-0-2    slow-proto(u)       ffff.ffff.ffff  Peer      N/A
eth-0-2    slow-proto(t)       ffff.ffff.ffff  Peer      N/A
eth-0-2    dot1x(u)            ffff.ffff.ffff  Peer      N/A
eth-0-2    dot1x(t)            ffff.ffff.ffff  Peer      N/A
eth-0-2    cfm(u)              ffff.ffff.ffff  Peer      N/A
eth-0-2    cfm(t)              ffff.ffff.ffff  Peer      N/A
eth-0-2    lldp(u)             ffff.ffff.ffff  Peer      N/A
eth-0-2    lldp(t)             ffff.ffff.ffff  Peer      N/A
eth-0-2    cdp(u)              ffff.ffff.ffff  Peer      N/A
eth-0-2    cdp(t)              ffff.ffff.ffff  Peer      N/A
eth-0-2    vtp(u)              ffff.ffff.ffff  Peer      N/A
eth-0-2    vtp(t)              ffff.ffff.ffff  Peer      N/A
eth-0-2    N/A                 N/A             Uplink    N/A
```

Для отображения информации о MAC-адресе назначения туннеля используйте следующую команду:

```
Switch1# show l2protocol tunnel-dmac
Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd2
```

3.15 Настройка MSTP

3.15.1 Общие положения

3.15.1.1 Описание функции

MSTP (Multiple Spanning Tree Algorithm and Protocol (IEEE 802.1Q-2005)) позволяет передавать информацию о нескольких VLAN в одном блоке данных (BPDU), тем самым уменьшая количество отправляемых BPDU, необходимых для поддержки большого количества VLAN. MSTP

обеспечивает несколько путей пересылки трафика данных и позволяет балансировать нагрузку. Он повышает отказоустойчивость сети, поскольку сбой на одном пути пересылки не влияет на другие пути пересылки.

Наиболее распространенное первоначальное развертывание MSTP - на магистральном и распределительном уровнях коммутируемой сети уровня L2; такое развертывание обеспечивает высокую доступность сети, необходимую в среде поставщиков услуг.

Когда коммутатор находится в режиме MST, протокол быстрого соединения (RSTP), основанный на IEEE 802.1w, автоматически включается. Протокол RSTP обеспечивает быструю сходимость связующего дерева, что устраняет задержку пересылки в соответствии со стандартом IEEE 802.1D и быстро переводит корневые порты и назначенные порты в состояние пересылки.

3.15.2 Настройка

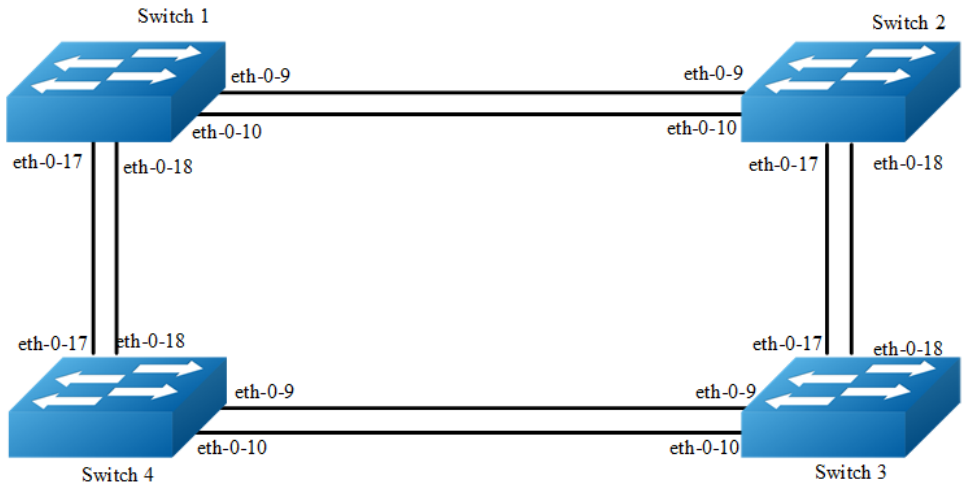


Рисунок 1-1 MSTP

Конфигурации коммутаторов Switch1-Switch4 приведены ниже. Конфигурации этих 4 коммутаторов одинаковы.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите режим STP.

```
Switch(config)# spanning-tree mode mstp
```

Шаг 3. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
```

```
Switch(config-vlan)# vlan 20
Switch(config-vlan)# exit
```

Шаг 4. Войдите в режим настройки MSTP, создайте регион и инстанцию. Привяжите VLAN к инстанции.

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# region RegionName
Switch(config-mst)# instance 1 vlan 10
Switch(config-mst)# instance 2 vlan 20
Switch(config-mst)# exit
```

Шаг 5. Войдите в режим настройки интерфейса и задайте атрибуты интерфейсов.

```
Switch(config)# interface eth-0-9
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-10
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-17
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-18
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 6. Включите STP и установите приоритет для каждого коммутатора.

Switch1:

```
Switch# configure terminal
Switch(config)# spanning-tree priority 0
Switch(config)# spanning-tree enable
```

Switch2:

```
Switch# configure terminal
Switch(config)# spanning-tree instance 1 priority 0
Switch(config)# spanning-tree enable
```

Switch3:

```
Switch# configure terminal
Switch(config)# spanning-tree instance 2 priority 0
Switch(config)# spanning-tree enable
```

Switch4:

```
Switch# configure terminal
Switch(config)# spanning-tree enable
```

Шаг 7. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 8. Проверка.

Для отображения информации о протоколе MSTP на коммутаторе Switch1 используйте следующую команду:

```
Switch# show spanning-tree mst brief
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority       0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
Bridge ID   Priority       0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
            Aging Time  300 sec
Interface    Role          State            Cost      Priority.Number
Type
--------------------------------------------------------------------------------
---
eth-0-9     Designated     Forwarding      20000           128.9        P2p
eth-0-10    Designated     Forwarding      20000           128.10       P2p
eth-0-17    Designated     Forwarding      20000           128.17       P2p
eth-0-18    Designated     Forwarding      20000           128.18       P2p
##### MST1:  Vlans: 10
Root ID     Priority       1 (0x0001)
            Address     9c9a.7d91.9f00
Bridge ID   Priority    32769 (0x8001)
            Address     2225.fa28.c900
Interface    Role          State            Cost      Priority.Number
Type
```

```
--------------------------------------------------------------------------------
---
eth-0-9     Rootport       Forwarding      20000           128.9          P2p
eth-0-10    Alternate      Discarding      20000           128.10         P2p
eth-0-17    Designated     Forwarding      20000           128.17         P2p
eth-0-18    Designated     Forwarding      20000           128.18         P2p
##### MST2:  Vlans: 20
Root ID     Priority       2 (0x0002)
            Address     304c.275b.b200
Bridge ID   Priority    32770 (0x8002)
            Address     2225.fa28.c900
Interface    Role          State            Cost      Priority.Number
Type
--------------------------------------------------------------------------------
---
eth-0-9     Alternate      Discarding      20000           128.9          P2p
eth-0-10    Alternate      Discarding      20000           128.10         P2p
eth-0-17    Rootport       Forwarding      20000           128.17         P2p
eth-0-18    Alternate      Discarding      20000           128.18         P2p
```

Для отображения информации о протоколе MSTP на коммутаторе Switch2 используйте следующую команду:

```
Switch# show spanning-tree mst brief
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority       0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
Bridge ID   Priority    32768 (0x8000)
            Address     9c9a.7d91.9f00
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
            Aging Time  300 sec
Interface    Role          State            Cost      Priority.Number
Type
--------------------------------------------------------------------------------
---
eth-0-9     Rootport       Forwarding      20000           128.9          P2p
eth-0-10    Alternate      Discarding      20000           128.10         P2p
eth-0-17    Designated     Forwarding      20000           128.17         P2p
eth-0-18    Designated     Forwarding      20000           128.18         P2p
##### MST1:  Vlans: 10
Root ID     Priority       1 (0x0001)
            Address     9c9a.7d91.9f00
Bridge ID   Priority       1 (0x0001)
            Address     9c9a.7d91.9f00
Interface    Role          State            Cost      Priority.Number
Type
```

```
--------------------------------------------------------------------------------
---
eth-0-9     Designated     Forwarding      20000           128.9          P2p
eth-0-10    Designated     Forwarding      20000           128.10         P2p
eth-0-17    Designated     Forwarding      20000           128.17         P2p
eth-0-18    Designated     Forwarding      20000           128.18         P2p
##### MST2:  Vlans: 20
Root ID     Priority       2 (0x0002)
            Address     304c.275b.b200
Bridge ID   Priority    32770 (0x8002)
            Address     9c9a.7d91.9f00
Interface    Role          State            Cost      Priority.Number
Type
--------------------------------------------------------------------------------
---
eth-0-9     Designated     Forwarding      20000           128.9          P2p
eth-0-10    Designated     Forwarding      20000           128.10         P2p
eth-0-17    Rootport       Forwarding      20000           128.17         P2p
eth-0-18    Alternate      Discarding      20000           128.18         P2p
```

Для отображения информации о протоколе MSTP на коммутаторе Switch3 используйте следующую команду:

```
Switch# show spanning-tree mst brief
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority       0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
Bridge ID   Priority    32768 (0x8000)
            Address     304c.275b.b200
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
            Aging Time  300 sec
Interface    Role          State            Cost      Priority.Number
Type
--------------------------------------------------------------------------------
---
eth-0-9     Rootport       Forwarding      20000           128.9          P2p
eth-0-10    Alternate      Discarding      20000           128.10         P2p
eth-0-17    Alternate      Discarding      20000           128.17         P2p
eth-0-18    Alternate      Discarding      20000           128.18         P2p
##### MST1:  Vlans: 10
Root ID     Priority       1 (0x0001)
            Address     9c9a.7d91.9f00
Bridge ID   Priority    32769 (0x8001)
            Address     304c.275b.b200
Interface    Role          State            Cost      Priority.Number
Type
```

```
--------------------------------------------------------------------------------
---
eth-0-9     Designated     Forwarding      20000           128.9          P2p
eth-0-10    Designated     Forwarding      20000           128.10         P2p
eth-0-17    Rootport       Forwarding      20000           128.17         P2p
eth-0-18    Alternate      Discarding      20000           128.18         P2p
##### MST2:  Vlans: 20
Root ID     Priority       2 (0x0002)
            Address     304c.275b.b200
Bridge ID   Priority       2 (0x0002)
            Address     304c.275b.b200
Interface    Role          State            Cost      Priority.Number
Type
--------------------------------------------------------------------------------
---
eth-0-9     Designated     Forwarding      20000           128.9          P2p
eth-0-10    Designated     Forwarding      20000           128.10         P2p
eth-0-17    Designated     Forwarding      20000           128.17         P2p
eth-0-18    Designated     Forwarding      20000           128.18         P2p
```

Для отображения информации о протоколе MSTP на коммутаторе Switch4 используйте следующую команду:

```
Switch# show spanning-tree mst brief

Switch# show spanning-tree mst brief
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority       0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
Bridge ID   Priority    32768 (0x8000)
            Address     80a4.be55.6400
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
            Aging Time  300 sec
Interface    Role          State            Cost      Priority.Number
Type
--------------------------------------------------------------------------------
---
eth-0-9     Designated     Forwarding      20000           128.9          P2p
eth-0-10    Designated     Forwarding      20000           128.10         P2p
eth-0-17    Rootport       Forwarding      20000           128.17         P2p
eth-0-18    Alternate      Discarding      20000           128.18         P2p
##### MST1:  Vlans: 10
Root ID     Priority       1 (0x0001)
            Address     9c9a.7d91.9f00
Bridge ID   Priority    32769 (0x8001)
            Address     80a4.be55.6400
```

```
Interface    Role          State            Cost      Priority.Number
Type
--------------------------------------------------------------------------
---
eth-0-9      Alternate     Discarding       20000          128.9         P2p
eth-0-10     Alternate     Discarding       20000          128.10        P2p
eth-0-17     Rootport      Forwarding       20000          128.17        P2p
eth-0-18     Alternate     Discarding       20000          128.18        P2p
##### MST2:  Vlans: 20
Root ID      Priority      2 (0x0002)
             Address       304c.275b.b200
Bridge ID    Priority      32770 (0x8002)
             Address       80a4.be55.6400
Interface    Role          State            Cost      Priority.Number
Type
--------------------------------------------------------------------------
---
eth-0-9      Rootport      Forwarding       20000          128.9         P2p
eth-0-10     Alternate     Discarding       20000          128.10        P2p
eth-0-17     Designated    Forwarding       20000          128.17        P2p
eth-0-18     Designated    Forwarding       20000          128.18        P2p
```

3.16 Настройка MLAG

3.16.1 Общие положения

3.16.1.1 Описание функции

В сетевой топологии высокодоступного центра обработки данных коммутатор TOR или сервер обычно подключается к двум агрегирующим коммутаторам для обеспечения резервирования и распределения нагрузки. В этой ситуации протокол Spanning Tree Protocol (STP) может предотвратить петли, блокируя половину портов на агрегирующих коммутаторах; однако это вдвое снизит использование полосы пропускания сети; хотя использование MSTP может в определенной степени улучшить использование полосы пропускания, оно так же увеличивает сложность сети.

Использование MLAG (Multi-Chassis Link Aggregation) может решить эту проблему. MLAG — это технология виртуализации, которая представляет два разных коммутатора как единый узел для установления агрегационного канала с одним и тем же терминалом или устройством. Между двумя коммутаторами существует единый канал связи, который логически объединяет два коммутатора в одно устройство. Порты на этих двух устройствах генерируют агрегационные порты, позволяя всем портам участвовать в пересылке данных. Таким образом, MLAG повышает надежность от уровня канала связи до уровня устройства, формируя систему Active-Active.

3.16.1.2 Предыстория

По сравнению со стекированием, устройства MLAG по-прежнему требуют раздельного управления, но конфигурация такого устройства достаточно проста. При пересылке одноадресного трафика выбирается локальный порт агрегации, отличный от порта MLAG-партнера, чтобы предотвратить перегрузку трафика через канал связи между партнерами и избежать потери пропускной способности соединения, что снижает задержку в сети.

MLAG предоставляет следующие технические преимущества:

- обеспечивает более высокую пропускную способность и надежность каналов связи по мере увеличения сетевого трафика;

- MPAG обеспечивает топологию уровня 2 для поддержки резервного копирования без петель. Не требует настройки STP и упрощает сеть и конфигурацию;

- поддерживает статический LAG или LACP для подключения к другим коммутаторам или серверам вместо использования других протоколов;

- поддерживает active-active резервирование уровня 2;

- поддержка раздельного обновления устройств, поэтому одно из устройств всегда может поддерживать нормальную работу сети.

3.16.1.3 Описание механизма работы и основные термины

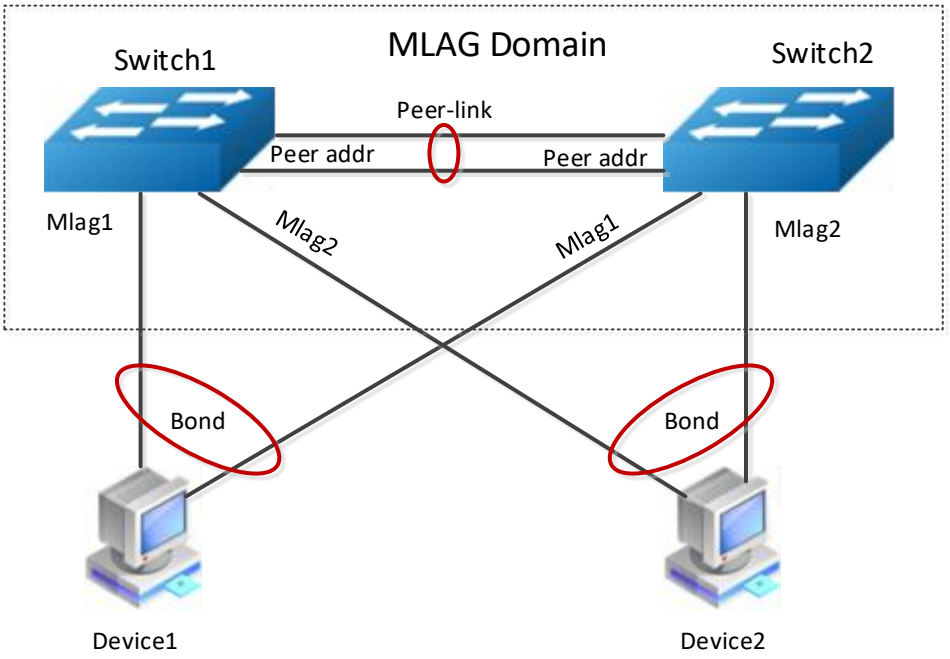


Рисунок 20 – Схема топологии MLAG

На рисунке выше представлена схема сети MLAG. На схеме домен MLAG содержит два коммутатора; устройство, которое к ним подключается, может быть сервером, коммутатором или другим доменом MLAG. Коммутатор 1 и коммутатор 2 имеют по два порта, которые объединяются в разные группы MLAG; соответствующая терминология приведена ниже:

- MLAG: Multi-Chassis Link Aggregation; два устройства образуют группу MLAG, называемую MLAG-партнерством;

- MLAG group: интерфейсы, входящие в одну и ту же группу MLAG, будут рассматриваться внешним устройством как один и тот же порт агрегации;

- Orphan Port: это интерфейсы, которые не входят в группу MLAG на устройствах MLAG;

- Peer-link: используется для соединения двух устройств, образующих группу MLAG; если порт на одной из сторон группы MLAG выходит из строя, трафик будет проходить через peer-link и перенаправляться через устройство-партнер группы MLAG;

- Peer-address: адрес для коммуникации протокола MLAG на устройстве MLAG;

- Reload-delay: после перезапуска устройства, его порты на некоторое время перейдут в состояние errdisable, чтобы предотвратить зацикливание сети до установления соединения с соседями MLAG; по истечении этого времени, эти порты автоматически перейдут в состояние admin up (этот таймер можно настроить).

- System ID: по умолчанию это Route-MAC адрес устройства. Идентификатор системы используется для выбора роли ведущего и ведомого устройства в MLAG (он отличается от идентификатора системы LACP).

Механизм пересылки (обычная пересылка)

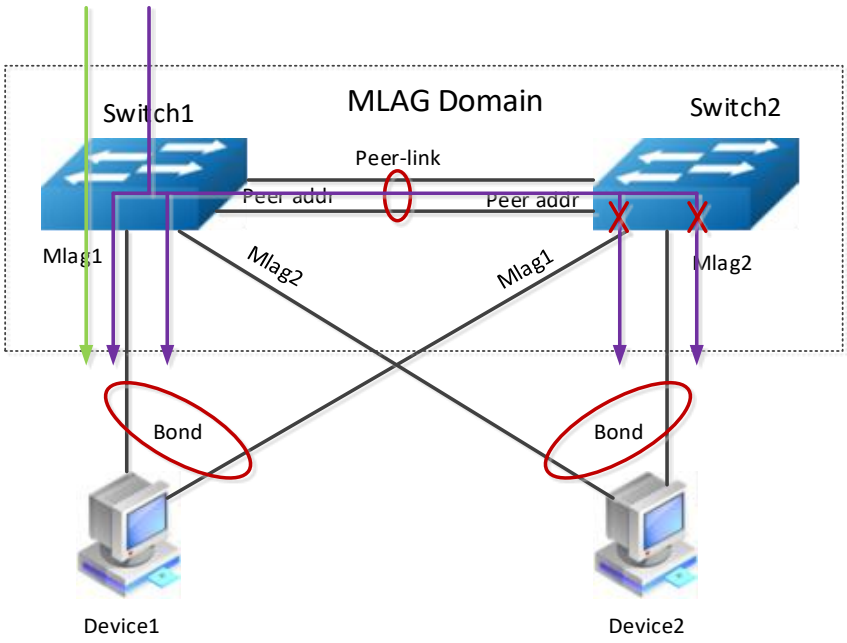


Рисунок 21 – Схема пересылки трафика MLAG

Процесс создания MLAG-домена и принцип его работы описан ниже:

- коммутаторы 1 и 2 устанавливают TCP-соединение, обмениваются служебными сообщениями протокола MLAG и устанавливают соседство MLAG;

- выбор ведущего/ведомого режима осуществляется путем сравнения размеров идентификаторов систем, передаваемых в сообщениях протокола MLAG; по умолчанию в качестве ведущего выбирается больший идентификатор системы; MLAG будет использовать идентификатор ведущей системы в качестве системного MAC-адреса LACP для всей топологии4

- после установления соседства, между устройствами отправляются сообщения keepalive, активируя механизм тайм-аута; если в течение этого времени не поступает ни одного сообщения keepalive, устройство считает, что сосед MLAG разорвал связь, и возвращается в одиночный режим работы;

- соответствующие агрегирующие порты двух устройств будут объединены в одну и ту же группу MLAG;

- когда агрегирующий порт привязки в группе MLAG изучает новые MAC-адреса, устройство синхронизирует эти MAC-адреса с соседним устройством, обеспечивая синхронизацию таблиц MAC-адресов на обоих устройствах;

- Для известного одноадресного трафика будет выполнена Проверка. локальной таблицы MAC-адресов, поскольку обе стороны имеют свои таблицы MAC-адресов. Зеленые линии на рисунке показывают трафик, поступающий с коммутатора 1, который проверяет свою таблицу MAC-адресов и пересылает трафик; трафик, поступающий на коммутатор 2 (на рисунке не показан) он использует те же принципы пересылки, что и коммутатор 1;

- Для неизвестного одноадресного или широковещательного трафика потребуется широковещательная рассылка, как показано синей линией; он пройдет через PEER-LINK и попадет на устройство MLAG PEER. Коммутатор 2 увидит, что MLAG 1 и 2 имеют статус UP (коммутатор 1 в соответствии с протоколом MLAG). Следовательно, коммутатор 2 отбросит эту часть трафика, чтобы предотвратить сетевую петлю потока.

Защита при падении соединения (сбой интерфейса MLAG)

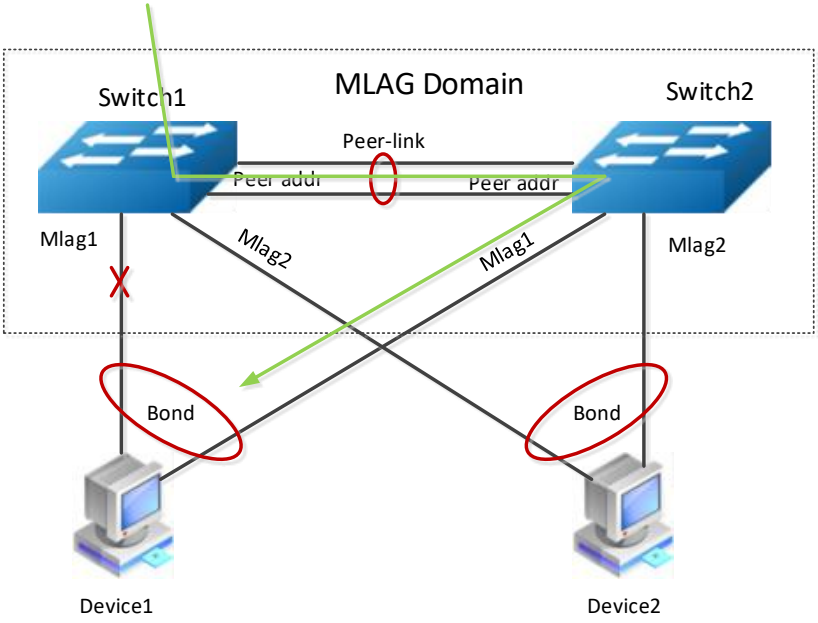


Рисунок 22 – Резервное переключение MLAG для пересылки трафика

Как показано на рисунке выше, когда интерфейс MLAG 1 на коммутаторе Switch 1 переходит в неактивное (выключенное) состояние, для сохранения возможности пересылки трафика, система действует по следующему алгоритму:

- если на одном из коммутаторов MLAG-пары выходят из строя все порты MLAG-группы, таблица MAC-адресов на нем обновляется так, чтобы трафик для MAC-адресов, находящихся за вышедшими из строя портами, отправлялся через peer-link второму коммутатору пары;
- второй коммутатор принимает трафик через peer-link, проверяет свою таблицу MAC-адресов и передает их по оставшимся активными портам этой MLAG-группы;
- если на коммутатор приходит одноадресный трафик с неизвестным MAC-адресом (unknown unicast) или широковещательный трафик (broadcast), который должен быть передан через вышедшие из строя порты MLAG-группы, то после его передачи по peer-link второму коммутатору он перестает блокироваться на портах этой MLAG-группы второго коммутатора;
- для MLAG-групп с нормально работающими портами коммутация трафика выполняется как и прежде. Когда работа вышедших из строя портов MLAG-группы нормализуется, система возвращается к обычному режиму коммутации.

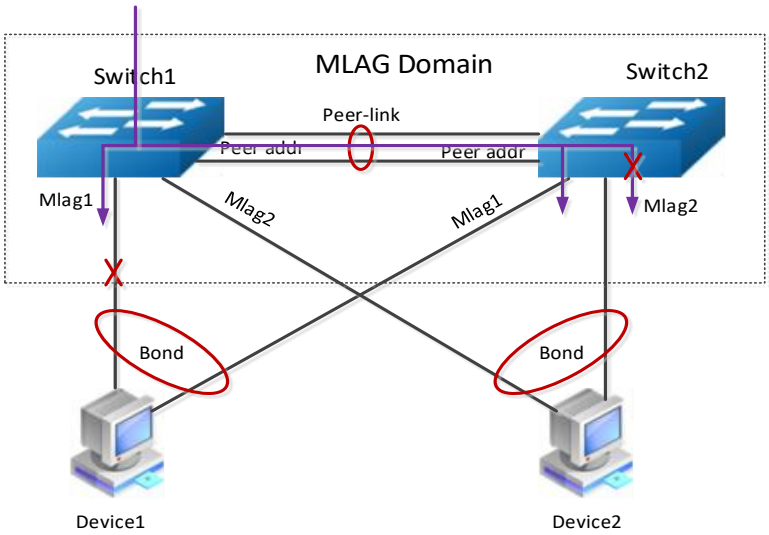


Рисунок 23 – MLAG защита от лавинного трафика

Для переадресации трафика система выполнит следующие действия:

- когда коммутатор 1 обнаружит, что локальный интерфейс MLAG 1 не отвечает, он уведомит коммутатор 2 по протоколу MLAG; после получения сообщений от коммутатора 1 коммутатор 2 больше не будет отбрасывать трафик на MLAG 1;

- когда порт MLAG восстановится, коммутатор 1 уведомит коммутатор 2, используя протокол MLAG; коммутатор 2 снова начнет отбрасывать трафик, направляемый на порт MLAG 1.

Защита от падения каналов (сбои в работе Peer-каналов)

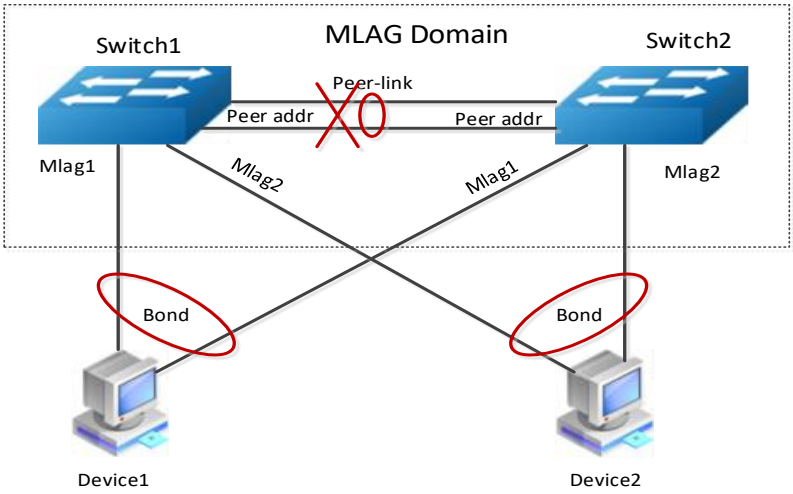


Рисунок 24 – Защита при падении Peer-линка

- когда Peer-соединение разрывается и истекает таймер его восстановления, устройство MLAG разделяется на два отдельных коммутатора.

- если Устройство 1 и Устройство 2 используют агрегированное соединение LACP с устройством MLAG, то при истечении срока действия одноранговое соединения и разделении

MLAG коммутаторы 1 и 2 будут использовать разные идентификаторы независимо друг от друга. Следовательно, активен только один канал связи, поэтому риск петли отсутствует.

- если Устройство 1 и Устройство 2 подключаются к устройству MLAG с использованием статической агрегации каналов, то оба канала остаются активными; поскольку участники не могут пересылать трафик внутри одной и той же агрегационной группы, это не вызовет зацикливания трафика.

3.16.1.4 Дополнительный функционал

LACP с MLAG

Для реализации LACP для MLAG мы выполняем следующие действия:

- сообщения LACP, отправляемые двумя устройствами MLAG через интерфейс MLAG, имеют одинаковые Actor System Priority и Actor System ID
- сообщения LACP, отправляемые двумя устройствами MLAG через интерфейс MLAG, имеют одинаковый Actor Key.
- устройство MLAG использует тот же идентификатор системы LACP, что и ведущее устройство (идентификатор системы LACP включает в себя системный приоритет LACP и системный LACP MAC-адрес). Ведущее устройство должно синхронизировать системный идентификатор LACP с ведомым устройством.
- после установления соединения MLAG ведомое устройство MLAG должно использовать системный MAC-адрес LACP. Если ведущее устройство MLAG выходит из строя или перезагружается, сессия MLAG разрывается, и ведомое устройство должно переключиться на свой собственный MAC-адрес LACP. Это событие приведет к повторному согласованию протокола LACP, и соединение LACP изменится с активного на неактивное, а затем снова станет активным после успешного согласования. Для повышения надежности в этом случае наше устройство предоставляет команду для настройки системного MAC-адреса LACP для MLAG. После настройки этой команды все интерфейсы MLAG могут использовать один и тот же MAC-адрес LACP.
- идентификатор системы LACP — это атрибут протокола LACP, используемый для маркировки устройства в протоколе LACP. Рекомендуется использовать агрегацию в режиме LACP. Статическая агрегация используется только в том случае, если удаленное устройство не поддерживает LACP.

Реализация ISSU для MLAG

ISSU (In-Service Software Upgrade) для MLAG позволяет обновлять ПО коммутаторов без прерывания трафика. Устройство MLAG будет использовать механизм блокировки errdisable для реализации ISSU. После перезапуска устройств, завершивших обновление, устройства, на которых настроен MLAG, на некоторое время переведут локальные порты в режим errdisable. В течение этого периода времени MLAG будет повторно согласовывать и синхронизировать таблицы,

а также вычислять STP; по истечении времени таймера порты восстановят нормальный режим работы. Этот период времени можно настроить с помощью команды «reload-delay»; значение по умолчанию составляет 300 секунд.

Порт, находящийся в состоянии errdisable, аналогичен порту в состоянии «down»: он не будет участвовать в пересылке данных; его можно восстановить командой «no shutdown», а для проверки состояния использовать команду «show errdisable recovery».

VARP с MLAG

Система предоставит общую конфигурацию «виртуальный MAC-адрес» и «виртуальный IP-адрес», чтобы обеспечить единые сетевые адреса для противоположного терминала, подключенного к устройству MLAG. Независимо от того, какое устройство получит эти сообщения (о виртуальном IP-адресе и виртуальном MAC-адресе), все они будут корректно обрабатываться локально. Виртуальный IP-адрес может находиться в той же подсети, что и IP-адрес интерфейса, или в другой подсети; каждый интерфейс может настроить до 15 виртуальных IP-адресов. Коммутатор поддерживает только один виртуальный MAC-адрес.

Для виртуальной установки MAC-адреса необходимо задать MAC-адрес, которого нет в локальной сети; этот адрес не может совпадать с маршрутизируемым MAC-адресом устройства или MAC-адресом интерфейса.

Сопряжение MLAG с сервером с двумя сетевыми подключениями

Для серверов с двумя сетевыми интерфейсами обычно устанавливается режим объединения 4; в этом случае коммутатору необходимо настроить режим агрегации LACP и добавить порт агрегации в группу mlag, используя команду «channel-group» для настройки режима агрегации LACP.

Когда режим объединения настроен на 0 или 2, коммутатору необходимо настроить статическую агрегацию портов, и агрегированные порты добавляются в группу mlag; для других режимов объединения настраивать группу mlag не требуется.

3.16.2 Ограничения и меры предосторожности

Два коммутатора, входящие в состав MLAG, должны быть коммутаторами нашего производства; их нельзя комбинировать с коммутаторами других производителей для формирования MLAG.

Peer-address подключаются напрямую к соответствующим сегментам сети.

Порты в состоянии errdisable аналогичны портам в состоянии shutdown: они не будут перенаправлять трафик, а автоматически восстановятся по истечении таймера, если причиной является «reload-delay»; или же системный администратор может проверить это с помощью команды «show errdisable recovery» и восстановить их, используя команду «shutdown/no shutdown».

MLAG не поддерживает синхронизацию записей в таблице многоадресной рассылки. Использование MLAG в сценариях многоадресной рассылки не рекомендуется. Рекомендуется отключить функцию IGMP snooping на устройствах MLAG. (Функция IGMP snooping включена по умолчанию)

3.16.3 Настройка

3.16.3.1 Базовая конфигурация

Конфигурации коммутаторов Switch1-Switch2 приведены ниже. Конфигурации этих двух коммутаторов одинаковы.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10,4094
Switch(config-vlan)# exit
```

Шаг 3. Создайте статическую агрегацию.

```
Switch(config)# interface eth-0-1
Switch(config-if)# static-channel-group 1
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 4. Настройте атрибуты интерфейса связи между узлами MLAG.

interface eth-0-9 будет установлен в качестве peer link interface позже

```
Switch(config)# interface eth-0-9
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# spanning-tree port disable
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 5. Привяжите интерфейс Agg к MLAG.

```
Switch(config)# interface agg1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10
Switch(config-if)# mlag 1
```

```
Switch(config-if)# exit
```

Шаг 6. Настройте атрибуты интерфейса VLAN.

Switch1:

```
Switch(config)# interface vlan4094
Switch(config-if)# ip address 12.1.1.1/24
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface vlan4094
Switch(config-if)# ip address 12.1.1.2/24
Switch(config-if)# exit
```

Шаг 7. Войдите в режим настройки MLAG и задайте атрибуты MLAG.

Switch1:

```
Switch(config)# mlag configuration
Switch(config-mlag)# peer-link eth-0-9
Switch(config-mlag)# peer-address 12.1.1.2
Switch(config-mlag)# exit
```

Switch2:

```
Switch(config)# mlag configuration
Switch(config-mlag)# peer-link eth-0-9
Switch(config-mlag)# peer-address 12.1.1.1
Switch(config-mlag)# end
```

Шаг 8. Проверка.

Используйте следующую команду для отображения информации о MLAG на коммутаторе Switch1

```
Switch# show mlag
MLAG configuration:
-----------------
role         : Master
local_sysid  : ea90.aecc.cc00
mlag_sysid   : ea90.aecc.cc00
peer-link    : eth-0-9
peer conf    : Yes

Switch# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up

Switch# show mlag peer
```

```
MLAG neighbor is 12.1.1.2, MLAG version 1
MLAG state = Established, up for 00:13:07
Last read 00:00:48, hold time is 240, keepalive interval is 60 seconds
Received 17 messages,Sent 19 messages
Open     : received 1, sent 2
KAlive   : received 15, sent 16
Fdb sync : received 0, sent 0
Failover : received 0, sent 0
Conf     : received 1, sent 1

Connections established 1; dropped 0
Local host: 12.1.1.1, Local port: 61000
Foreign host: 12.1.1.2, Foreign port: 46157
remote_sysid: baa7.8606.8b00



Switch# show mac address-table
          Mac Address Table
------------------------------------------
(*) - Security Entry
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

Используйте следующую команду для отображения информации о таблице MAC-адресов на коммутаторе Switch2

```
Switch# show mlag
MLAG configuration:
-----------------
role         : Slave
local_sysid : baa7.8606.8b00
mlag_sysid   : ea90.aecc.cc00
peer-link    : eth-0-9
peer conf    : Yes

Switch# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up

Switch# show mlag peer
MLAG neighbor is 12.1.1.1, MLAG version 1
MLAG state = Established, up for 00:14:29
Last read 00:00:48, hold time is 240, keepalive interval is 60 seconds
Received 19 messages,Sent 19 messages
Open     : received 1, sent 1
KAlive   : received 17, sent 17
Fdb sync : received 0, sent 0
```

```
Failover : received 0, sent 0
Conf     : received 1, sent 1

Connections established 1; dropped 0
Local host: 12.1.1.2, Local port: 46157
Foreign host: 12.1.1.1, Foreign port: 61000
remote_sysid: ea90.aecc.cc00
```

Для отображения информации о MLAG на коммутаторе Switch2 используйте следующую команду:

```
Switch# show mac address-table
          Mac Address Table
------------------------------------------
(*) - Security Entry
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

3.16.3.2 Защита пересылки данных уровня 2 (Layer 2)

3.16.3.3 Топология

3.16.3.4 Требования и условия

Хост 1 и Хост 2 находятся в одном сетевом разделе, их две сетевые карты (NIC) используют метод Active-Active для подключения к устройству MLAG, и им требуется сеть без зацикливания. Хост 1 и Хост 2 реализуют межсетевое взаимодействие уровня 2. MLAG1 будет использовать динамический канал агрегации, MLAG 2 — статический канал агрегации.

3.16.3.5 Этапы настройки

Шаг 1. Настройка портов для установки соединения MLAG PEER.

Для двух устройств, использующих протокол MLAG, выберите как минимум два канала 10G для соединения (если и сервисный порт имеет скорость 10G).

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1 (config)# interface range eth-0-9 - 10
Switch_1 (config-if-range)# no shutdown
Switch_1 (config-if-range)# lacp timeout short
Switch_1 (config-if-range)# channel-group 55 mode active
Switch_1 (config-if-range)# exit
Switch_1 (config)# interface agg 55
Switch_1 (config-if)# spanning-tree port disable
Switch_1 (config-if)# switchport mode trunk
Switch_1 (config-if)# switchport trunk allowed vlan all
Switch_1 (config-if)#end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# interface range eth-0-9 - 10
Switch_2 (config-if-range)# no shutdown
Switch_2 (config-if-range)# lacp timeout short
Switch_2(config-if-range)# channel-group 55 mode active
Switch_2(config-if-range)# exit
Switch_2(config)# interface agg 55
Switch_2(config-if)# spanning-tree port disable
Switch_2(config-if)# switchport mode trunk
Switch_2(config-if)# switchport trunk allowed vlan all
Switch_2(config-if)#end
```

Шаг 2. Настройка адреса коммуникации для MLAG PEER.

В приведенном примере vlan 4094 используется для настройки коммуникационного адреса MLAG; рекомендуется не подключать сервисный порт к vlan 4094, поскольку vlan 4094 предназначен только для использования в рамках peer-link.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 4094
Switch_1(config-vlan)# exit
Switch_1(config)# interface vlan 4094
Switch_1(config-if)# ip address 10.10.0.1/30
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 4094
Switch_2(config-vlan)# exit
Switch_2(config)# interface vlan 4094
Switch_2(config-if)# ip address 10.10.0.2/30
Switch_2(config-if)# end
```

Шаг 3. Настройка MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# mlag configuration
```

```
Switch_1(config-mlag)# timers mlag 1 5
Switch_1(config-mlag)# peer-link agg55
Switch_1(config-mlag)# peer-address 10.10.0.2
Switch_1(config-mlag)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# mlag configuration
Switch_2(config-mlag)# timers mlag 1 5
Switch_2(config-mlag)# peer-link agg 55
Switch_2(config-mlag)# peer-address 10.10.0.1
Switch_2(config-mlag)# end
```

Шаг 4. Настройка порта MLAG.

Примечание: lacp mlag system-id HHHH.HHHH.HHHH — это определяемый пользователем идентификатор системы LACP. Два устройства в MLAG должны использовать один и тот же идентификатор системы LACP, например: 0000.0000.aaaa; при каскадном соединении двух пар устройств MLAG идентификатор системы LACP должен быть разным для каждой пары MLAG.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# no ip igmp snooping
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 10
Switch_1(config-vlan)# exit
Switch_1(config)# lacp mlag system-id 0000.0000.aaaa
Switch_1(config)# interface eth-0-1
Switch_1(config-if)# no shutdown
Switch_1(config-if)# switchport access vlan 10
Switch_1(config-if)# channel-group 1 mode active
Switch_1(config-if)# exit
Switch_1(config)# interface eth-0-2
Switch_1(config-if)# no shutdown
Switch_1(config-if)# switchport access vlan 10
Switch_1(config-if)# static-channel-group 2
Switch_1(config-if)# exit
Switch_1(config)# interface agg 1
Switch_1(config-if)# mlag 1
Switch_1(config-if)# exit
Switch_1(config)# interface agg 2
Switch_1(config-if)# mlag 2
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# no ip igmp snooping
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 10
Switch_2(config-vlan)# exit
Switch_2(config)# lacp mlag system-id 0000.0000.aaaa
Switch_2(config)# interface eth-0-1
Switch_2(config-if)# no shutdown
Switch_2(config-if)# switchport access vlan 10
Switch_2(config-if)# channel-group 1 mode active
Switch_2(config-if)# exit
Switch_2(config)# interface eth-0-2
Switch_2(config-if)# no shutdown
Switch_2(config-if)# switchport access vlan 10
Switch_2(config-if)# static-channel-group 2
Switch_2(config-if)# exit
Switch_2(config)# interface agg 1
Switch_2(config-if)# mlag 1
Switch_2(config-if)# exit
Switch_2(config)# interface agg 2
Switch_2(config-if)# mlag 2
Switch_2(config-if)# end
```

Шаг 5. Проверка результатов настройки.

Проверьте статус соседей (peer) MLAG, убедитесь, что MLAG находится в established состоянии после настройки:

```
Switch_1# show mlag peer
MLAG neighbor is 10.10.0.2, MLAG version 1
MLAG state = Established, up for 00:00:01
Last read 00:00:01, hold time is 240, keepalive interval is 60 seconds
Received 4 messages,Sent 4 messages
Open      : received 1, sent 1
KAlive    : received 1, sent 1
Fdb sync  : received 0, sent 0
Failover  : received 0, sent 0
Conf      : received 0, sent 0
Syspri    : received 1, sent 1
Peer fdb : received 1, sent 1

Connections established 1; dropped 0
Local host: 10.10.0.1, Local port: 50040
Foreign host: 10.10.0.2, Foreign port: 61000
remote_sysid: 1a53.71e9.c000
```

Проверьте состояние устройств MLAG: одно устройство находится в режиме Master, а другое — в режиме Slave:

```
Switch_1# show mlag
MLAG configuration:
-----------------
role          : Master
local_sysid   : 8e79.b120.2e00
remote_sysid  : 1a53.71e9.c000
mlag_sysid    : 8e79.b120.2e00
local_syspri  : 32768
remote_syspri: 32768
mlag_syspri   : 32768
peer-link     : agg55
peer conf     : Yes
reload-delay  : 300

Switch_2# show mlag
MLAG configuration:
-----------------
role          : Slave
local_sysid   : 1a53.71e9.c000
remote_sysid  : 8e79.b120.2e00
mlag_sysid    : 8e79.b120.2e00
local_syspri  : 32768
remote_syspri: 32768
mlag_syspri   : 32768
peer-link     : agg55
peer conf     : Yes
reload-delay  : 300
```

Проверьте состояние группы MLAG; все интерфейсы должны быть в состоянии UP.

```
Switch_1# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up
2       agg2      up             up
```

3.16.3.6 Домен MLAG в сети уровня 3 (каждая VLAN имеет только один адрес)

3.16.3.7 Топология

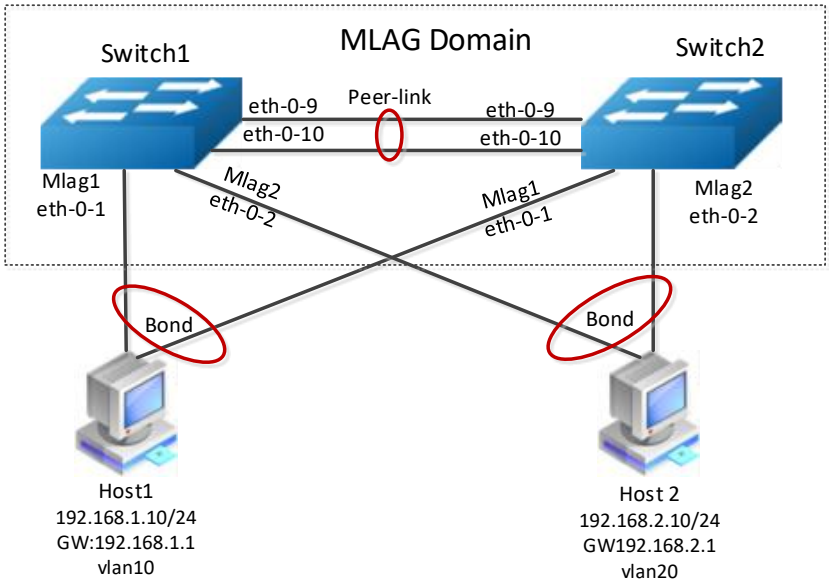


Рисунок 1-2 Схема сетевого шлюза MLAG уровня 3

3.16.3.8 Требования

Хост 1 и Хост 2 используют две сетевые карты с активным подключением к домену MLAG, обеспечивая передачу данных по сети; их шлюз находится на устройстве MLAG и не использует протокол VRRP.

3.16.3.9 Этапы настройки

Примечание: Номер группы каналов 55, используемой для соединения двух коммутаторов в примере конфигурации, может быть изменен в соответствии с различными стандартами плат; использование любого другого номера группы каналов не повлияет на данный сценарий конфигурации.

Шаг 1. Настройки портов соединения для MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1 (config)# interface range eth-0-9 - 10
Switch_1 (config-if-range)# no shutdown
Switch_1 (config-if-range)# lacp timeout short
Switch_1 (config-if-range)# channel-group 55 mode active
Switch_1 (config-if-range)# exit
```

```
Switch_1 (config)# interface agg 55
Switch_1 (config-if)# spanning-tree port disable
Switch_1 (config-if)# switchport mode trunk
Switch_1 (config-if)# switchport trunk allowed vlan all
Switch_1 (config-if)#end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# interface range eth-0-9 - 10
Switch_2 (config-if-range)# no shutdown
Switch_2 (config-if-range)# lacp timeout short
Switch_2(config-if-range)# channel-group 55 mode active
Switch_2(config-if-range)# exit
Switch_2(config)# interface agg 55
Switch_2(config-if)# spanning-tree port disable
Switch_2(config-if)# switchport mode trunk
Switch_2(config-if)# switchport trunk allowed vlan all
Switch_2(config-if)#end
```

Шаг 2. Настройка адреса коммуникации для MLAG PEER

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 4094
Switch_1(config-vlan)# exit
Switch_1(config)# interface vlan 4094
Switch_1(config-if)# ip address 10.10.0.1/30
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 4094
Switch_2(config-vlan)# exit
Switch_2(config)# interface vlan 4094
Switch_2(config-if)# ip address 10.10.0.2/30
Switch_2(config-if)# end
```

Шаг 3. Настройка MLAG PEER

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch_1(config)# mlag configuration
Switch_1(config-mlag)# timers mlag 1 5
Switch_1(config-mlag)# peer-link agg55
Switch_1(config-mlag)# peer-address 10.10.0.2
Switch_1(config-mlag)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# mlag configuration
Switch_2(config-mlag)# timers mlag 1 5
Switch_2(config-mlag)# peer-link agg 55
Switch_2(config-mlag)# peer-address 10.10.0.1
Switch_2(config-mlag)# end
```

Шаг 4. Настройка интерфейса MLAG

В сценарии уровня 3 рекомендуется установить режим короткого таймаута LACP как для сервисного порта коммутатора, так и для порта партнера с помощью команды «lacp timeout short».

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# no ip igmp snooping
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 10,20
Switch_1(config-vlan)# exit
Switch_1(config)# interface eth-0-1
Switch_1(config-if)# no shutdown
Switch_1(config-if)# lacp timeout short
Switch_1(config-if)# switchport access vlan 10
Switch_1(config-if)# channel-group 1 mode active
Switch_1(config-if)# exit
Switch_1(config)# interface eth-0-2
Switch_1(config-if)# no shutdown
Switch_1(config-if)# lacp timeout short
Switch_1(config-if)# switchport access vlan 20
Switch_1(config-if)# channel-group 2 mode active
Switch_1(config-if)# exit
Switch_1(config)# interface agg 1
Switch_1(config-if)# mlag 1
Switch_1(config-if)# exit
Switch_1(config)# interface agg 2
Switch_1(config-if)# mlag 2
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# no ip igmp snooping
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 10,20
Switch_2(config-vlan)# exit
Switch_2(config)# interface eth-0-1
Switch_2(config-if)# no shutdown
Switch_2(config-if)# lacp timeout short
Switch_2(config-if)# switchport access vlan 10
Switch_2(config-if)# channel-group 1 mode active
Switch_2(config-if)# exit
Switch_2(config)# interface eth-0-2
Switch_2(config-if)# no shutdown
Switch_2(config-if)# lacp timeout short
Switch_2(config-if)# switchport access vlan 20
Switch_2(config-if)# channel-group 2 mode active
Switch_2(config-if)# exit
Switch_2(config)# interface agg 1
Switch_2(config-if)# mlag 1
Switch_2(config-if)# exit
Switch_2(config)# interface agg 2
Switch_2(config-if)# mlag 2
Switch_2(config-if)# end
```

Шаг 5. Настройте VARP в качестве шлюза для хоста

Примечание: lacp mlag system-id HHHH.HHHH.HHHH — это определяемый пользователем идентификатор системы LACP. Два устройства в MLAG должны использовать один и тот же идентификатор системы LACP, например: 0000.0000.aaaa; при каскадном соединении двух пар устройств MLAG идентификатор системы LACP должен быть разным для каждой пары MLAG.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# interface vlan 10
Switch_1(config-if)# ip address 192.168.1.253/24
Switch_1(config-if)# ip virtual-router address 192.168.1.1
Switch_1(config-if)# exit
Switch_1(config)# interface vlan 20
Switch_1(config-if)# ip address 192.168.2.253/24
Switch_1(config-if)# ip virtual-router address 192.168.2.1
Switch_1(config-if)# exit
Switch_1(config)# ip virtual-router mac 0000.0000.aaaa
Switch_1(config)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# interface vlan 10
Switch_2(config-if)# ip address 192.168.1.254/24
Switch_2(config-if)# ip virtual-router address 192.168.1.1
Switch_2(config-if)# exit
Switch_2(config)# interface vlan 20
Switch_2(config-if)# ip address 192.168.2.254/24
Switch_2(config-if)# ip virtual-router address 192.168.2.1
Switch_2(config-if)# exit
Switch_2(config)# ip virtual-router mac 0000.0000.aaaa
Switch_2(config)# end
```

Шаг 6. Проверка. результатов настройки

Проверьте статус соседа MLAG; после настройки статус MLAG изменится на Established.

```
Switch_1# show mlag peer
MLAG neighbor is 10.10.0.2, MLAG version 1
MLAG state = Established, up for 00:00:01
Last read 00:00:01, hold time is 240, keepalive interval is 60 seconds
Received 4 messages,Sent 4 messages
Open     : received 1, sent 1
KAlive    : received 1, sent 1
Fdb sync  : received 0, sent 0
Failover  : received 0, sent 0
Conf     : received 0, sent 0
Syspri   : received 1, sent 1
Peer fdb : received 1, sent 1

Connections established 1; dropped 0
Local host: 10.10.0.1, Local port: 50040
Foreign host: 10.10.0.2, Foreign port: 61000
remote_sysid: 1a53.71e9.c000
```

Проверьте состояние устройства MLAG; оба устройства будут находиться в режиме Master/Slave.

```
Switch_1# show mlag
MLAG configuration:
-----------------
role         : Master
local_sysid  : 8e79.b120.2e00
remote_sysid : 1a53.71e9.c000
mlag_sysid   : 8e79.b120.2e00
local_syspri : 32768
remote_syspri: 32768
mlag_syspri  : 32768
peer-link    : agg55
```

```
peer conf     : Yes
reload-delay  : 300

Switch_2# show mlag
MLAG configuration:
-----------------
role          : Slave
local_sysid   : 1a53.71e9.c000
remote_sysid  : 8e79.b120.2e00
mlag_sysid    : 8e79.b120.2e00
local_syspri  : 32768
remote_syspri: 32768
mlag_syspri   : 32768
peer-link     : agg55
peer conf     : Yes
reload-delay  : 300
```

Проверьте состояние группы MLAG; все интерфейсы должны быть в состоянии UP

```
Switch_1# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up
2       agg2      up             up
```

Проверьте состояние и таблицу VARP

```
Switch_1# show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    10.10.0.1              -   8e79.b120.2e00  vlan4094
 Internet    10.10.0.2              0   1a53.71e9.c000  vlan4094
 Internet    192.168.1.1            -   0000.0000.0001  vlan10
 Internet    192.168.1.253          -   8e79.b120.2e00  vlan10
 Internet    192.168.2.1            -   0000.0000.0001  vlan20
 Internet    192.168.2.253          -   8e79.b120.2e00  vlan20
```

3.16.3.10 Домен MLAG в сети уровня 3 (каждая VLAN имеет несколько адресов)

3.16.3.11 Топология

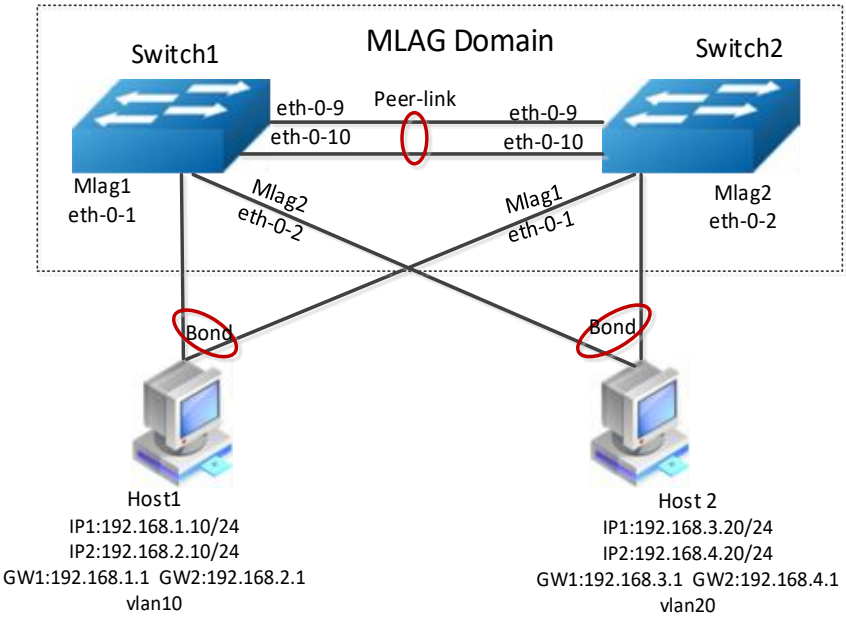


Рисунок 25 – Схема сетевого шлюза MLAG уровня 3

3.16.3.12 Требования

Хост 1 и Хост 2 используют две сетевые карты с активным режимом подключения к устройству MLAG, обеспечивая сетевое взаимодействие между подсетями; их сетевой шлюз развернут на устройстве MLAG, и он имеет несколько IP-адресов в одной и той же VLAN (оба коммутатора являются сетевым шлюзом для всех этих сетей).

Шаг 1. Настройка портов межсоединения MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1 (config)# interface range eth-0-9 - 10
Switch_1 (config-if-range)# no shutdown
Switch_1 (config-if-range)# lacp timeout short
Switch_1 (config-if-range)# channel-group 55 mode active
Switch_1 (config-if-range)# exit
Switch_1 (config)# interface agg 55
Switch_1 (config-if)# spanning-tree port disable
Switch_1 (config-if)# switchport mode trunk
Switch_1 (config-if)# switchport trunk allowed vlan all
Switch_1 (config-if)#end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# interface range eth-0-9 – 10
Switch_2 (config-if-range)# no shutdown
Switch_2 (config-if-range)# lacp timeout short
Switch_2(config-if-range)# channel-group 55 mode active
Switch_2(config-if-range)# exit
Switch_2(config)# interface agg 55
Switch_2(config-if)# spanning-tree port disable
Switch_2(config-if)# switchport mode trunk
Switch_2(config-if)# switchport trunk allowed vlan all
Switch_2(config-if)#end
```

Шаг 2. Настройка адреса связи для MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 4094
Switch_1(config-vlan)# exit
Switch_1(config)# interface vlan 4094
Switch_1(config-if)# ip address 10.10.0.1/30
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 4094
Switch_2(config-vlan)# exit
Switch_2(config)# interface vlan 4094
Switch_2(config-if)# ip address 10.10.0.2/30
Switch_2(config-if)# end
```

Шаг 3. Настройка MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# mlag configuration
Switch_1(config-mlag)# timers mlag 1 5
Switch_1(config-mlag)# peer-link agg55
Switch_1(config-mlag)# peer-address 10.10.0.2
Switch_1(config-mlag)# end
```

SWITCH 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# mlag configuration
Switch_2(config-mlag)# timers mlag 1 5
Switch_2(config-mlag)# peer-link agg 55
Switch_2(config-mlag)# peer-address 10.10.0.1
Switch_2(config-mlag)# end
```

Шаг 4. Настройка порта MLAG.

SWITCH 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# no ip igmp snooping
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 10,20
Switch_1(config-vlan)# exit
Switch_1(config)# interface eth-0-1
Switch_1(config-if)# no shutdown
Switch_1(config-if)# lacp timeout short
Switch_1(config-if)# switchport access vlan 10
Switch_1(config-if)# channel-group 1 mode active
Switch_1(config-if)# exit
Switch_1(config)# interface eth-0-2
Switch_1(config-if)# no shutdown
Switch_1(config-if)# lacp timeout short
Switch_1(config-if)# switchport access vlan 20
Switch_1(config-if)# channel-group 2 mode active
Switch_1(config-if)# exit
Switch_1(config)# interface agg 1
Switch_1(config-if)# mlag 1
Switch_1(config-if)# exit
Switch_1(config)# interface agg 2
Switch_1(config-if)# mlag 2
Switch_1(config-if)# end
```

SWITCH 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# no ip igmp snooping
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 10,20
Switch_2(config-vlan)# exit
Switch_2(config)# interface eth-0-1
Switch_2(config-if)# no shutdown
Switch_2(config-if)# lacp timeout short
Switch_2(config-if)# switchport access vlan 10
```

```
Switch_2(config-if)# channel-group 1 mode active
Switch_2(config-if)# exit
Switch_2(config)# interface eth-0-2
Switch_2(config-if)# no shutdown
Switch_2(config-if)# lacp timeout short
Switch_2(config-if)# switchport access vlan 20
Switch_2(config-if)# channel-group 2 mode active
Switch_2(config-if)# exit
Switch_2(config)# interface agg 1
Switch_2(config-if)# mlag 1
Switch_2(config-if)# exit
Switch_2(config)# interface agg 2
Switch_2(config-if)# mlag 2
Switch_2(config-if)# end
```

Шаг 5. Настройте VARP в качестве шлюза для хоста

SWITCH 1

IP-адрес интерфейса VLAN должен отличаться от IP-адреса виртуального маршрутизатора.

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# interface vlan 10
Switch_1(config-if)# ip address 192.168.10.253/24
Switch_1(config-if)# ip virtual-router address 192.168.1.1/24
Switch_1(config-if)# ip virtual-router address 192.168.2.1/24
Switch_1(config-if)# exit
Switch_1(config)# interface vlan 20
Switch_1(config-if)# ip address 192.168.20.253/24
Switch_1(config-if)# ip virtual-router address 192.168.3.1/24
Switch_1(config-if)# ip virtual-router address 192.168.4.1/24
Switch_1(config-if)# exit
Switch_1(config)# ip virtual-router mac 0.0.1
Switch_1(config)# end
```

SWITCH 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# interface vlan 10
Switch_2(config-if)# ip address 192.168.10.254/24
Switch_2(config-if)# ip virtual-router address 192.168.1.1/24
Switch_2(config-if)# ip virtual-router address 192.168.2.1/24
Switch_2(config-if)# exit
Switch_2(config)# interface vlan 20
Switch_2(config-if)# ip address 192.168.20.254/24
Switch_2(config-if)# ip virtual-router address 192.168.3.1/24
Switch_2(config-if)# ip virtual-router address 192.168.4.1/24
Switch_2(config-if)# exit
```

```
Switch_2(config)# ip virtual-router mac 0.0.1
Switch_2(config)# end
```

Шаг 6. Проверка.

Проверьте статус соседа MLAG; после настройки MLAG он должен быть в статусе Established.

```
Switch_1# show mlag peer
MLAG neighbor is 10.10.0.2, MLAG version 1
MLAG state = Established, up for 00:00:01
Last read 00:00:01, hold time is 240, keepalive interval is 60 seconds
Received 4 messages,Sent 4 messages
Open      : received 1, sent 1
KAlive    : received 1, sent 1
Fdb sync  : received 0, sent 0
Failover  : received 0, sent 0
Conf      : received 0, sent 0
Syspri    : received 1, sent 1
Peer fdb  : received 1, sent 1

Connections established 1; dropped 0
Local host: 10.10.0.1, Local port: 50040
Foreign host: 10.10.0.2, Foreign port: 61000
remote_sysid: 1a53.71e9.c000
```

Проверьте состояние устройства MLAG: оба устройства находятся в режиме Master/Slave.

```
Switch_1# show mlag
MLAG configuration:
-----------------
role          : Master
local_sysid   : 8e79.b120.2e00
remote_sysid  : 1a53.71e9.c000
mlag_sysid    : 8e79.b120.2e00
local_syspri  : 32768
remote_syspri: 32768
mlag_syspri   : 32768
peer-link     : agg55
peer conf     : Yes
reload-delay  : 300

Switch_2# show mlag
MLAG configuration:
-----------------
role          : Slave
local_sysid   : 1a53.71e9.c000
remote_sysid  : 8e79.b120.2e00
mlag_sysid    : 8e79.b120.2e00
```

```
local_syspri : 32768
remote_syspri: 32768
mlag_syspri  : 32768
peer-link    : agg55
peer conf    : Yes
reload-delay : 300
```

Проверьте состояние группы MLAG; все интерфейсы должны быть активны (UP).

```
Switch_1# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up
2       agg2      up             up
```

Проверьте состояние и таблицу VARP

```
Switch_1# show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    10.10.0.1              -   8e79.b120.2e00  vlan4094
 Internet    10.10.0.2              0   1a53.71e9.c000  vlan4094
 Internet    192.168.1.1            -   0000.0000.0001  vlan10
 Internet    192.168.2.1            -   0000.0000.0001  vlan10
 Internet    192.168.10.253         -   8e79.b120.2e00  vlan10
 Internet    192.168.3.1            -   0000.0000.0001  vlan20
 Internet    192.168.4.1            -   0000.0000.0001  vlan20
 Internet    192.168.20.253         -   8e79.b120.2e00  vlan20
```

3.16.3.13 MLAG на orphan портах

Orphan порт - сетевой интерфейс, подключенный только к одному коммутатору в паре MLAG, не имеющий двойного подключения к обоим.

3.16.3.14 Топология

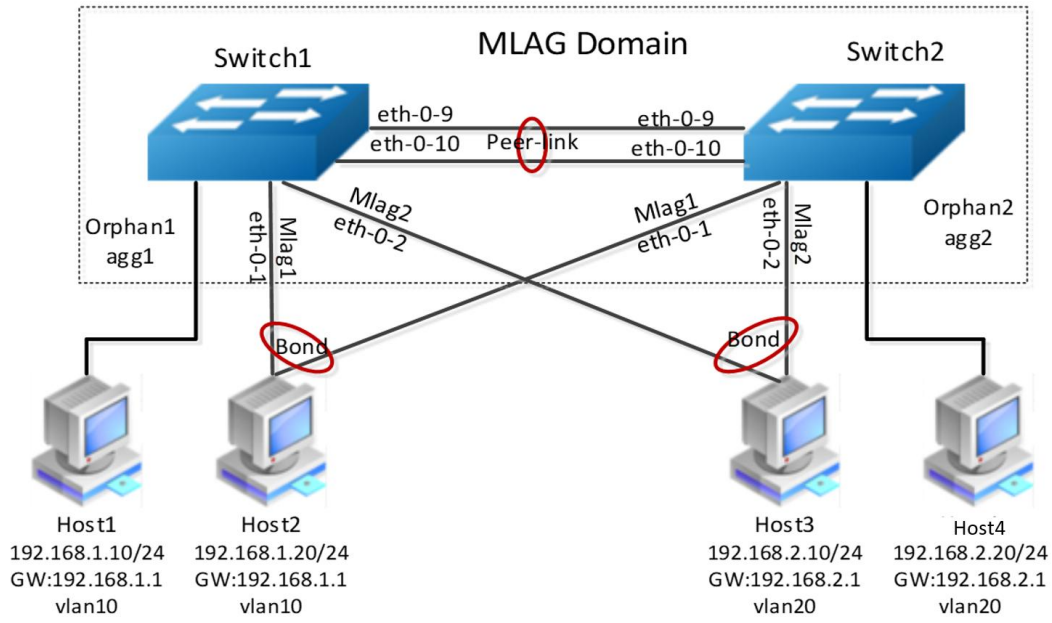


Рисунок 26 – MLAG orphan порт

3.16.3.15 Требования и условия

Хост 1 и Хост 4 используют одну сетевую карту для подключения к устройству MLAG, Хост 2 и Хост 3 используют две сетевые карты с активным режимом подключения к устройству MLAG, обеспечивая сетевое взаимодействие между сетями; их сетевой шлюз развернут на устройстве MLAG и не использует протокол VRRP.

Шаг 1. Настройка портов межсоединения MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1 (config)# interface range eth-0-9 - 10
Switch_1 (config-if-range)# no shutdown
Switch_1 (config-if-range)# lacp timeout short
Switch_1 (config-if-range)# channel-group 55 mode active
Switch_1 (config-if-range)# exit
Switch_1 (config)# interface agg 55
Switch_1 (config-if)# spanning-tree port disable
Switch_1 (config-if)# switchport mode trunk
Switch_1 (config-if)# switchport trunk allowed vlan all
Switch_1 (config-if)#end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# interface range eth-0-9 - 10
Switch_2 (config-if-range)# no shutdown
Switch_2 (config-if-range)# lacp timeout short
Switch_2(config-if-range)# channel-group 55 mode active
Switch_2(config-if-range)# exit
Switch_2(config)# interface agg 55
Switch_2(config-if)# spanning-tree port disable
Switch_2(config-if)# switchport mode trunk
Switch_2(config-if)# switchport trunk allowed vlan all
Switch_2(config-if)#end
```

Шаг 2. Настройка адреса связи MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 4094
```

```
Switch_1(config-vlan)# exit
Switch_1(config)# interface vlan 4094
Switch_1(config-if)# ip address 10.10.0.1/30
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 4094
Switch_2(config-vlan)# exit
Switch_2(config)# interface vlan 4094
Switch_2(config-if)# ip address 10.10.0.2/30
Switch_2(config-if)# end
```

Шаг 3. Настройка MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# mlag configuration
Switch_1(config-mlag)# timers mlag 1 5
Switch_1(config-mlag)# peer-link agg55
Switch_1(config-mlag)# peer-address 10.10.0.2
Switch_1(config-mlag)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# mlag configuration
Switch_2(config-mlag)# timers mlag 1 5
Switch_2(config-mlag)# peer-link agg 55
Switch_2(config-mlag)# peer-address 10.10.0.1
Switch_2(config-mlag)# end
```

Шаг 4. Настройка интерфейса MLAG Interface и orphan порта.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# no ip igmp snooping
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 10,20
Switch_1(config-vlan)# exit
Switch_1(config)# interface eth-0-20
Switch_1(config-if)# no shutdown
Switch_1(config-if)# switchport access vlan 10
```

```
Switch_2(config-if)# exit
Switch_1(config)# interface eth-0-21
Switch_1(config-if)# no shutdown
Switch_1(config-if)# lacp timeout short
Switch_1(config-if)# switchport access vlan 10
Switch_1(config-if)# channel-group 1 mode active
Switch_1(config-if)# exit
Switch_1(config)# interface eth-0-22
Switch_1(config-if)# no shutdown
Switch_1(config-if)# lacp timeout short
Switch_1(config-if)# switchport access vlan 20
Switch_1(config-if)# channel-group 2 mode active
Switch_1(config-if)# exit
Switch_1(config)# interface agg 1
Switch_1(config-if)# mlag 1
Switch_1(config-if)# exit
Switch_1(config)# interface agg 2
Switch_1(config-if)# mlag 2
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# no ip igmp snooping
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 10,20
Switch_2(config-vlan)# exit
Switch_2(config)# interface eth-0-21
Switch_2(config-if)# no shutdown
Switch_2(config-if)# lacp timeout short
Switch_2(config-if)# switchport access vlan 10
Switch_2(config-if)# channel-group 1 mode active
Switch_2(config-if)# exit
Switch_2(config)# interface eth-0-22
Switch_2(config-if)# no shutdown
Switch_2(config-if)# lacp timeout short
Switch_2(config-if)# switchport access vlan 20
Switch_2(config-if)# channel-group 2 mode active
Switch_2(config-if)# exit
Switch_2(config)# interface agg 1
Switch_2(config-if)# mlag 1
Switch_2(config-if)# exit
Switch_2(config)# interface agg 2
Switch_2(config-if)# mlag 2
Switch_2(config)# interface eth-0-23
Switch_2(config-if)# no shutdown
Switch_2(config-if)# switchport access vlan 20
```

```
Switch_2(config-if)# exit
Switch_2(config-if)# end
```

Шаг 5. Настройте VARP в качестве шлюза для хоста.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# interface vlan 10
Switch_1(config-if)# ip address 192.168.1.253/24
Switch_1(config-if)# ip virtual-router address 192.168.1.1
Switch_1(config-if)# exit
Switch_1(config)# interface vlan 20
Switch_1(config-if)# ip address 192.168.2.253/24
Switch_1(config-if)# ip virtual-router address 192.168.2.1
Switch_1(config-if)# exit
Switch_1(config)# ip virtual-router mac 0.0.1
Switch_1(config)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# interface vlan 10
Switch_2(config-if)# ip address 192.168.1.254/24
Switch_2(config-if)# ip virtual-router address 192.168.1.1
Switch_2(config-if)# exit
Switch_2(config)# interface vlan 20
Switch_2(config-if)# ip address 192.168.2.254/24
Switch_2(config-if)# ip virtual-router address 192.168.2.1
Switch_2(config-if)# exit
Switch_2(config)# ip virtual-router mac 0.0.1
Switch_2(config)# end
```

3.16.3.16 Каскадирование нескольких доменов MLAG

3.16.3.17 Топология

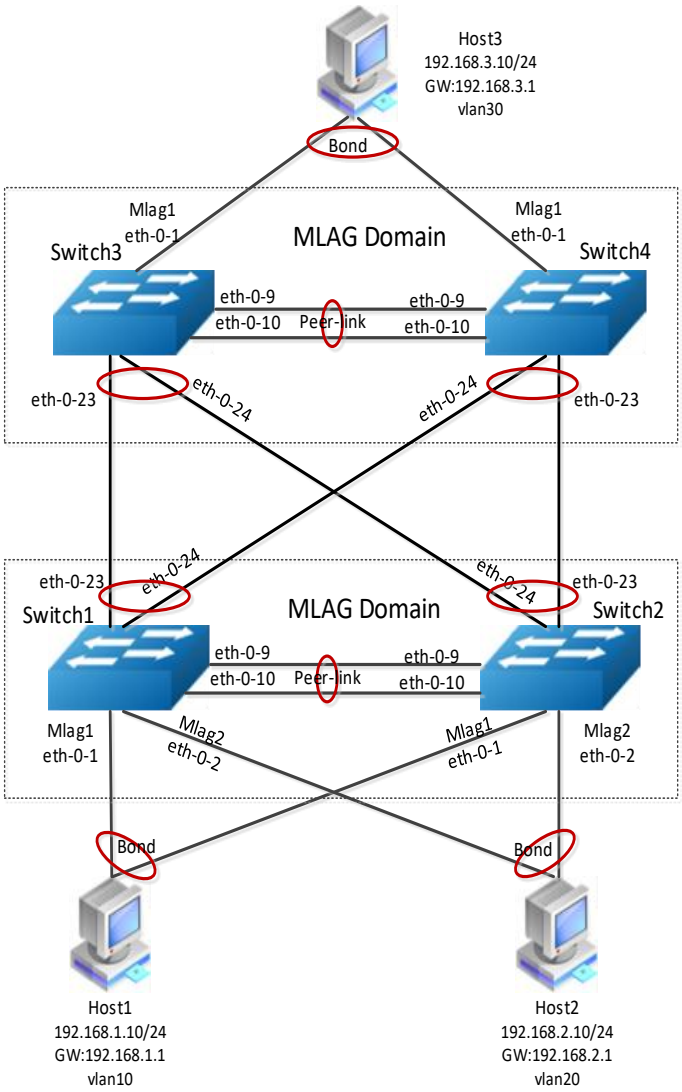


Рисунок 27 – Сетевая диаграмма каскадирования доменов MLAG

3.16.3.18 Требования и условия

По мере увеличения размеров сети иногда требуется каскадирование нескольких MLAG, обеспечивающих соединения между хостами 1, 2 и 3 и с развернутым шлюзом на коммутаторах 3 и 4. При этом сообщения, отправляемые хостом 1 и 2, должны проходить через уровень 2 для пересылки на коммутаторы 3 и 4.

Шаг 1. Настройка портов межсоединения MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1 (config)# interface range eth-0-9 - 10
Switch_1 (config-if-range)# no shutdown
Switch_1 (config-if-range)# lacp timeout short
Switch_1 (config-if-range)# channel-group 55 mode active
Switch_1 (config-if-range)# exit
Switch_1 (config)# interface agg 55
Switch_1 (config-if)# spanning-tree port disable
Switch_1 (config-if)# switchport mode trunk
Switch_1 (config-if)# switchport trunk allowed vlan all
Switch_1 (config-if)#end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# interface range eth-0-9 - 10
Switch_2 (config-if-range)# no shutdown
Switch_2 (config-if-range)# lacp timeout short
Switch_2(config-if-range)# channel-group 55 mode active
Switch_2(config-if-range)# exit
Switch_2(config)# interface agg 55
Switch_2(config-if)# spanning-tree port disable
Switch_2(config-if)# switchport mode trunk
Switch_2(config-if)# switchport trunk allowed vlan all
Switch_2(config-if)#end
```

Switch 3

```
Switch_3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_3 (config)# interface range eth-0-9 - 10
Switch_3 (config-if-range)# no shutdown
Switch_3 (config-if-range)# lacp timeout short
Switch_3(config-if-range)# channel-group 55 mode active
Switch_3 (config-if-range)# exit
Switch_3 (config)# interface agg 55
Switch_3 (config-if)# spanning-tree port disable
Switch_3 (config-if-range)# switchport mode trunk
Switch_3 (config-if-range)# switchport trunk allowed vlan all
Switch_3 (config-if)#exit
```

Switch 4

```
Switch_4# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_4(config)# interface range eth-0-9 - 10
Switch_4 (config-if-range)# no shutdown
Switch_4 (config-if-range)# lacp timeout short
Switch_4(config-if-range)# static-channel-group 55
```

```
Switch_4(config-if-range)# exit
Switch_4(config)# interface agg 55
Switch_4(config-if)# spanning-tree port disable
Switch_4(config-if-range)# switchport mode trunk
Switch_4(config-if-range)# switchport trunk allowed vlan all
Switch_4(config-if)#exit
```

Шаг 2. Настройка адреса связи для MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 4094
Switch_1(config-vlan)# exit
Switch_1(config)# interface vlan 4094
Switch_1(config-if)# ip address 10.10.0.1/30
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 4094
Switch_2(config-vlan)# exit
Switch_2(config)# interface vlan 4094
Switch_2(config-if)# ip address 10.10.0.2/30
Switch_2(config-if)# end
```

Switch 3

```
Switch_3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_3(config)# vlan database
Switch_3(config-vlan)# vlan 4094
Switch_3(config-vlan)# exit
Switch_3(config)# interface vlan 4094
Switch_3(config-if)# ip address 10.10.0.5/30
Switch_3(config-if)# end
```

Switch 4

```
Switch_4# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_4(config)# vlan database
Switch_4(config-vlan)# vlan 4094
Switch_4(config-vlan)# exit
Switch_4(config)# interface vlan 4094
```

```
Switch_4(config-if)# ip address 10.10.0.6/30
Switch_4(config-if)# end
```

Шаг 3. Настройка MLAG PEER.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# mlag configuration
Switch_1(config-mlag)# timers mlag 1 5
Switch_1(config-mlag)# peer-link agg55
Switch_1(config-mlag)# peer-address 10.10.0.2
Switch_1(config-mlag)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# mlag configuration
Switch_2(config-mlag)# timers mlag 1 5
Switch_2(config-mlag)# peer-link agg 55
Switch_2(config-mlag)# peer-address 10.10.0.1
Switch_2(config-mlag)# end
```

Switch 3

```
Switch_3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_3(config)# mlag configuration
Switch_3(config-mlag)# timers mlag 1 5
Switch_3(config-mlag)# peer-link agg55
Switch_3(config-mlag)# peer-address 10.10.0.6
Switch_3(config-mlag)# end
```

Switch 4

```
Switch_4# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_4(config)# mlag configuration
Switch_4(config-mlag)# timers mlag 1 5
Switch_4(config-mlag)# peer-link agg 55
Switch_4(config-mlag)# peer-address 10.10.0.5
Switch_4(config-mlag)# end
```

Шаг 4. Настройка соединительного порта между коммутаторами 1, 2 и коммутаторами 3, 4.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# vlan database
Switch_1(config)# no ip igmp snooping
Switch_1(config-vlan)# vlan 10,20
Switch_1(config-vlan)# exit
Switch_1(config)# interface range eth-0-23 - 24
Switch_1(config-if-range)# no shutdown
Switch_1(config-if-range)# lacp timeout short
Switch_1(config-if-range)# switchport mode trunk
Switch_1(config-if-range)# switchport trunk allowed vlan add 10,20
Switch_1(config-if-range)# channel-group 54 mode active
Switch_1(config-if-range)# exit
Switch_1(config)# interface agg 54
Switch_1(config-if)# mlag 54
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# no ip igmp snooping
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 10,20
Switch_2(config-vlan)# exit
Switch_2(config)# interface range eth-0-23 - 24
Switch_2(config-if-range)# no shutdown
Switch_2(config-if-range)# lacp timeout short
Switch_2(config-if-range)# switchport mode trunk
Switch_2(config-if-range)# switchport trunk allowed vlan add 10,20
Switch_2(config-if-range)# channel-group 54 mode active
Switch_2(config-if-range)# exit
Switch_2(config)# interface agg 54
Switch_2(config-if)# mlag 54
Switch_2(config-if)# end
```

Switch 3

```
Switch_3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_3(config)# no ip igmp snooping
Switch_3(config)# vlan database
Switch_3(config-vlan)# vlan 10,20
Switch_3(config-vlan)# exit
Switch_3(config)# interface range eth-0-23 - 24
Switch_3(config-if-range)# no shutdown
Switch_3(config-if-range)# lacp timeout short
Switch_3(config-if-range)# switchport mode trunk
Switch_3(config-if-range)# switchport trunk allowed vlan add 10,20
Switch_3(config-if-range)# channel-group 54 mode active
```

```
Switch_3(config-if-range)# exit
Switch_3(config)# interface agg 54
Switch_3(config-if)# mlag 54
Switch_3(config-if)# end
```

Switch 4

```
Switch_4# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_4(config)# no ip igmp snooping
Switch_4(config)# vlan database
Switch_4(config-vlan)# vlan 10,20
Switch_4(config-vlan)# exit
Switch_4(config)# interface range eth-0-23 - 24
Switch_4(config-if-range)# no shutdown
Switch_4(config-if-range)# lacp timeout short
Switch_4(config-if-range)# switchport mode trunk
Switch_4(config-if-range)# switchport trunk allowed vlan add 10,20
Switch_4(config-if-range)# channel-group 54 mode active
Switch_4(config-if-range)# exit
Switch_4(config)# interface agg 54
Switch_4(config-if)# mlag 54
Switch_4(config-if)# end
```

Шаг 5. Настройка группы MLAG для подключения хостов.

Switch 1

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# vlan database
Switch_1(config-vlan)# vlan 10,20
Switch_1(config-vlan)# exit
Switch_1(config)# mlag lacp system-id 0000.0000.aabb
Switch_1(config)# interface eth-0-1
Switch_1(config-if)# no shutdown
Switch_1(config-if)# switchport access vlan 10
Switch_1(config-if)# channel-group 1 mode active
Switch_1(config-if)# exit
Switch_1(config)# interface eth-0-2
Switch_1(config-if)# no shutdown
Switch_1(config-if)# switchport access vlan 20
Switch_1(config-if)# channel-group 2 mode active
Switch_1(config-if)# exit
Switch_1(config)# interface agg 1
Switch_1(config-if)# mlag 1
Switch_1(config-if)# exit
Switch_1(config)# interface agg 2
```

```
Switch_1(config-if)# mlag 2
Switch_1(config-if)# end
```

Switch 2

```
Switch_2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_2(config)# vlan database
Switch_2(config-vlan)# vlan 10,20
Switch_2(config-vlan)# exit
Switch_2(config)# mlag lacp system-id 0000.0000.aabb
Switch_2(config)# interface eth-0-1
Switch_2(config-if)# no shutdown
Switch_2(config-if)# switchport access vlan 10
Switch_2(config-if)# channel-group 1 mode active
Switch_2(config-if)# exit
Switch_2(config)# interface eth-0-2
Switch_2(config-if)# no shutdown
Switch_2(config-if)# switchport access vlan 20
Switch_2(config-if)# channel-group 2 mode active
Switch_2(config-if)# exit
Switch_2(config)# interface agg 1
Switch_2(config-if)# mlag 1
Switch_2(config-if)# exit
Switch_2(config)# interface agg 2
Switch_2(config-if)# mlag 2
Switch_2(config-if)# end
```

Switch 3

```
Switch_3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_3(config)# vlan database
Switch_3(config-vlan)# vlan 30
Switch_3(config-vlan)# exit
Switch_3(config)# interface eth-0-1
Switch_3(config-if)# no shutdown
Switch_3(config-if)# lacp timeout short
Switch_3(config-if)# switchport access vlan 30
Switch_3(config-if)# channel-group 1 mode active
Switch_3(config-if)# exit
Switch_3(config)# interface agg 1
Switch_3(config-if)# mlag 1
Switch_3(config-if)# end
```

Switch 4

```
Switch_4# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_4(config)# vlan database
Switch_4(config-vlan)# vlan 30
```

```
Switch_4(config-vlan)# exit
Switch_4(config)# interface eth-0-1
Switch_4(config-if)# no shutdown
Switch_4(config-if)# lacp timeout short
Switch_4(config-if)# switchport access vlan 30
Switch_4(config-if)# channel-group 1 mode active
Switch_4(config-if)# exit
Switch_4(config)# interface agg 1
Switch_4(config-if)# mlag 1
Switch_4(config-if)# end
```

Шаг 6. Настройте VARP в качестве шлюза для хоста.

Шлюз развернут на коммутаторах 3, 4, коммутаторы 1 и 2 настраивать не нужно.

Switch 3

```
Switch_3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_3(config)# interface vlan 10
Switch_3(config-if)# ip address 192.168.1.253/24
Switch_3(config-if)# ip virtual-router address 192.168.1.1
Switch_3(config-if)# exit
Switch_3(config)# interface vlan 20
Switch_3(config-if)# ip address 192.168.2.253/24
Switch_3(config-if)# ip virtual-router address 192.168.2.1
Switch_3(config-if)# exit
Switch_3(config)# interface vlan 30
Switch_3(config-if)# ip address 192.168.3.253/24
Switch_3(config-if)# ip virtual-router address 192.168.3.1
Switch_3(config-if)# exit
Switch_3(config)# ip virtual-router mac 0.0.1
Switch_3(config)# end
```

Switch 4

```
Switch_4# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_4(config)# interface vlan 10
Switch_4(config-if)# ip address 192.168.1.254/24
Switch_4(config-if)# ip virtual-router address 192.168.1.1
Switch_4(config-if)# exit
Switch_4(config)# interface vlan 20
Switch_4(config-if)# ip address 192.168.2.254/24
Switch_4(config-if)# ip virtual-router address 192.168.2.1
Switch_4(config-if)# exit
Switch_4(config)# interface vlan 30
Switch_4(config-if)# ip address 192.168.3.254/24
Switch_4(config-if)# ip virtual-router address 192.168.3.1
Switch_4(config-if)# exit
```

```
Switch_4(config)# ip virtual-router mac 0.0.1
Switch_4(config)# end
```

Шаг 7. Проверка.

Проверьте статус соседа MLAG; после настройки MLAG он должен быть в состоянии Established.

```
Switch_1# show mlag peer
MLAG neighbor is 10.10.0.2, MLAG version 1
MLAG state = Established, up for 00:00:01
Last read 00:00:01, hold time is 240, keepalive interval is 60 seconds
Received 4 messages,Sent 4 messages
Open     : received 1, sent 1
KAlive    : received 1, sent 1
Fdb sync  : received 0, sent 0
Failover  : received 0, sent 0
Conf     : received 0, sent 0
Syspri   : received 1, sent 1
Peer fdb : received 1, sent 1

Connections established 1; dropped 0
Local host: 10.10.0.1, Local port: 50040
Foreign host: 10.10.0.2, Foreign port: 61000
remote_sysid: 1a53.71e9.c000
```

Проверьте состояние устройства MLAG: оба устройства находятся в режиме Master/Slave

```
Switch_1# show mlag
MLAG configuration:
-----------------
role          : Master
local_sysid   : 8e79.b120.2e00
remote_sysid  : 1a53.71e9.c000
mlag_sysid    : 8e79.b120.2e00
local_syspri  : 32768
remote_syspri: 32768
mlag_syspri   : 32768
peer-link     : agg55
peer conf     : Yes
reload-delay  : 300

Switch_2# show mlag
MLAG configuration:
-----------------
role          : Slave
local_sysid   : 1a53.71e9.c000
remote_sysid  : 8e79.b120.2e00
mlag_sysid    : 8e79.b120.2e00
```

```
local_syspri : 32768
remote_syspri: 32768
mlag_syspri  : 32768
peer-link    : agg55
peer conf    : Yes
reload-delay : 300
```

Проверьте состояние группы MLAG; все интерфейсы должны быть активны (UP)

```
Switch_1# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up
2       agg2      up             up
54      agg54     up             up
```

Проверьте состояние и таблицу VARP

```
Switch_3# show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    10.10.0.5              -    50bd.ac96.f800  vlan4094
 Internet    10.10.0.6              0    fef0.6b89.5800  vlan4094
 Internet    192.168.1.1            -   0000.0000.0001  vlan10
 Internet    192.168.1.253          -   50bd.ac96.f800   vlan10
Internet    192.168.2.1            -   0000.0000.0001  vlan20
 Internet    192.168.2.253          -   50bd.ac96.f800   vlan20
Internet    192.168.3.1            -   0000.0000.0001  vlan30
 Internet    192.168.3.253          -   50bd.ac96.f800   vlan30
```

После настройки, от каждого хоста следует использовать Ping до любого адреса во внешней сети для проверки прохождения пакетов через шлюз. Также можно использовать ping между хостами.

3.17 Настройка балансировки нагрузки по хэш

3.17.1 Настройка хэш для Linkagg

3.17.1.1 Общие положения

Linkagg может объединять несколько физических интерфейсов в логический канал для повышения производительности и резервирования. При использовании Linkagg для передачи пакетов может происходить передача одного и того же потока данных через разные физические интерфейсы. Из-за этого встречное оборудование может получать пакеты в неупорядоченном виде. Чтобы избежать этого явления, Linkagg может анализировать данные пакетов, получать хеш-значение, а затем выбирать подходящий физический интерфейс для передачи пакетов. Это повышает эффективность балансировки нагрузки Linkagg.

3.17.1.2 Configuring Linkagg Hash Globally

Следующие шаги показывают, как установить хэш-функцию для unicast и другого трафика.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите хэш-поле.

```
Switch(config)# hash-field user
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip ipsa
Switch(config-hash-field)# exit
```

Шаг 3. Установите хеш-значение глобально.

```
Switch(config)# hash-value global
Switch(config-hash-value-global)# port-channel select user
Switch(config-hash-value-global)# end
```

Шаг 4. Проверка.

Для отображения информации о поле хеша используйте следующую команду:

```
Switch# show hash-field user
hash-field name: user
 Option                                Control type
------------------------------------------------------------------------
 ipv6 address compress                 xor
 hash seed                             user set (0)
 hash arithmetic                       xor
 hash symmetry                         disable
 ip                                    enable
 ipv6                                  enable
 mpls                                  enable
------------------------------------------------------------------------
 hash field select
 Packet                HashField
------------------------------------------------------------------------
 l2:                   macsa

 ip:                   ipsa

 ipv6:                 ipsa                  ipda
                       l4-sourceport         l4-destport
                       ip-protocol

 gre:                  ipsa                  ipda
                       gre-key
```

```
vxlan:                  vni                     outer-l4-sourceport
                        outer-ipda              outer-ipsa

nvgre:                  vsid                    outer-ipda
                        outer-ipsa

mpls:                   top-label               2nd-label

vpws:                   top-label               2nd-label

vpls(inner-l2):         inner-macda             inner-macsa

vpls(inner-l3):         inner-ipda              inner-ipsa

l3vpn:                  inner-ipsa              inner-ipda
                        inner-ip-protocol       inner-l4-sourceport
                        inner-l4-destport
```

Для отображения информации о глобальном хеш-значении используйте следующую команду:

```
Switch# show hash-value global
LBT:load balance type          LBM :load balance mode
PT :packet type                HF  :hash field
HA :hash arithmetic
hash-value global
 LBT             LBM             PT              HF              HA
------------------------------------------------------------------------
 port-channel    -               all             user            xor
 ecmp            -               all             ecmp            xor
 ecmp            flow id         all             ecmp            xor
 entropy         -               all             ecmp            xor
------------------------------------------------------------------------
 Efd hash field select:
  macsa                  macda
  ipsa                   ipda
  sourceport             destport
  ip-protocol
```

3.17.1.3 Настройка хэша для Linkagg (input)

Следующие шаги показывают, как установить хеш для одноадресного (unicast) трафика на входящем Linkagg интерфейсе, при этом приоритет конфигурации должен быть выше, чем на исходящем. Когда значение хеша применяется на входе порта Linkagg, это значение хеша будет применяться и к порту-участнику порта Linkagg.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите хэш-поле.

```
Switch(config)# hash-field user
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip ipsa
Switch(config-hash-field)# exit
```

Шаг 3. Установите хеш-значение.

```
Switch(config)# hash-value aaa
Switch(config-hash-value)# port-channel unicast select user
Switch(config-hash-value)# exit
```

Шаг 4. Установите хеш-значение для интерфейса.

```
Switch(config)# interface range eth-0-1 - 2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# static-channel-group 1S
witch(config-if-range)# exit
Switch(config)# interface agg 1
Switch(config-if)# load-balance hash-value aaa input
Switch(config-if)# exit
Switch(config)# interface eth-0-3
Switch(config-if)# load-balance hash-value aaa input
Switch(config-if)# end
```

Шаг 5. Проверка.

Для отображения информации о поле хеша пользователя используйте следующую команду:

```
Switch# show hash-field user
hash-field name: user
 Option                              Control type
------------------------------------------------------------------------
 ipv6 address compress               xor
 hash seed                           user set (0)
 hash arithmetic                     xor
 hash symmetry                       disable
 ip                                  enable
 ipv6                                enable
 mpls                                enable
------------------------------------------------------------------------
 hash field select
```

```
 Packet                  HashField
-------------------------------------------------------------------
 l2:                     macsa

 ip:                     ipsa

 ipv6:                   ipsa                    ipda
                         l4-sourceport           l4-destport
                         ip-protocol

 gre:                    ipsa                    ipda
                         gre-key

 vxlan:                  vni                     outer-l4-sourceport
                         outer-ipda              outer-ipsa

 nvgre:                  vsid                    outer-ipda
                         outer-ipsa

 mpls:                   top-label               2nd-label

 vpws:                   top-label               2nd-label

 vpls(inner-l2):         inner-macda             inner-macsa

 vpls(inner-l3):         inner-ipda              inner-ipsa

 l3vpn:                  inner-ipsa              inner-ipda
                         inner-ip-protocol       inner-l4-sourceport
                         inner-l4-destport
```

Для отображения информации о хеш-значении используйте следующую команду:

```
Switch# show hash-value aaa
LBT:load balance type          LBM:load balance mode
PT :packet type                HF :hash field
HA :hash arithmetic
hash-value name: aaa
 LBT             LBM             PT              HF              HA
-------------------------------------------------------------------
 port-channel    unicast         all             user            xor
 port-channel    non-unicast     all             NOCFG           NOCFG
 ecmp            -               all             NOCFG           NOCFG
 ecmp            flow id         all             NOCFG           NOCFG
```

Для отображения хеш-значения, применяемого на данном порту, используйте следующую команду:

```
Switch# show hash-value interface-applied
eth-0-3
```

```
 hash-value aaa input
agg1
 hash-value aaa input
```

3.17.1.4 Настройка хэша для Linkagg (output)

Следующие шаги показывают, как настроить хэширование Linkagg для одноадресной (unicast) рассылки на выходном интерфейсе, приоритет конфигурации будет ниже, чем на входном. Это применимо только к порту Linkagg.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите хэш-поле.

```
Switch(config)# hash-field user
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip ipsa
Switch(config-hash-field)# exit
```

Шаг 3. Установите хеш-значение.

```
Switch(config)# hash-value aaa
Switch(config-hash-value)# port-channel unicast select user
Switch(config-hash-value)# exit
```

Шаг 4. Установите хеш-значение для интерфейса.

```
Switch(config)# interface range eth-0-1 - 2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# static-channel-group 1
Switch(config-if-range)# exit
Switch(config)# interface agg 1
Switch(config-if)# load-balance hash-value aaa output
Switch(config-if)# exit
```

Шаг 5. Проверка.

Для отображения информации о поле хеша пользователя используйте следующую команду:

```
Switch# show hash-field user
hash-field name: user
 Option                              Control type
-------------------------------------------------------------------
 ipv6 address compress               xor
 hash seed                           user set (0)
```

```
 hash arithmetic                    xor
 hash symmetry                      disable
 ip                                 enable
 ipv6                               enable
 mpls                               enable
-------------------------------------------------------------------
 hash field select
 Packet                 HashField
-------------------------------------------------------------------
 l2:                    macsa

 ip:                    ipsa

 ipv6:                  ipsa                  ipda
                        l4-sourceport         l4-destport
                        ip-protocol

 gre:                   ipsa                  ipda
                        gre-key

 vxlan:                 vni                   outer-l4-sourceport
                        outer-ipda            outer-ipsa

 nvgre:                 vsid                  outer-ipda
                        outer-ipsa

 mpls:                  top-label             2nd-label

 vpws:                  top-label             2nd-label

 vpls(inner-l2):        inner-macda           inner-macsa

 vpls(inner-l3):        inner-ipda            inner-ipsa

 l3vpn:                 inner-ipsa            inner-ipda
                        inner-ip-protocol     inner-l4-sourceport
                        inner-l4-destport
```

Для отображения информации о хеш-значении используйте следующую команду:

```
Switch# show hash-value aaa
LBT:load balance type          LBM:load balance mode
PT :packet type                HF :hash field
HA :hash arithmetic
hash-value name: aaa
 LBT             LBM             PT              HF              HA
-------------------------------------------------------------------
 port-channel    unicast         all             user            xor
 port-channel    non-unicast     all             NOCFG           NOCFG
```

```
 ecmp            -               all             NOCFG           NOCFG
 ecmp            flow id         all             NOCFG           NOCFG
```

Для отображения хеш-значения, применяемого на данном порту, используйте следующую команду:

```
Switch# show hash-value interface-applied
agg1
 hash-value aaa output
```

3.17.1.5 Настрйка хэша для Linkagg совместно с ACL

Следующие шаги показывают, как настроить хеш для Linkagg в качестве действия ACL, такая конфигурация должна иметь наивысший приоритет.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите хэш-поле.

```
Switch(config)# hash-field user
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip ipsa
Switch(config-hash-field)# exit
```

Шаг 3. Установите хеш-значение.

```
Switch(config)# hash-value aaa
Switch(config-hash-value)# port-channel unicast select user
Switch(config-hash-value)# exit
```

Шаг 4. Добавьте действие ACL к интерфейсу и установите хэш-значение для интерфейса.

```
Switch(config)# mac access-list mac
Switch(config-mac-acl)# permit src-mac host 0.0.1 dest-mac any
Switch(config-mac-acl)# exit
Switch(config)# class-map cmap1
Switch(config-cmap)# match access-group mac
Switch(config-cmap)# exit
Switch(config)# policy-map pmap1
Switch(config-pmap)# class cmap1
Switch(config-pmap-c)# load-balance hash-value aaa
Switch(config-pmap-c)# port-channel load-balance round-robin disable
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

```
Switch(config)# interface eth-0-3
Switch(config-if)# no shutdown
Switch(config-if)# service-policy input pmap1
Switch(config-if)# end
```

Шаг 5. Проверка.

Для отображения информации о поле хеша пользователя используйте следующую команду:

```
Switch# show hash-field user
hash-field name: user
 Option                              Control type
------------------------------------------------------------------------
 ipv6 address compress               xor
 hash seed                           user set (0)
 hash arithmetic                     xor
 hash symmetry                       disable
 ip                                  enable
 ipv6                                enable
 mpls                                enable
------------------------------------------------------------------------
 hash field select
 Packet                HashField
------------------------------------------------------------------------
 l2:                   macsa

 ip:                   ipsa

 ipv6:                 ipsa                  ipda
                       l4-sourceport         l4-destport
                       ip-protocol

 gre:                  ipsa                  ipda
                       gre-key

 vxlan:                vni                   outer-l4-sourceport
                       outer-ipda            outer-ipsa

 nvgre:                vsid                  outer-ipda
                       outer-ipsa

 mpls:                 top-label             2nd-label

 vpws:                 top-label             2nd-label

 vpls(inner-l2):       inner-macda           inner-macsa

 vpls(inner-l3):       inner-ipda            inner-ipsa
```

```
 l3vpn:                inner-ipsa            inner-ipda
                       inner-ip-protocol     inner-l4-sourceport
                       inner-l4-destport
```

Для отображения информации о хеш-значении используйте следующую команду:

```
Switch# show hash-value aaa
LBT:load balance type          LBM:load balance mode
PT :packet type                HF :hash field
HA :hash arithmetic
hash-value name: aaa
 LBT             LBM             PT              HF              HA
-------------------------------------------------------------------------
 port-channel    unicast         all             user            xor
 port-channel    non-unicast     all             NOCFG           NOCFG
 ecmp            -               all             NOCFG           NOCFG
 ecmp            flow id         all             NOCFG           NOCFG
```

Для отображения информации о списках контроля доступа (ACL) используйте следующую команду:

```
Switch# show running-config
mac access-list mac
  10 permit src-mac host 0000.0000.0001 dest-mac any
!
hash-field user
 l2 macsa
 ip ipsa
!
hash-value aaa
 port-channel unicast select user
!
class-map match-any cmap1
 match access-group mac
!
policy-map pmap1
 class cmap1
  port-channel load-balance round-robin disable
  load-balance hash-value aaa
!
interface eth-0-3
 service-policy input pmap1
!
interface null0
!
```

3.17.1.6 Настройка хэша для остального (не unicast) трафика для Linkagg

Следующие шаги показывают, как установить хеш для не-Unicast входящего трафика Linkagg интерфейса; данная конфигурация не поддерживается на выходе. Когда значение хеша применяется на входе порта Linkagg, оно будет применяться и к порту-участнику этого порта.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите хэш-поле.

```
Switch(config)# hash-field user
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip ipsa
Switch(config-hash-field)# exit
```

Шаг 3. Установите хеш-значение.

```
Switch(config)# hash-value aaa
Switch(config-hash-value)# port-channel non-unicast select user
Switch(config-hash-value)# exit
```

Шаг 4. Установите хеш-значение для интерфейса.

```
Switch(config)# interface range eth-0-1 - 2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# static-channel-group 1
Switch(config-if-range)# exit
Switch(config)# interface agg 1
Switch(config-if)# load-balance hash-value aaa input
Switch(config-if)# exit
Switch(config)# interface eth-0-3
Switch(config-if)# load-balance hash-value aaa input
Switch(config-if)# end
```

Шаг 5. Проверка.

Для отображения информации о поле хеша пользователя используйте следующую команду:

```
Switch# show hash-field user
hash-field name: user
 Option                              Control type
```

```
------------------------------------------------------------------------
 ipv6 address compress              xor
 hash seed                          user set (0)
 hash arithmetic                    xor
 hash symmetry                      disable
 ip                                 enable
 ipv6                               enable
 mpls                               enable
------------------------------------------------------------------------
 hash field select
 Packet                 HashField
------------------------------------------------------------------------
 l2:                    macsa

 ip:                    ipsa

 ipv6:                  ipsa                    ipda
                        l4-sourceport           l4-destport
                        ip-protocol

 gre:                   ipsa                    ipda
                        gre-key

 vxlan:                 vni                     outer-l4-sourceport
                        outer-ipda              outer-ipsa

 nvgre:                 vsid                    outer-ipda
                        outer-ipsa

 mpls:                  top-label               2nd-label

 vpws:                  top-label               2nd-label

 vpls(inner-l2):        inner-macda             inner-macsa

 vpls(inner-l3):        inner-ipda              inner-ipsa

 l3vpn:                 inner-ipsa              inner-ipda
                        inner-ip-protocol       inner-l4-sourceport
                        inner-l4-destport
```

Для отображения информации о хеш-значении используйте следующую команду:

```
Switch# show hash-value aaa
LBT:load balance type          LBM:load balance mode
PT :packet type                HF :hash field
HA :hash arithmetic
hash-value name: aaa
 LBT            LBM             PT              HF              HA
```

```
-------------------------------------------------------------------------
 port-channel   unicast        all            NOCFG          NOCFG
 port-channel   non-unicast    all            user           xor
 ecmp           -              all            NOCFG          NOCFG
 ecmp           flow id        all            NOCFG          NOCFG
```

Для отображения хеш-значения, применяемого на данном порту, используйте следующую команду:

```
Switch# show hash-value interface-applied
eth-0-3
 hash-value aaa input
agg1
 hash-value aaa input
```

3.17.2 Настройка хэш для ECMP маршрутизации

3.17.2.1 Общие положения

Маршрутизация с равной стоимостью (ECMP) — это стратегия маршрутизации, при которой пересылка пакетов на следующий узел в одно место назначения может осуществляться по нескольким «оптимальным путям», которые занимают первое место в расчетах метрик маршрутизации. Многопутевая маршрутизация может использоваться в сочетании с большинством протоколов маршрутизации. ECMP может существенно увеличить пропускную способность за счет балансировки нагрузки трафика по нескольким путям. Для балансировки нагрузки используется ECMP-хеш.

3.17.2.2 Настройка хэша ECMP глобально

Следующие шаги показывают, как установить хэш ECMP глобально.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите хэш-поле.

```
Switch(config)# hash-field user
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip ipsa
Switch(config-hash-field)# exit
```

Шаг 3. Установите хеш-значение как глобальное.

```
Switch(config)# hash-value global
Switch(config-hash-value-global)# ecmp select user
Switch(config-hash-value-global)# end
```

Шаг 4. Проверка.

Для отображения информации о поле хеша используйте следующую команду:

```
Switch# show hash-field user
hash-field name: user
 Option                                Control type
------------------------------------------------------------------------
 ipv6 address compress                 xor
 hash seed                             user set (0)
 hash arithmetic                       xor
 hash symmetry                         disable
 ip                                    enable
 ipv6                                  enable
 mpls                                  enable
------------------------------------------------------------------------
 hash field select
 Packet                 HashField
------------------------------------------------------------------------
 l2:                    macsa

 ip:                    ipsa

 ipv6:                  ipsa                    ipda
                        l4-sourceport           l4-destport
                        ip-protocol

 gre:                   ipsa                    ipda
                        gre-key

 vxlan:                 vni                     outer-l4-sourceport
                        outer-ipda              outer-ipsa

 nvgre:                 vsid                    outer-ipda
                        outer-ipsa

 mpls:                  top-label               2nd-label

 vpws:                  top-label               2nd-label

 vpls(inner-l2):        inner-macda             inner-macsa

 vpls(inner-l3):        inner-ipda              inner-ipsa

 l3vpn:                 inner-ipsa              inner-ipda
                        inner-ip-protocol       inner-l4-sourceport
                        inner-l4-destport
```

Для отображения информации о глобальном хеш-значении используйте следующую команду:

```
Switch# show hash-value global
LBT:load balance type          LBM :load balance mode
PT :packet type                HF  :hash field
HA :hash arithmetic
hash-value global
 LBT             LBM             PT              HF              HA
-------------------------------------------------------------------------
 port-channel    -               all             port-channel    xor
 ecmp            -               all             user            xor
 ecmp            flow id         all             user            xor
 entropy         -               all             ecmp            xor
-------------------------------------------------------------------------
 Efd hash field select:
  macsa                  macda
  ipsa                   ipda
  sourceport             destport
  ip-protocol
```

3.17.2.3 Настройка хэш для ECMP для входящего трафика

Следующие шаги показывают, как установить хеш ECMP на входном интерфейсе, с приоритетом выше, чем у глобальной конфигурации.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите хэш-поле.

```
Switch(config)# hash-field user
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip ipsa
Switch(config-hash-field)# exit
```

Шаг 3. Установите хеш-значение.

```
Switch(config)# hash-value bbb
Switch(config-hash-value)# ecmp select user
Switch(config-hash-value)# exit
```

Шаг 4. Установите хеш-значение для интерфейса.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
```

```
Switch(config-if)# load-balance hash-value bbb input
Switch(config-if)# end
```

Шаг 5. Проверка.

Для отображения информации о поле хеша пользователя используйте следующую команду:

```
    Switch# show hash-field user
hash-field name: user
 Option                              Control type
-------------------------------------------------------------------------
 ipv6 address compress               xor
 hash seed                           user set (0)
 hash arithmetic                     xor
 hash symmetry                       disable
 ip                                  enable
 ipv6                                enable
 mpls                                enable
-------------------------------------------------------------------------
 hash field select
 Packet                HashField
-------------------------------------------------------------------------
 l2:                   macsa

 ip:                   ipsa

 ipv6:                 ipsa                  ipda
                       l4-sourceport         l4-destport
                       ip-protocol

 gre:                  ipsa                  ipda
                       gre-key

 vxlan:                vni                   outer-l4-sourceport
                       outer-ipda            outer-ipsa

 nvgre:                vsid                  outer-ipda
                       outer-ipsa

 mpls:                 top-label             2nd-label

 vpws:                 top-label             2nd-label

 vpls(inner-l2):       inner-macda           inner-macsa

 vpls(inner-l3):       inner-ipda            inner-ipsa

 l3vpn:                inner-ipsa            inner-ipda
```

```
                        inner-ip-protocol     inner-l4-sourceport
                        inner-l4-destport
```

Для отображения информации о хеш-значении используйте следующую команду:

```
Switch# show hash-value bbb
LBT:load balance type          LBM:load balance mode
PT :packet type                HF :hash field
HA :hash arithmetic
hash-value name: bbb
 LBT             LBM             PT              HF              HA
-------------------------------------------------------------------------
 port-channel    unicast         all             NOCFG           NOCFG
 port-channel    non-unicast     all             NOCFG           NOCFG
 ecmp            -               all             user            xor
 ecmp            flow id         all             NOCFG           NOCFG
```

Для отображения хеш-значения, применяемого на данном порту, используйте следующую команду:

```
Switch# show hash-value interface-applied
eth-0-1
 hash-value bbb input
```

3.17.2.4 Настройка хэша ECMP для входящего трафика в сочетании с ACL

Следующие шаги показывают, как настроить хэширование для ECMP совместно с действием ACL.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите хэш-поле.

```
Switch(config)# hash-field user
Switch(config-hash-field)# l2 macsa
Switch(config-hash-field)# ip ipsa
Switch(config-hash-field)# exit
```

Шаг 3. Установите хеш-значение.

```
Switch(config)# hash-value bbb
Switch(config-hash-value)# ecmp select use
rSwitch(config-hash-value)# exit
```

Шаг 4. Добавьте действие ACL к интерфейсу и установите хэш-значение для интерфейса.

```
Switch(config)# mac access-list mac
Switch(config-mac-acl)# permit src-mac host 0.0.1 dest-mac any
Switch(config-mac-acl)# exit
Switch(config)# class-map cmap1
Switch(config-cmap)# match access-group mac
Switch(config-cmap)# exit
Switch(config)# policy-map pmap1
Switch(config-pmap)# class cmap1
Switch(config-pmap-c)# load-balance hash-value bbb
Switch(config-pmap-c)# ecmp load-balance round-robin disable
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# service-policy input pmap1
Switch(config-if)# end
```

Шаг 5. Проверка.

Для отображения информации о поле хеша используйте следующую команду:

```
Switch# show hash-field user
hash-field name: user
 Option                                Control type
------------------------------------------------------------------------
 ipv6 address compress                 xor
 hash seed                             user set (0)
 hash arithmetic                       xor
 hash symmetry                         disable
 ip                                    enable
 ipv6                                  enable
 mpls                                  enable
------------------------------------------------------------------------
 hash field select
 Packet                HashField
------------------------------------------------------------------------
 l2:                   macsa

 ip:                   ipsa

 ipv6:                 ipsa                  ipda
                       l4-sourceport         l4-destport
                       ip-protocol

 gre:                  ipsa                  ipda
```

```
                        gre-key

 vxlan:                 vni                    outer-l4-sourceport
                        outer-ipda             outer-ipsa

 nvgre:                 vsid                   outer-ipda
                        outer-ipsa

 mpls:                  top-label              2nd-label

 vpws:                  top-label              2nd-label

 vpls(inner-l2):        inner-macda            inner-macsa

 vpls(inner-l3):        inner-ipda             inner-ipsa

 l3vpn:                 inner-ipsa             inner-ipda
                        inner-ip-protocol      inner-l4-sourceport
                        inner-l4-destport
```

Для отображения информации о хеш-значении используйте следующую команду:

```
Switch# show hash-value bbb
LBT:load balance type          LBM:load balance mode
PT :packet type                HF :hash field
HA :hash arithmetic
hash-value name: bbb
 LBT             LBM             PT              HF              HA
------------------------------------------------------------------------
 port-channel    unicast         all             NOCFG           NOCFG
 port-channel    non-unicast     all             NOCFG           NOCFG
 ecmp            -               all             user            xor
 ecmp            flow id         all             NOCFG           NOCFG
```

Для отображения информации о списках контроля доступа (ACL) используйте следующую команду:

```
mac access-list mac
  10 permit src-mac host 0000.0000.0001 dest-mac any
!
hash-field user
 l2 macsa
 ip ipsa
!
hash-value bbb
 ecmp select user
!
class-map match-any cmap1
 match access-group mac
!
```

```
policy-map pmap1
 class cmap1
  ecmp load-balance round-robin disable
  load-balance hash-value bbb
!
interface eth-0-1
 service-policy input pmap1
!
interface null0
!
```

3.17.3 Настройка EFD хэширования

3.17.3.1 Общие положения

Согласно исследованиям, проведенным в реальных сетях академическими учреждениями, более 80% полосы пропускания занято «Elephant Flow». Elephant Flow - непрерывные сетевые потоки, занимающие большую часть пропускной способности канала и замедляющие работу сети. Механизм EFD (Elephant Flow Detection) - предназначен для обнаружения Elephant Flow путем распознавания свойств пакетов.

3.17.3.2 Настройка хэша EFD глобально

Следующие шаги показывают, как выбрать характеристики пакета для хэширования EFD в глобально.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установить глобальный хеш.

```
Switch(config)# hash-value global
Switch(config-hash-value-global)# efd select ipsa macsa
Switch(config-hash-value-global)# end
```

Шаг 3. Проверка.

Для отображения информации о глобальном хеш-значении используйте следующую команду:

```
Switch# show hash-value global
LBT:load balance type          LBM :load balance mode
PT :packet type                HF  :hash field
HA :hash arithmetic
hash-value global
 LBT            LBM             PT              HF              HA
```

```
-------------------------------------------------------------------
 port-channel    -               all             port-channel    xor
 ecmp            -               all             ecmp            xor
 ecmp            flow id         all             ecmp            xor
 entropy         -               all             ecmp            xor
-------------------------------------------------------------------
 Efd hash field select:
  macsa                  ipsa
```

3.18 Настройка функции PORT-XCONNECT

3.18.1 Общие положения

3.18.1.1 Описание функции

Эта функция позволяет пересылать пакеты напрямую в соответствии с настроенным интерфейсом назначения без анализа каких-либо таблиц.

В настоящее время поддерживаются только физические и агрегированные порты.

3.18.2 Конфигурация

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Перейдите в режим интерфейса и отключите выключение.

```
Switch(config)# interface range eth-0-1, eth-0-2
Switch(config-if-range)# no shutdown
```

Шаг 3. Установите целевой интерфейс eth-0-1 port-xconnect.

```
Switch(config)# interface eth-0-1
Switch(config-if)# port-xconnect destination-interface eth-0-2
Switch(config-if)# end
```

Шаг 4. Отобразите текущий конфиг.

```
Switch# show running-config
Building configuration...
version 5.3.9.18
!
no service password-encryption
!
!
!
```

```
!
!
!
!
temperature 0 0 0
!
vlan database
!

interface eth-0-1
port-xconnect destination-interface eth-0-2
!
interface eth-0-2
!
interface eth-0-3
Switch#
```

4 Руководство по настройке IP-сервисов

4.1 Настройка Arp

4.1.1 Общие положения

4.1.1.1 Описание функции

Протокол разрешения адресов (ARP) — это протокол, используемый для динамического сопоставления адресов хостов в Интернете (IP) и адресов Ethernet (MAC). ARP кэширует записи сопоставления адресов Интернет-Ethernet. Когда интерфейс запрашивает сопоставление для адреса, отсутствующего в кэше, ARP рассылает широковещательное сообщение в соответствующей сети с запросом на поиск адреса. Если получен ответ, новая запись кэшируется. ARP ставит в очередь не более одного пакета, ожидая ответа на запрос сопоставления; сохраняется только последний отправленный пакет. Если целевой хост не отвечает после 3 запросов, хост считается недоступным. Если целевой хост не отправляет сообщения в течение определенного периода (обычно один час), хост считается ненадежным. Перед удалением записи ARP хосту будет отправлено несколько запросов (3 одноадресных и 3 широковещательных). Записи ARP могут быть добавлены, удалены или изменены вручную. Добавленные вручную записи могут быть временными или постоянными.

4.1.2 Настройка

В этом примере интерфейсу eth-0-1 назначен адрес 11.11.11.1/24, в подсети 11.11.11.0/24 находятся два хоста с IP-адресами 11.11.11.2 и 11.11.11.3, и MAC-адресами 001a-a011-eca2 и 001a-a011-eca3. Запись ARP для хоста 11.11.11.2 добавлена вручную, а запись для хоста 11.11.11.3 — динамически. Время ожидания записей ARP для интерфейса eth-0-1 установлено на 20 минут, задержка повторной отправки запроса ARP для интерфейса eth-0-1 — 2 секунды.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройте интерфейс уровня 3 и задайте IP-адрес.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 11.11.11.1/24
```

Шаг 3. Настройте значение таймаута устаревания ARP и значение интервала повторных попыток ARP.

```
Switch(config-if)# arp timeout 1200
Switch(config-if)# arp retry-interval 2
Switch(config-if)# exit
```

Шаг 4. Добавьте статическую запись ARP.

```
Switch(config)# arp 11.11.11.2 1a.a011.eca2
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Для отображения информации о записи ARP используйте следующую команду:

```
Switch# show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    11.11.11.2             -   001a.a011.eca2     eth-0-1

Switch# show ip arp summary
 1 IP ARP entries, with 0 of them incomplete
(Static:0,  Dyamic:0, Interface:1)
 ARP Pkt Received is: 0
 ARP Pkt Send number is: 0
 ARP Pkt Dicard number is: 0
```

Для отображения информации о конфигурациях ARP на интерфейсе используйте следующую команду:

```
Switch# show interface eth-0-1
Interface eth-0-1
  Interface current state: Administratively DOWN
  Hardware is Ethernet, address is 6c02.530c.2300 (bia 6c02.530c.2300)
  Bandwidth 1000000 kbits
  Index 1 , Metric 1 , Encapsulation ARPA
  Speed - Auto , Duplex - Auto  , Media type is 1000BASE_T
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  VRRP master of :  VRRP is not configured on this interface
  ARP timeout 00:20:00,  ARP retry interval 2s
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    0 packets output, 0 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output
```

4.2 Настройка Arp proxy

4.2.1 Общие положения

4.2.1.1 Описание функции

ARP Proxy это наиболее распространенный метод получения информации о других маршрутах недоступных подсетей. ARP Proxy - метод использования ARP-протокола, позволяющий объединить две не связанные на канальном уровне сети в одну. ARP Proxy позволяет Ethernet-узлу без информации о маршрутизации взаимодействовать с узлами в других сетях или подсетях при помощи прокси-сервера ARP. Если коммутатор получает ARP-запрос для хоста, который находится не в той же сети, что и отправитель, коммутатор оценивает, имеет ли он наилучший маршрут к этому хосту. Если имеет, он отправляет ответный ARP-пакет со своим собственным MAC-адресом Ethernet, и хост, отправивший запрос, отправляет пакет коммутатору, который пересылает его нужному хосту. Пересылка пакетов ICMP (Internet Control Message Protocol) отключена на интерфейсах, где включена функция локального прокси ARP.

4.2.2 Настройка ARP Proxy

Как видно из приведенной выше топологии, PC1 принадлежит VLAN10, а PC2 — VLAN20. Если функция ARP-прокси не включена, PC1 и PC2 не смогут взаимодействовать друг с другом. Ниже показаны шаги для включения функции ARP-прокси для интерфейса VLAN 10 и интерфейса VLAN 20.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10,20
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса, установите режим порта и привяжите его к VLAN.

```
Switch(config)# interface eth-0-22
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-23
Switch(config-if)# switchport access vlan 20
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 4. Создайте интерфейс VLAN, настройте IP-адрес и включите ARP-прокси.

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1/24
Switch(config-if)# proxy-arp enable
Switch(config-if)# exit

Switch(config)# interface vlan 20
Switch(config-if)# ip address 192.168.20.1/24
Switch(config-if)# proxy-arp enable
Switch(config-if)# exit
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Для отображения информации о конфигурации ARP-прокси на коммутаторе используйте следующую команду:

```
Switch# show ip interface vlan 10
Interface vlan10
  Interface current state: UP
  Internet address(es):
    192.168.10.1/24 broadcast 192.168.10.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 01:00:00,  ARP retry interval 1s
```

```
  ARP Proxy is enabled, Local ARP Proxy is disabled
  VRRP master of :  VRRP is not configured on this interface

Switch# show ip interface vlan 20
Interface vlan20
  Interface current state: UP
  Internet address(es):
    192.168.20.1/24 broadcast 192.168.20.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 01:00:00,  ARP retry interval 1s
  ARP Proxy is enabled, Local ARP Proxy is disabled
  VRRP master of :  VRRP is not configured on this interface
```

Для отображения информации об ARP-записи на коммутаторе используйте следующую команду:

```
Switch# show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    192.168.10.1           -   7cc3.11f1.aa00  vlan10
 Internet    192.168.10.111         5   0cf9.11b6.6e2e  vlan10
 Internet    192.168.20.1           -   7cc3.11f1.aa00  vlan20
 Internet    192.168.20.222         6   5a94.031f.2357  vlan20
```

Для отображения информации на ПК1 используйте следующую команду:

```
[Host:~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 0C:F9:11:B6:6E:2E
          inet addr:192.168.10.111  Bcast:192.168.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1600  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:588 (588.0 b)  TX bytes:700 (700.0 b)
          Interrupt:5

[Host:~]$ arp -a
? (192.168.20.222) at 7c:c3:11:f1:aa:00 [ether] on eth0
[Host: ~]$ route -v
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     *               255.255.0.0     U     0      0        0 eth0

[Host:~]$ ping 192.168.20.222
PING 192.168.20.222 (192.168.20.222) 56(84) bytes of data.
```

```
64 bytes from 192.168.20.222: icmp_seq=0 ttl=63 time=189 ms
64 bytes from 192.168.20.222: icmp_seq=1 ttl=63 time=65.2 ms
--- 192.168.20.222 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 65.209/127.226/189.244/62.018 ms, pipe 2
```

Для отображения информации на ПК2 используйте следующую команду:

```
[Host:~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 5A:94:03:1F:23:57
          inet addr:192.168.20.222  Bcast:192.168.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1600  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:784 (784.0 b)  TX bytes:1174 (1.1 KiB)
          Interrupt:5

[Host:~]$ arp -a
? (192.168.10.111) at 7c:c3:11:f1:aa:00 [ether] on eth0

[Host: ~]$ route -v
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     *               255.255.0.0     U     0      0        0 eth0

[Host: ~]$ ping 192.168.10.111
PING 192.168.10.111 (192.168.10.111) 56(84) bytes of data.
64 bytes from 192.168.10.111: icmp_seq=0 ttl=63 time=53.8 ms
64 bytes from 192.168.10.111: icmp_seq=1 ttl=63 time=65.8 ms
--- 192.168.10.111 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 53.832/59.842/65.852/6.010 ms, pipe 2
```

4.2.2.1 Настройка локального ARP-Proxy

В соответствии с описанной выше топологией, порты eth-0-2, eth-0-3 и eth-0-4 принадлежат VLAN 10. Оба порта eth-0-3 и eth-0-4 находятся в группе изоляции портов 1, а eth-0-2 — в группе изоляции портов 3, поэтому пакеты, полученные через eth-0-3, не могут быть отправлены на eth-0-4, но пакеты, полученные через eth-0-2, могут быть отправлены на оба порта eth-0-3 и eth-0-4. PC1 подключен к порту eth-0-3, а PC2 — к порту eth-0-4. Для обеспечения связи между PC1 и PC2 выполните следующие действия. Конфигурации коммутаторов A и B одинаковы.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса, установите режим порта коммутатора и назначьте VLAN.

Конфигурация коммутатора A:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Конфигурация коммутатора B:

```
Switch(config)# interface range eth-0-2 - 4
Switch(config-if-range# switchport access vlan 10
Switch(config-if-range# no shutdown
Switch(config-if-range# exit
```

Шаг 4. Создайте интерфейс VLAN, настройте IP-адрес и включите локальный ARP-прокси.

Конфигурация коммутатора A:

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1/24
Switch(config-if)# local-proxy-arp enable
Switch(config-if)# exit
```

Шаг 5. Настройка изоляции портов (необязательно).

Конфигурация коммутатора B:

После настройки изоляции портов, как показано ниже, порты eth-0-3 и eth-0-4 на коммутаторе B изолированы на уровне 2.

```
Switch(config)# port-isolate mode l2
Switch(config)# interface eth-0-3 – 4
Switch(config-if-range# port-isolate group 1
Switch(config-if-range# exit

Switch(config)# interface eth-0-2
Switch(config-if)# port-isolate group 3
Switch(config-if)# exit
```

Шаг 6. Проверка.

Для отображения информации о записи ARP на коммутаторе A используйте следующую команду:

```
Switch# show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    192.168.10.1           -   eeb4.2a8d.6c00  vlan10
 Internet    192.168.10.111         0   34b0.b279.5f67  vlan10
 Internet    192.168.10.222         0   2a65.9618.57fa  vlan10
```

Для отображения информации о конфигурациях ARP на интерфейсе коммутатора A используйте следующую команду:

```
Switch# show ip interface vlan 10
Interface vlan10
  Interface current state: UP
  Internet address(es):
    192.168.10.1/24 broadcast 192.168.10.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 01:00:00,  ARP retry interval 1s
  ARP Proxy is disabled, Local ARP Proxy is enabled
  VRRP master of :  VRRP is not configured on this interface
```

Для отображения информации на ПК1 используйте следующую команду:

```
[Host: ~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 34:B0:B2:79:5F:67
          inet addr:192.168.10.111  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1600  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1344 (1.3 KiB)  TX bytes:2240 (2.1 KiB)
          Interrupt:5

[Host: ~]$ arp -a
? (192.168.10.222) at ee:b4:2a:8d:6c:00 [ether] on eth0

[Host: ~]$ ping 192.168.10.222
PING 192.168.10.222 (192.168.10.222) 56(84) bytes of data.
64 bytes from 192.168.10.222: icmp_seq=0 ttl=63 time=131 ms
64 bytes from 192.168.10.222: icmp_seq=1 ttl=63 time=159 ms
--- 192.168.10.222 ping statistics ---
```

```
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 131.078/145.266/159.454/14.188 ms, pipe 2
```

Для отображения информации на ПК2 используйте следующую команду:

```
[Host:~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 2A:65:96:18:57:FA
          inet addr:192.168.10.222  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1600  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1148 (1.1 KiB)  TX bytes:1524 (1.4 KiB)
          Interrupt:5

[Host:~]$ arp -a
? (192.168.10.111) at ee:b4:2a:8d:6c:00 [ether] on eth0

[Host: ~]$ ping 192.168.10.111
PING 192.168.10.111 (192.168.10.111) 56(84) bytes of data.
64 bytes from 192.168.10.111: icmp_seq=0 ttl=63 time=198 ms
64 bytes from 192.168.10.111: icmp_seq=1 ttl=63 time=140 ms
64 bytes from 192.168.10.111: icmp_seq=2 ttl=63 time=146 ms
--- 192.168.10.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 140.196/161.959/198.912/26.267 ms, pipe 2
```

4.3 Настройка редистрибуции ARP записей (ARP host-route)

4.3.1 Общие положения

Описание функции

Функция ARP host-route преобразует записи ARP на устройстве и перераспределяет их в протоколы маршрутизации. Эта функция включается в разделе «Интерфейсы» и перераспределяет все доступные записи ARP. В протоколах маршрутизации маршруты, сгенерированные этой функцией, будут рассматриваться как подключенные маршруты.

4.3.2 Настройка ARP host-route

4.3.2.1 Топология

В этом примере конфигурации хосты host1 и host2 подключены к коммутаторам switch1 и switch2 по отдельности через интерфейс eth-0-1. Коммутаторы switch1 и switch2 установили соединение ebgp. После включения функции arp host-route на интерфейсах, подключенных к хосту, коммутатор может преобразовывать записи ARP в маршруты хоста и перераспределять их по

протоколам маршрутизации. С помощью route-map коммутатор может объявлять только маршруты хоста, без сетевых маршрутов.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройте интерфейс уровня 3 и задайте IP-адрес.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.254/24
```

Шаг 3. Включите функцию «arp host-route» в интерфейсе.

```
Switch(config-if)# arp host-route enable
Switch(config-if)# exit
```

Шаг 4. Добавьте статическую запись ARP.

```
Switch(config)# arp 10.1.1.2 1.1.1
```

Шаг 5. Включите перераспределение подключенных маршрутов BGP.

```
Switch(config)# router bgp 100
Switch(config-router)# redistribute connected
```

Шаг 6. Выход из режима настройки.

```
Switch(config-router)# end
```

Шаг 7. Проверка.

Для отображения информации о маршруте в BGP используйте следующую команду

```
Switch# show ip bgp
BGP table version is 1, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                              32768 ?
```

```
*> 10.1.1.2/32      0.0.0.0                                32768 ?

Total number of prefixes 2
```

4.4 Настройка DHCP клиента

4.4.1 Общие положения

4.4.1.1 Описание функции

Клиент, использующий протокол DHCP (Dynamic Host Configuration Protocol), может динамически получать IP-адрес и конфигурацию от DHCP-сервера. Если клиент и сервер находятся в одной физической подсети, клиент может взаимодействовать с сервером напрямую; в противном случае им требуется агент ретрансляции DHCP, используемый для пересылки сообщений DHCP. DHCP-клиент может запрашивать IP-адрес у DHCP-сервера, рассылая широковещательные сообщения DHCP. Клиент получает IP-адрес и срок его аренды. По истечении половины срока клиент отправляет сообщения DHCP для получения нового срока аренды, чтобы продолжать использовать IP-адрес. В случае успеха DHCP-клиент продлевает аренду. DHCP-клиент может отправлять серверу запрос на параметры, которые могут представлять собой один или несколько из следующих параметров: router, static-route, classless-static-route, classless-static-route-ms, tftp-server-address, dns-nameserver, domain-name, netbios-nameserver. По умолчанию с сервера будут запрашиваться следующие параметры: router, static-route, classless-static-route, classless-static-route-ms, tftp-server-address.

4.4.2 Конфигурация

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
```

Шаг 3. Отключите статическую маршрутизацию и включите DHCP-клиент.

```
Switch(config-if)# no dhcp client request static-route
Switch(config-if)# ip address dhcp
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 5. Проверка.

Проверьте конфигурацию интерфейса:

```
Switch# show running-config interface eth-0-1
Building configuration...
!
interface eth-0-1
 no switchport
 ip address dhcp
 no dhcp client request static-route
!
```

Проверьте состояние всех DHCP-клиентов:

```
Switch# show dhcp client verbose
DHCP client informations:
=========================================================
eth-0-1 DHCP client information:
  Current state: BOUND
  Allocated IP: 4.4.4.199 255.255.255.0
  Lease/renewal/rebinding: 1187/517/1037 seconds
  Lease from 2011-11-18 05:59:59 to 2011-11-18 06:19:59
  Will Renewal in 0 days 0 hours 8 minutes 37 seconds
  DHCP server: 4.4.4.1
  Transaction ID: 0x68857f54
  Client ID: switch-7e39.3457.b700-eth-0-1
```

Показать статистику DHCP-клиента:

```
Switch# show dhcp client statistics
DHCP client packet statistics:
=========================================================
DHCP OFFERS     received: 1
DHCP ACKs       received: 2
DHCP NAKs       received: 0
DHCP Others     received: 0
DHCP DISCOVER       sent: 1
DHCP DECLINE        sent: 0
DHCP RELEASE        sent: 0
DHCP REQUEST        sent: 2
DHCP packet send failed: 0
```

4.5 Настройка DHCP-ретранслятора

4.5.1 Общие положения

4.5.1.1 Описание функции

Ретранслятор DHCP — это любой хост, который пересылает пакеты DHCP между клиентами и серверами. Агенты ретрансляции используются для пересылки запросов и ответов между клиентами и серверами, когда они находятся в разных физических подсетях. Пересылка пакетов агентами ретрансляции отличается от обычной пересылки IP-маршрутизатором, где IP-дейтаграммы переключаются между сетями относительно прозрачно. В отличие от этого, агенты ретрансляции получают сообщения DHCP, а затем генерируют новое сообщение DHCP для отправки через другой интерфейс. Агент ретрансляции устанавливает адрес шлюза (поле girder пакета DHCP) и, если настроено, добавляет в пакет опцию информации агента ретрансляции (option82) и пересылает его на DHCP-сервер. Ответ от сервера пересылается обратно клиенту после удаления опции 82.

4.5.2 Настройка

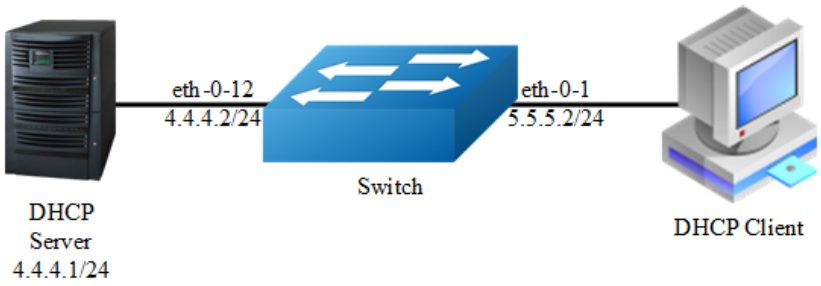


Рисунок 28 – DHCP-ретранслятор

На этом рисунке представлена сетевая топология для тестирования функций ретрансляции DHCP. Для создания тестового стенда нам понадобятся два компьютера под управлением Linux и один коммутатор.

Компьютер A используется в качестве DHCP-сервера.

Компьютер B используется в качестве DHCP-клиента.

Коммутатор используется в качестве агента ретрансляции DHCP.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес.

```
Switch(config)# interface eth-0-12
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip address 4.4.4.2/24
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 5.5.5.2/24
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 3. Создайте DHCP-сервер.

```
Switch(config)# dhcp-server 1 4.4.4.1
```

Шаг 4. Включите DHCP-сервер и опцию 82 для интерфейса.

```
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp relay information trusted
Switch(config-if)# dhcp-server 1
Switch(config-if)# exit
```

Шаг 5. Включите DHCP-сервер и DHCP-ретранслятор глобально.

```
Switch(config)# service dhcp enable
Switch(config)# dhcp relay
```

Шаг 6. Проверка.

Проверьте конфигурацию интерфейса

```
Switch# show running-config interface eth-0-12
!
interface eth-0-12
 no switchport
 ip address 4.4.4.2/24
!
Switch# show running-config interface eth-0-1
!
interface eth-0-1
 no switchport
 dhcp relay information trusted
 dhcp-server 1
 ip address 5.5.5.2/24
!
```

Проверьте состояние службы DHCP

```
Switch# show services
Networking services configuration:
Service Name          Status
============================================================
dhcp                    enable
```

Проверьте конфигурацию группы DHCP-серверов

```
Switch# show dhcp-server
DHCP server group information:
============================================================
group 1 ip address list:
[1] 4.4.4.1
```

Проверьте статистику ретрансляции DHCP

```
Switch# show dhcp relay statistics
DHCP relay packet statistics:
============================================================
Client relayed packets:  20
Server relayed packets:  20
Client error packets:     20
Server error packets:     0
Bogus GIADDR drops:       0
Bad circuit ID packets:   0
Corrupted agent options:  0
Missing agent options:    0
Missing circuit IDs:      0
```

Проверьте IP-адрес вашего компьютера на DHCP-сервере

```
Ipconfig /all
Dhcp Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : 5.5.5.1
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 5.5.5.2
DHCP Server . . . . . . . . . . . : 4.4.4.1
DNS Servers . . . . . . . . . . . : 4.4.4.1
```

4.6 Настройка DHCP-сервера

4.6.1 Общие положения

4.6.1.1 Описание функции

DHCP-сервер возвращает параметры конфигурации DHCP-клиентам. DHCP-сервер может предоставлять IP-адрес и сетевую конфигурацию. DHCP-сервер должен быть предварительно настроен. Например, необходимо создать пул IP-адресов, установить шлюз по умолчанию в пуле и задать некоторые сетевые параметры. После запуска DHCP-сервер будет находить

действительный IP-адрес в пуле для DHCP-клиента. IP-адрес, назначенный DHCP-сервером, имеет срок действия (аренду), поэтому DHCP-клиенту необходимо продлить свою аренду до истечения срока ее действия, чтобы зарезервировать текущий IP-адрес, отправив сообщение DHCP REQUEST.

Если DHCP-сервер находится в той же подсети, что и клиент, он будет нормально работать после подключения к подсети. В противном случае, для пересылки DHCP-сообщений между сервером и клиентом потребуется DHCP-ретранслятор.

Основные параметры, поддерживаемые DHCP-сервером, включают bootfile-name, dns-server, domain-name, адрес шлюза, netbios-name-server, netbios-node-type, tftp-server-address.

4.6.2 Настройка

4.6.2.1 Настройка DHCP-сервера

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите DHCP-сервер глобально и настройте пул IP-адресов.

Настройка на DUT1:

```
Switch(config)#service dhcp enable
Switch(config)#dhcp server
Switch(config)#dhcp pool pool5
Switch(dhcp-config)#network 5.5.5.0/24
Switch(dhcp-config)#gateway 5.5.5.1
Switch(dhcp-config)#exit
```

Шаг 3. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес.

Настройка на DUT1:

```
Switch(config)#interface eth-0-9
Switch (config-if)#no switchport
Switch (config-if)# no shutdown
Switch (config-if)# ip address 5.5.5.1/24
Switch (config-if)# dhcp server enable
Switch (config-if)#exit
```

Настройка на DUT2:

```
Switch#configure terminal
Switch(config)#interface eth-0-9
Switch (config-if)#no switchport
Switch (config-if)# no shutdown
Switch (config-if)# ip address dhcp
```

```
Switch (config-if)#exit
```

Шаг 4. Проверка.

Проверьте конфигурацию DHCP-сервера (dut1):

```
Switch# show running-config
!
service dhcp enable
!
interface eth-0-9
 no switchport
 dhcp server enable
 ip address 5.5.5.1/24!
!
dhcp server
dhcp pool pool5
 network 5.5.5.0/24
 gateway 5.5.5.1
```

Проверка. состояния DHCP-клиента (dut2):

```
Switch# show dhcp client verbose
DHCP client informations:
=========================================================
eth-0-9 DHCP client information:
  Current state: BOUND
  Allocated IP: 5.5.5.2 255.255.255.0
  Lease/renewal/rebinding: 1194/546/1044 seconds
  Lease from 2012-02-04 07:40:12 to 2012-02-04 08:00:12
  Will Renewal in 0 days 0 hours 9 minutes 6 seconds
  DHCP server: 5.5.5.1
  Transaction ID: 0x45b0b27b
  Default router: 5.5.5.1
  Classless static route:
    Destination: 5.5.4.0, mask: 255.255.255.0, Nexthop: 5.5.5.1
  TFTP server addresses: 5.5.5.3
Client ID: switch-6e6e.361f.8400-eth-0-9
```

Проверьте статистику DHCP-сервера (dut1):

```
Switch# show dhcp server statistics
DHCP server packet statistics:
=============================================================
Message Received:
BOOTREQUEST:   0
DHCPDISCOVER:  1
DHCPREQUEST:   1
DHCPDECLINE:   0
DHCPRELEASE:   0
```

```
DHCPINFORM:  0
Message Sent:
BOOTREPLY:  0
DHCPOFFER:  1
DHCPACK:  1
DHCPNAK:  0
```

Проверьте адреса и интерфейсы DHCP-сервера (dut1):

```
Switch# show dhcp server binding all
 IP address      Client-ID/              Lease expiration             Type
                 Hardware address
 5.5.5.2         6e:6e:36:1f:84:00      Sat 2012.02.04 08:00:12      Dynamic
Switch# show dhcp server interfaces
List of DHCP server enabled interface(s):
DHCP server service status: enabled
Interface Name
=============================================================
eth-0-9
```

4.6.2.2 Настройка DHCP-сервера с ретрансляцией

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите DHCP-сервер глобально, настройте пул IP-адресов и DHCP-ретранслятор.

Настройка на DUT1:

```
Switch(config)#service dhcp enable
Switch(config)#dhcp server
Switch(dhcp-config)#dhcp pool pool4
Switch(dhcp-config)#network 4.4.4.0/24
Switch(dhcp-config)#gateway 4.4.4.1
Switch(dhcp-config)#exit
```

Настройка на DUT2:

```
Switch(config)#service dhcp enable
Switch(config)#dhcp relay
Switch(config)#dhcp-server 1 5.5.5.1
```

Шаг 3. Добавьте IP-маршрут.

Настройка на DUT1:

```
Switch(config)#ip route 4.4.4.0/24 5.5.5.2
```

Шаг 4. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес.

Настройка на DUT1:

```
Switch(config)#interface eth-0-9
Switch (config-if)#no switchport
Switch (config-if)# no shutdown
Switch (config-if)# ip address 5.5.5.1/24
Switch (config-if)# dhcp server enable
Switch (config-if)#exit
```

Настройка на DUT2:

```
Switch(config)#interface eth-0-17
Switch (config-if)#no switchport
Switch (config-if)# no shutdown
Switch (config-if)# ip address 4.4.4.1/24
Switch (config-if)# dhcp-server 1

Switch (config-if)#interface eth-0-9
Switch (config-if)#no switchport
Switch (config-if)# no shutdown
Switch (config-if)# ip address 5.5.5.2/24
Switch (config-if)#exit
```

Настройка на DUT3:

```
Switch(config)#interface eth-0-17
Switch (config-if)#no switchport
Switch (config-if)# no shutdown
Switch (config-if)# ip address dhcp
Switch (config-if)#exit
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Проверьте конфигурацию DHCP-сервера (dut1):

```
Switch# show running-config
!
service dhcp enable
!
interface eth-0-9
 no switchport
 dhcp server enable
 ip address 5.5.5.1/24!
!
```

```
ip route 4.4.4.0/24 5.5.5.2
!
dhcp server
dhcp pool pool4
 network 4.4.4.0/24
 gateway 4.4.4.1
```

Проверка. состояния DHCP-клиентов DHCP-сервера (dut1):

```
Switch# show dhcp client verbose
DHCP client informations:
============================================================
eth-0-17 DHCP client information:
  Current state: BOUND
  Allocated IP: 4.4.4.5 255.255.255.0
  Lease/renewal/rebinding: 1199/517/1049 seconds
  Lease from 2012-02-06 05:23:09 to 2012-02-06 05:43:09
  Will Renewal in 0 days 0 hours 8 minutes 37 seconds
  DHCP server: 5.5.5.1
  Transaction ID: 0x192a4f7d
  Default router: 4.4.4.1
  Classless static route:
    Destination: 5.5.4.0, mask: 255.255.255.0, Nexthop: 4.4.4.1
  TFTP server addresses: 5.5.5.3
  Client ID: switch-3c9a.b29a.ba00-eth-0-17
```

Проверьте статистику DHCP-сервера (dut1):

```
Switch# show dhcp server statistics
DHCP server packet statistics:
============================================================
Message Received:
BOOTREQUEST:  0
DHCPDISCOVER:  1
DHCPREQUEST:  1
DHCPDECLINE:  0
DHCPRELEASE:  0
DHCPINFORM:  0
Message Sent:
BOOTREPLY:  0
DHCPOFFER:  1
DHCPACK:  1
DHCPNAK:  0
```

Проверьте адреса и интерфейсы DHCP-сервера (dut1):

```
Switch# show dhcp server binding all
IP address      Client-ID/              Lease expiration              Type
                 Hardware address
 4.4.4.5         3c:9a:b2:9a:ba:00     Mon 2012.02.06 05:43:09      Dynamic
Switch# show dhcp server interfaces
```

```
List of DHCP server enabled interface(s):
DHCP server service status: enabled
Interface Name
============================================================
eth-0-9
```

4.7 Настройка DNS

4.7.1 Общие положения

4.7.1.1 Описание функции

Протокол DNS управляет системой доменных имен (DNS), с помощью которой можно сопоставлять имена хостов с IP-адресами. При настройке DNS на коммутаторе вы можете заменить IP-адрес именем хоста для многих команд, таких как ping, telnet, connect. Доменные имена объединяются с помощью точек (.) в качестве разделительных символов. Необходимо сначала определить имена хостов, указать сервер имен, присутствующий в вашей сети, и включить DNS.

4.7.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Укажите доменное имя DNS и адрес DNS-сервера.

```
Switch(config)#dns domain server1
Switch(config)#dns server 202.100.10.20
```

Шаг 3. Установите статические сопоставления имени хоста с адресом (необязательно).

```
Switch(config)# ip host www.example1.com 192.0.2.141
```

Шаг 4. Проверка.

```
Switch# show dns server
Current DNS name server configuration:
     Server                  IP Address
------------------------------------------------------------
1    nameserver              202.100.10.20
```

5 Руководство по настройке IP-маршрутизации

5.1 Настройка IP-маршрутизации Unicast трафика

5.1.1 Общие положения

5.1.1.1 Описание функции

Статическая маршрутизация — это один из способов настройки выбора пути маршрутизаторами в компьютерных сетях. При статической маршрутизации нет обмена информацией между маршрутизаторами о текущей топологии сети. Маршруты вносятся вручную в таблицу маршрутизации. Противоположностью статической маршрутизации является динамическая маршрутизация.

Статические маршруты обычно вводятся в маршрутизатор системным администратором. Вся сеть может быть настроена с использованием статических маршрутов, но такой тип конфигурации не является отказоустойчивым. При изменении в сети или сбое между двумя узлами, имеющими статические маршруты друг к другу, трафик не будет перенаправлен. Нужно будет либо дождаться устранения сбоя, либо обновления статического маршрута администратором. Однако бывают случаи, когда статические маршруты могут улучшить производительность сети. К таким случаям относятся не транзитные сети и маршруты по умолчанию.

5.1.2 Настройка

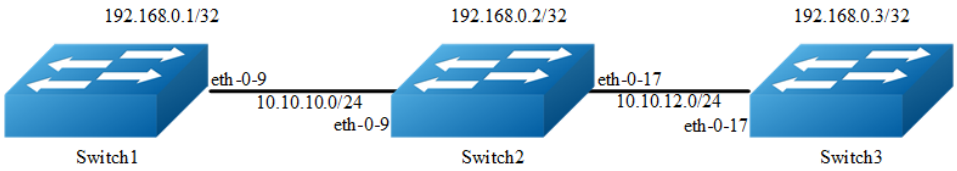


Рисунок 29 – IP-маршрутизация для unicast

В этом примере показано, как включить статическую маршрутизацию в простой сетевой топологии.

На коммутаторе Switch1 имеется 3 статических маршрута: один к удаленной сети 10.10.12.0/24, два других — к адресам на коммутаторах Switch2 и Switch3. На коммутаторе Switch3 есть статический маршрут по умолчанию, то есть статические маршруты используют один и тот же шлюз или адрес следующего перехода. На коммутаторе Switch2 имеется 2 статических маршрута, оба к адресам на удаленном коммутаторе.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес.

Switch1:

```
Switch(config)# interface eth-0-9
Switch(config-if)# no shutdown
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
Switch(config-if)# exit

Switch(config)# interface loopback 0
Switch(config-if)# ip address 192.168.0.1/32
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-9
Switch(config-if)# no shutdown
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.2/24
Switch(config-if)# exit

Switch(config)# interface eth-0-17
Switch(config-if)# no shutdown
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.12.2/24
Switch(config-if)# exit

Switch(config)# interface loopback 0
Switch(config-if)# ip address 192.168.0.2/32
Switch(config-if)# exit
```

Switch3:

```
Switch(config)# interface eth-0-17
Switch(config-if)# no shutdown
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.12.3/24
Switch(config-if)# exit

Switch(config)# interface loopback 0
Switch(config-if)# ip add 192.168.0.3/32
Switch(config-if)# exit
```

Шаг 3. Настройка статического маршрута.

Switch1:

Примечание: Укажите префикс назначения и маску для сети, для которой требуется шлюз, например, 10.10.12.0/24. Добавьте шлюз для каждой из них (в данном случае 10.10.10.2 для всех). Поскольку R2 является единственным доступным следующим узлом, вы можете настроить маршрут по умолчанию вместо настройки одного и того же статического маршрута для отдельных адресов.

```
Switch(config)# ip route 10.10.12.0/24 10.10.10.2
Switch(config)# ip route 192.168.0.2/32 10.10.10.2
Switch(config)# ip route 192.168.0.3/32 10.10.10.2
```

Switch2:

```
Switch(config)# ip route 192.168.0.1/32 10.10.10.1
Switch(config)# ip route 192.168.0.3/32 10.10.12.3
```

Switch3:

Примечание: Укажите 10.10.12.2 в качестве шлюза по умолчанию для доступа к любой сети. Поскольку 10.10.12.2 — это единственный доступный маршрут, вы можете указать его в качестве шлюза по умолчанию вместо того, чтобы указывать его в качестве шлюза для отдельных сетевых адресов.

```
Switch(config)# ip route 0.0.0.0/0 10.10.12.2
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

Для отображения информации о маршруте на коммутаторе Switch1 используйте следующую команду:

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       [*] - [AD/Metric]
       * - candidate default
C       10.10.10.0/24 is directly connected, eth-0-9
C       10.10.10.1/32 is in local loopback, eth-0-9
S       10.10.12.0/24 [1/0] via 10.10.10.2, eth-0-9
```

```
C       192.168.0.1/32 is directly connected, loopback0
S       192.168.0.2/32 [1/0] via 10.10.10.2, eth-0-9
S       192.168.0.3/32 [1/0] via 10.10.10.2, eth-0-9
```

Для отображения информации о маршруте на коммутаторе Switch2 используйте следующую команду:

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       [*] - [AD/Metric]
       * - candidate default
C       10.10.10.0/24 is directly connected, eth-0-9
C       10.10.10.2/32 is in local loopback, eth-0-9
C       10.10.12.0/24 is directly connected, eth-0-17
C       10.10.12.2/32 is in local loopback, eth-0-17
S       192.168.0.1/32 [1/0] via 10.10.10.1, eth-0-9
C       192.168.0.2/32 is directly connected, loopback0
S       192.168.0.3/32 [1/0] via 10.10.12.3, eth-0-17
```

Для отображения информации о маршруте на коммутаторе Switch3 используйте следующую команду:

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       [*] - [AD/Metric]
       * - candidate default
Gateway of last resort is 10.10.12.2 to network 0.0.0.0
S*      0.0.0.0/0 [1/0] via 10.10.12.2, eth-0-17
C       10.10.12.0/24 is directly connected, eth-0-17
C       10.10.12.3/32 is in local loopback, eth-0-17
C       192.168.0.3/32 is directly connected, loopback0
```

5.2 Настройка протокола RIP

5.2.1 Общие положения

5.2.1.1 Описание функции

Routing Information Protocol (RIP) это протокол обмена IP-маршрутами. RIP является протоколом дистанционно-векторной маршрутизации и для нахождения кратчайшего маршрута использует количество транзитных участков (метрику). Если маршрутизатор получает информацию от другого маршрутизатора, содержащую более короткий путь, старый маршрут заменяется на новый. Новый путь добавляется в таблицу, которая анонсируется другим маршрутизаторам. Маршрутизатор, передавший информацию о используемом маршруте, отмечается в таблице маршрутизации как следующий узел (next-hop). Маршрутизаторы RIP могут изменять метрику маршрута путем ее добавления, чтобы изменить выбор маршрута. В этом случае фактическое количество транзитных участков на маршрутах может быть одинаковым, однако метрика одного из маршрутов будет иметь более высокое значение. Максимальная допустимая для RIP метрика равна 15. Любой пункт назначения с более высокой метрикой считается недоступным. Низкое максимальное количество переходов предотвращает образование бесконечных петель в сети.

В этой главе приведены примеры базовой конфигурации RIP. Для получения подробной информации о командах, используемых в этих примерах, или для просмотра результатов выполнения команд проверки обратитесь к справочнику команд RIP. Во избежание повторений некоторые распространенные команды, такие как configure terminal, не указаны в разделе «Используемые команды».

5.2.1.2 Стандартизированное описание прокола

Ссылка на RFC 2453

5.2.2 Настройка

5.2.2.1 Включение RIP

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
```

```
Switch(config-if)# ip address 10.10.10.10/24
Switch(config-if)# exit

Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 10.10.11.10/24
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 10.10.12.10/24
Switch(config-if)# exit

Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 10.10.11.50/24
Switch(config-if)# exit
```

Шаг 3. Включите процесс маршрутизации RIP и свяжите сети.

Switch1:

```
Switch(config)# router rip
Switch(config-router)#network 10.10.10.0/24
Switch(config-router)#network 10.10.11.0/24
Switch(config-router)# exit
```

Switch2:

```
Switch(config)# router rip
Switch(config-router)#network 10.10.11.0/24
Switch(config-router)#network 10.10.12.0/24
Switch(config-router)# exit
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

Для отображения базы данных RIP на коммутаторе Switch1 используйте следующую команду:

```
Switch# show ip rip database
Codes:  R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
```

```
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
   Network            Next Hop         Metric From            If        Time
Rc 10.10.10.0/24                           1                   eth-0-1
Rc 10.10.11.0/24                           1                   eth-0-9
R  10.10.12.0/24      10.10.11.50        2 10.10.11.50     eth-0-9   00:02:52
```

Для отображения состояния протокола RIP на коммутаторе Switch1 используйте следующую команду:

```
Switch# show ip protocols rip
Routing protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds, next due in 17 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send          Recv   Key-chain
    eth-0-1          2             2
    eth-0-9          2             2
  Routing for Networks:
    10.10.10.0/24
    10.10.11.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.11.50           120  00:00:22               0           0
  Number of routes (including connected): 3
  Distance: (default is 120)
```

Для отображения интерфейса RIP на Switch1 используйте следующую команду:

```
Switch# show ip rip interface
eth-0-1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth-0-9 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
```

```
    IP interface address :
      10.10.11.10/24
```

Для отображения маршрутов на коммутаторе Switch1 используйте следующую команду:

```
Switch# show ip route
Codes :  K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       [*] - [AD/Metric]
       * - candidate default
C       10.10.10.0/24 is directly connected, eth-0-1
C       10.10.10.10/32 is in local loopback, eth-0-1
C       10.10.11.0/24 is directly connected, eth-0-9
C       10.10.11.10/32 is in local loopback, eth-0-9
R       10.10.12.0/24 [120/2] via 10.10.11.50, eth-0-9, 00 : 25 : 50
```

5.2.2.2 Настройка версии RIP

Настройте прием и отправку определенных версий пакетов на интерфейсе.

В этом примере коммутатор Switch2 настроен на прием и отправку протоколов RIP версий 1 и 2 через интерфейсы eth-0-9 и eth-0-20.

Шаг 1. Войдите в режим настройки.

На коммутаторе Switch2 выполняются следующие команды:

```
Switch# configure terminal
```

Шаг 2. Включить процесс маршрутизации RIP.

```
Switch(config)# router rip
Switch(config-router)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и установите версию для отправки и приема RIP-пакетов.

```
Switch(config)# interface eth-0-9
Switch(config-if)# ip rip send version 1 2
Switch(config-if)# ip rip receive version 1 2
Switch(config-if)# quit

Switch(config)# interface eth-0-20
Switch(config-if)# ip rip send version 1 2
```

```
Switch(config-if)# ip rip receive version 1 2
Switch(config-if)# quit
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

Для отображения конфигурации на коммутаторе Switch1 используйте следующую команду:

```
Switch# show running-config
interface eth-0-9
 no switchport
 ip address 10.10.11.10/24
!
router rip
 network 10.10.11.0/24
```

Для отображения базы данных RIP на Switch2 используйте следующую команду:

```
Switch# show ip rip database
Codes:  R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
        C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
    Network            Next Hop         Metric From            If       Time
R   10.0.0.0/8                               1                  eth-0-9
Rc 10.10.11.0/24                            1                 eth-0-9
Rc 10.10.12.0/24                            1                 eth-0-20
```

Для отображения состояния протокола RIP на коммутаторе Switch2 используйте следующую команду:

```
Switch# show ip protocols rip
Routing protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds, next due in 1 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control:  send version 2, receive version 2
    Interface         Send          Recv   Key-chain
    eth-0-9           1 2           1 2
    eth-0-20          1 2           1 2
  Routing for Networks:
    10.10.11.0/24
    10.10.12.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
```

```
    10.10.11.10            120   00:00:22              0            0
    10.10.12.50            120   00:00:27              0            0
  Number of routes (including connected) :  3
  Distance :  (default is 120)
```

Для отображения интерфейса RIP на Switch2 используйте следующую команду:

```
Switch# show ip rip interface
eth-0-9 is up, line protocol is up
  Routing Protocol :  RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface :  Disabled
    Split horizon :  Enabled with Poisoned Reversed
    IP interface address :
      10.10.11.50/24
eth-0-20 is up, line protocol is up
  Routing Protocol :  RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface :  Disabled
    Split horizon :  Enabled with Poisoned Reversed
    IP interface address :
      10.10.12.10/24
```

Для отображения конфигурации на коммутаторе Switch2 используйте следующую команду:

```
Switch# show run
interface eth-0-9
 no switchport
 ip address 10.10.11.50/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth-0-20
 no switchport
 ip address 10.10.12.10/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
 network 10.10.11.0/24
 network 10.10.12.0/24
```

Для отображения конфигурации на коммутаторе Switch3 используйте следующую команду:

```
Switch# show running-config
interface eth-0-20
 no switchport
```

```
 ip address 10.10.12.50/24
!
router rip
 network 10.10.12.0/24
```

5.2.2.3 Настройка параметров метрик

Offset list - механизм, позволяющий изменять метрики маршрутов. Offset list может быть применен к конкретному интерфейсу или с помощью ACL могут быть отфильтрованы конкретные сети для которых требуется изменение метрики. Изменением метрики можно повлиять на выбор маршрута коммутатором

Offset list состоит из следующих параметров:

- Список контроля доступа (ACL), определяющий маршруты, к которым следует добавить метрику. Направление:
- In: применяется к маршрутам, которые маршрутизатор получает от соседей по протоколу RIP.
- Out: применяется к маршрутам, которые маршрутизатор объявляет своим RIP-соседям.
- Значение смещения, которое будет добавлено к метрике маршрутизации маршрутов, соответствующих списку контроля доступа (ACL).
- Интерфейс, к которому применяется список смещений (необязательно)).

Если маршрут соответствует как глобальному offset листу (без указания интерфейса), так и offset листу на основе интерфейса, то приоритет имеет тот, что на основе интерфейса. В этом случае к маршруту добавляется метрика из offset листа на основе интерфейса.

В этом примере коммутатор Switch1 будет объявлять маршрут 1.1.1.0 из интерфейса eth-0-13 с метрикой 3.

Шаг 1. Текущая конфигурация.

Switch1

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
interface eth-0-13
no switchport
```

```
ip address 13.1.1.1/24
!
router rip
network 1.1.1.0/24
network 10.10.11.0/24
network 13.1.1.0/24
```

Switch2

```
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
interface eth-0-20
no switchport
ip address 10.10.12.10/24
!
router rip
network 10.10.11.0/24
network 10.10.12.0/24
```

Switch3

```
interface eth-0-13
no switchport
ip address 13.1.1.2/24
!
interface eth-0-20
no switchport
ip address 10.10.12.50/24
!
router rip
network 10.10.12.0/24
network 13.1.1.0/24
```

Маршруты на Switch3:

```
Switch# show ip route rip
R       1.1.1.0/24 [120/2] via 13.1.1.1, eth-0-13, 00:07:46
R       10.10.11.0/24 [120/2] via 13.1.1.1, eth-0-13, 00:07:39
                      [120/2] via 10.10.12.10, eth-0-20, 00:07:39
Change router 1.1.1.0/24 via 10.10.12.10
```

Шаг 2. Войдите в режим настройки.

Следующие команды выполняются на коммутаторе Switch1:

```
Switch# configure terminal
```

Шаг 3. Настройка списка доступа.

```
Switch(config)#ip access-list ripoffset
Switch(config-ip-acl)#permit any 1.1.1.0 0.0.0.255 any
```

Шаг 4. Включите процесс маршрутизации RIP и задайте offset лист для интерфейса.

```
Switch(config-ip-acl)# router rip
Switch(config-router)# offset-list ripoffset out 3 eth-0-13
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config-router)# end
```

Шаг 6. Проверка.

Отобразить маршруты на коммутаторе Switch3. Метрика для маршрута, распределяемого коммутатором Switch1, теперь равна 3.

```
Switch# show ip route rip
R       1.1.1.0/24 [120/3] via 10.10.12.10, eth-0-20, 00:00:02
R       10.10.11.0/24 [120/2] via 13.1.1.1, eth-0-13, 00:11:40
                    [120/2] via 10.10.12.10, eth-0-20, 00:11:40
```

5.2.2.4 Настройка административного расстояния

По умолчанию RIP назначает маршрутам RIP стандартное административное расстояние (120). При сравнении маршрутов на основе административного расстояния маршрутизатор выбирает маршрут с меньшим расстоянием. Вы можете изменить административное расстояние для маршрутов RIP.

В этом примере все коммутаторы используют два протокола маршрутизации: RIP и OSPF. Маршрут OSPF имеет более высокий приоритет, коммутатор 3 изменит маршрут 1.1.1.0 с административным расстоянием 100.

Шаг 1. Текущая конфигурация.

Switch1

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
```

```
router ospf
network 1.1.1.0/24 area 0
network 10.10.11.0/24 area 0
!
router rip
network 1.1.1.0/24
network 10.10.11.0/24
```

Switch2

```
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
interface eth-0-20
no switchport
ip address 10.10.12.10/24
!
router ospf
network 10.10.11.0/24 area 0
network 10.10.12.0/24 area 0
!
router rip
network 10.10.11.0/24
network 10.10.12.0/24
```

Switch3

```
interface eth-0-20
no switchport
ip address 10.10.12.50/24
!
router ospf
network 10.10.12.0/24 area 0
!
router rip
network 10.10.12.0/24
```

Маршруты на Switch3:

```
Switch# show ip route
Codes:  K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
        [*] - [AD/Metric]
        * - candidate default
O       1.1.1.0/24 [110/3] via 10.10.12.10, eth-0-20, 01:05:49
```

```
O       10.10.11.0/24 [110/2] via 10.10.12.10, eth-0-20, 01:05:49
C       10.10.12.0/24 is directly connected, eth-0-20
C       10.10.12.50/32 is in local loopback, eth-0-20
```

Шаг 2. Войдите в режим настройки.

На коммутаторе Switch3 выполняются следующие команды:

```
Switch# configure terminal
```

Шаг 3. Настройка списка доступа.

```
Switch(config)#ip access-list ripdistancelist
Switch(config-ip-acl)#permit any 1.1.1.0 0.0.0.255 any
```

Шаг 4. Включите процесс маршрутизации RIP и установите административное расстояние.

```
Switch(config-ip-acl)# router rip
Switch(config-router)# distance 100 0.0.0.0/0 ripdistancelist
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config-router)# end
```

Шаг 6. Проверка.

Отобразите маршруты на Switch3. Расстояние для маршрута Rip теперь составляет 100.

```
Switch# show ip route
Codes:  K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
        [*] - [AD/Metric]
        * - candidate default
R        1.1.1.0/24 [100/3] via 10.10.12.10, eth-0-20, 00:00:02
O        10.10.11.0/24 [110/2] via 10.10.12.10, eth-0-20, 01:10:42
C        10.10.12.0/24 is directly connected, eth-0-20
C        10.10.12.50/32 is in local loopback, eth-0-20
```

5.2.2.5 Настройка перераспределения

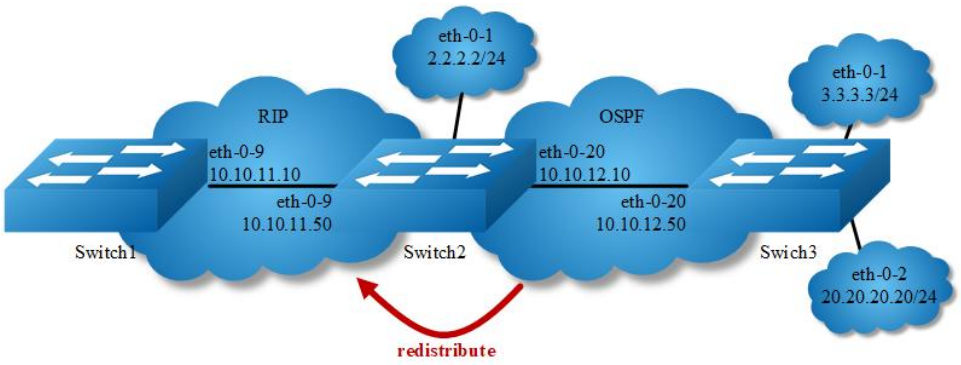


Рисунок 30 – RIP перераспределение

Вы можете настроить маршрутизатор для перераспределения статических маршрутов, маршрутов прямого подключения или маршрутов, полученных через протокол OSPF (Open Shortest Path First), в протокол RIP. При перераспределении маршрута в RIP, маршрутизатор может использовать RIP для объявления маршрута своим соседям по протоколу RIP.

Измените метрику перераспределения по умолчанию (необязательно). По умолчанию маршрутизатор присваивает каждому перераспределяемому маршруту метрику RIP, равную 1. Вы можете изменить значение метрики по умолчанию на значение до 16.

Включите перераспределение указанных маршрутов с метрикой по умолчанию или указанной метрикой. В этом примере маршрутизатор установит метрику по умолчанию равной 2 для перераспределяемых маршрутов и будет перераспределять статические маршруты и маршруты прямого подключения в RIP с метрикой по умолчанию 2, а маршруты OSPF — с указанной метрикой 5.

Шаг 1. Текущая конфигурация.

Switch1

```
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
router rip
network 10.10.11.0/24
```

Switch2

```
interface eth-0-1
no switchport
ip address 2.2.2.2/24
!
interface eth-0-9
no switchport
```

```
ip address 10.10.11.50/24
!
interface eth-0-20
no switchport
ip address 10.10.12.10/24
!
router ospf
network 10.10.12.0/24 area 0
!
router rip
network 10.10.11.0/24
!
ip route 20.20.20.0/24 10.10.12.50
```

Switch3

```
interface eth-0-1
no switchport
ip address 3.3.3.3/24
!
interface eth-0-2
no switchport
ip address 20.20.20.20/24
!
interface eth-0-20
no switchport
ip address 10.10.12.50/24
!
router ospf
network 3.3.3.0/24 area 0
network 10.10.12.0/24 area 0
```

Маршруты Switch1:

```
Switch# show ip route
Codes:  K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
        [*] - [AD/Metric]
        * - candidate default
C        10.10.11.0/24 is directly connected, eth-0-9
C        10.10.11.10/32 is in local loopback, eth-0-9
```

Маршруты Switch2:

```
Switch# show ip route
Codes:  K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       [*] - [AD/Metric]
       * - candidate default
C       2.2.2.0/24 is directly connected, eth-0-1
C       2.2.2.02/32 is in local loopback, eth-0-1
O       3.3.3.0/24 [110/2] via 10.10.12.50, eth-0-20, 01:05:41
C       10.10.11.0/24 is directly connected, eth-0-9
C       10.10.11.50/32 is in local loopback, eth-0-9
C       10.10.12.0/24 is directly connected, eth-0-20
C       10.10.12.10/24 is in local loopback, eth-0-20
S       20.20.20.0/24 [1/0] via 10.10.12.50, eth-0-20
```

Шаг 2. Войдите в режим настройки.

На коммутаторе Switch2 выполняются следующие команды:

```
Switch# configure terminal
```

Шаг 3. Включите процесс маршрутизации RIP, установите метрику и включите перераспределение.

```
Switch(config)# router rip
Switch(config-router)# default-metric 2
Switch(config-router)# redistribute static
Switch(config-router)# redistribute connected
Switch(config-router)# redistribute ospf metric 5
```

Перераспределение подключенных маршрутов по OSPF (необязательно)

```
Switch(config)# router ospf
Switch(config-router)# redistribute connected
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config-router)# end
```

Шаг 5. Проверка.

Отобразите маршруты на коммутаторе Switch1:

```
Switch# show ip route
Codes:  K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       [*] - [AD/Metric]
       * - candidate default
R       2.2.2.0/24 [120/3] via 10.10.11.50, eth-0-9, 00:02:36
R       3.3.3.0/24 [120/6] via 10.10.11.50, eth-0-9, 00:02:26
C       10.10.11.0/24 is directly connected, eth-0-9
C       10.10.11.10/32 is in local loopback eth-0-9
R       10.10.12.0/24 [120/3] via 10.10.11.50, eth-0-9, 00:02:36
R       20.20.20.0/24 [120/3] via 10.10.11.50, eth-0-9, 00:02:41
```

5.2.2.6 Настройка параметра Split-horizon

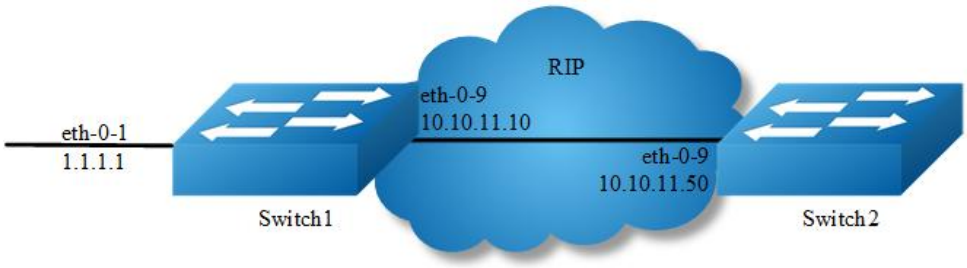


Рисунок 31 – RIP Split-Horizon

Обычно маршрутизаторы, подключенные к широковещательным IP-сетям и использующие протоколы маршрутизации на основе векторов расстояний, применяют механизм разделения горизонта (split horizon) для уменьшения вероятности образования маршрутных петель. Механизм разделения горизонта блокирует передачу информации о маршрутах маршрутизатором через любой интерфейс, с которого эта информация поступила. Такое поведение обычно оптимизирует обмен данными между несколькими маршрутизаторами, особенно при обрыве связи. Однако в сетях, не использующих широковещательную передачу (например, Frame Relay), могут возникать ситуации, когда такое поведение не является оптимальным. В таких случаях может потребоваться отключить механизм разделения горизонта для RIP.

Вы можете избежать включения маршрутов в обновления, отправляемые тому же шлюзу, от которого они были получены. Использование команды split horizon исключает маршруты, полученные от одного соседа, из обновлений, отправляемых ему же. Использование дополнительного параметра «poisoned» включает такие маршруты в обновления, но устанавливает их метрики в бесконечность. Таким образом, объявление этих маршрутов означает, что они недоступны.

Шаг 1. Текущая конфигурация.

Switch1

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
router rip
network 10.10.11.0/24
redistribute connected
```

Switch2

```
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
router rip
network 10.10.11.0/24
```

Шаг 2. Включение отладки на Switch2 (необязательно).

```
Switch# debug rip packet send detail
Switch# terminal monitor
```

Шаг 3. Войдите в режим настройки.

На коммутаторе Switch2 выполняются следующие команды:

```
Switch# configure terminal
```

Шаг 4. Войдите в режим настройки интерфейса и установите параметр split-horizon.

```
Switch(config)#interface eth-0-9
Switch(config-if)# no ip rip split-horizon
```

Если включена отладка, будут отображаться следующие сообщения:

```
Apr  8 06:24:25 Switch RIP4-7: SEND[eth-0-9]: Send to 224.0.0.9:520
Apr  8 06:24:25 Switch RIP4-7: SEND[eth-0-9]: RESPONSE version 2 packet
size 44
Apr  8 06:24:25 Switch RIP4-7: 1.1.1.0/24 -> 0.0.0.0 family 2 tag 0 metric
2
Apr  8 06:24:25 Switch RIP4-7: 10.10.11.0/24 -> 0.0.0.0 family 2 tag 0
metric 1
```

Включите Split-Horizon и параметр poisoned:

```
Switch(config-if)# ip rip split-horizon
Switch(config-if)# ip rip split-horizon poisoned
```

Если включена отладка, будут отображаться следующие сообщения:

```
Apr  8 06:38:35 Switch RIP4-7: SEND[eth-0-9]: Send to 224.0.0.9:520
Apr  8 06:38:35 Switch RIP4-7: SEND[eth-0-9]: RESPONSE version 2 packet
size 44
Apr  8 06:38:35 Switch RIP4-7: 1.1.1.0/24 -> 0.0.0.0 family 2 tag 0 metric
16
Apr  8 06:38:35 Switch RIP4-7: 10.10.11.0/24 -> 0.0.0.0 family 2 tag 0
metric 16
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config-router)# end
```

Шаг 6. Проверка.

Для отображения конфигурации используйте следующую команду:

```
Switch# show running-config
interface eth-0-9
 no switchport
 ip address 10.10.11.50/24
!
router rip
 network 10.10.11.0/24
!
```

Для отображения интерфейса RIP используйте следующую команду:

```
Switch# show ip rip interface
eth-0-9 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.50/24
```

5.2.2.7 Настройка таймеров

Протокол RIP использует несколько таймеров, которые определяют такие параметры, как частота обновлений маршрутизации, время до того, как маршрут станет недействительным, и другие параметры. Вы можете настроить эти таймеры, чтобы оптимизировать производительность

RIP в соответствии с вашими потребностями в работе. Вы можете внести следующие изменения в настройки таймеров:

- скорость (время в секундах между обновлениями), с которой отправляются обновления маршрутизации;
- интервал времени (в секундах), по истечении которого маршрут объявляется недействительным;
- время (в секундах), которое должно пройти до удаления маршрута из таблицы маршрутизации.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите процесс маршрутизации RIP и установите таймеры.

Укажите таймер обновления таблицы маршрутизации в 10 секунд. Укажите таймер истечения времени ожидания информации о маршрутизации в 180 секунд. Укажите таймер сборки мусора для маршрутизации в 120 секунд:

```
Switch(config)# router rip
Switch(config-router)# timers basic 10 180 120
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-router)# end
```

Шаг 4. Проверка.

Для отображения состояния протокола процесса RIP используйте следующую команду:

```
Switch# show ip protocols rip
Routing protocol is "rip"
  Sending updates every 10 seconds with +/-5 seconds, next due in 2 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface         Send          Recv   Key-chain
    eth-0-9           2             2
  Routing for Networks:
    10.10.11.0/24
  Routing Information Sources:
```

```
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.11.50           120  00:00:02               0           0
  Number of routes (including connected) :  5
  Distance :  (default is 120)
```

5.2.2.8 Настройка фильтров распределения маршрутов RIP

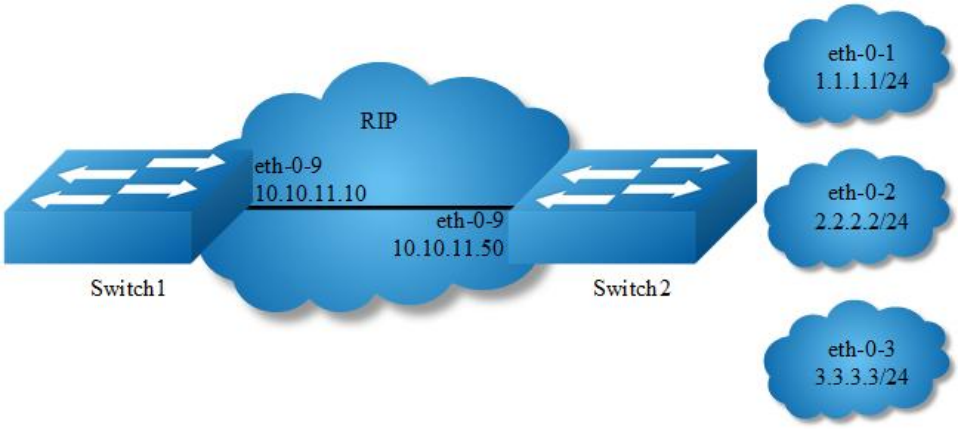


Рисунок 32 – RIP список фильтров

Список рассылки RIP позволяет разрешать или запрещать изучение или рассылку определенных маршрутов. Список рассылки состоит из следующих параметров:

- Список контроля доступа (ACL) или список префиксов, фильтрующий маршруты;
- Направление:
- входящее: фильтр применяется к входящим маршрутам;
- исходящее: фильтр применяется к исходящим маршрутам.

Шаг 1. Текущая конфигурация.

Switch1

```
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
router rip
network 10.10.11.0/24
```

Switch2

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-2
no switchport
ip address 2.2.2.2/24
```

```
!
interface eth-0-3
no switchport
ip address 3.3.3.3/24
!
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
router rip
network 1.1.1.0/24
network 2.2.2.0/24
network 3.3.3.0/24
network 10.10.11.0/24
```

Маршруты Switch1:

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       [*] - [AD/Metric]
       * - candidate default
R       1.1.1.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:01:50
R       2.2.2.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:01:50
R       3.3.3.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:01:50
C       10.10.11.0/24 is directly connected, eth-0-9
C       10.10.11.10/32 is in local loopback, eth-0-9
```

Шаг 2. Войдите в режим настройки.

На коммутаторе Switch2 выполняются следующие команды:

```
Switch# configure terminal
```

Шаг 3. Настройка списка префиксов.

```
Switch(config)# ip prefix-list 1 deny 1.1.1.0/24
Switch(config)# ip prefix-list 1 permit any
```

Шаг 4. Применить список префиксов.

```
Switch(config)# router rip
Switch(config-router)# distribute-list prefix 1 out
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config-router)# end
```

Шаг 6. Проверка.

Отобразите маршруты на коммутаторе Switch1:

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       [*] - [AD/Metric]
       * - candidate default
R       2.2.2.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:00:08
R       3.3.3.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:00:08
C       10.10.11.0/24 is directly connected, eth-0-9
C       10.10.11.10/32 is in local loopback, eth-0-9
```

5.2.2.9 Настройка аутентификации RIPv2 (один ключ)

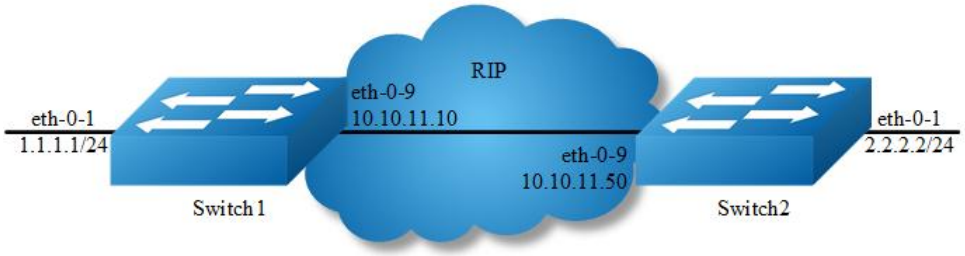


Рисунок 33 – RIP аутентификация

RIPv2 поддерживает 2 метода аутентификации: открытый текст и шифрование MD5.

В следующем примере показано, как включить аутентификацию в открытом текстовом виде.

Для использования этой функции необходимо выполнить следующие шаги:

- укажите интерфейс и задайте строку аутентификации.
- укажите режим аутентификации как «текстовый».

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# exit

Switch(config-if)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 10.10.11.10/24
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 2.2.2.2/24
Switch(config-if)# exit

Switch(config-if)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 10.10.11.50/24
Switch(config-if)# exit
```

Шаг 3. Включите процесс маршрутизации RIP и установите параметры.

```
Switch(config)# router rip
Switch(config-router)# network 10.10.11.0/24
Switch(config-router)# redistribute connected
Switch(config-router)# exit
```

Шаг 4. Укажите строку аутентификации и режим.

```
Switch(config)# interface eth-0-9
Switch(config-if)# ip rip authentication string Auth1
Switch(config-if)# ip rip authentication mode text
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 6. Проверка.

Для отображения базы данных RIP используйте следующую команду:

```
Switch# show ip rip database

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

   Network            Next Hop         Metric From            If       Time
R  2.2.2.0/24         10.10.11.50           2 10.10.11.50     eth-0-9
00:02:52
Rc 10.10.11.0/24
```

Для отображения состояния протокола RIP используйте следующую команду:

```
Switch# show ip protocols rip
Routing protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds, next due in 23 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
    connected  metric default
  Default version control: send version 2, receive version 2
    Interface        Send          Recv   Key-chain
    eth-0-9          2             2
  Routing for Networks:
    10.10.11.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.11.50           120  00:00:45               1           0
  Number of routes (including connected): 2
  Distance: (default is 120)



Switch# show ip rip interface
eth-0-9 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.10/24
```

Для отображения интерфейса RIP используйте следующую команду:

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       Dc - DHCP Client
       [*] - [AD/Metric]
       * - candidate default

R        2.2.2.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:02:28
C        10.10.11.0/24 is directly connected, eth-0-9
C        10.10.11.10/32 is in local loopback, eth-0-9
```

5.2.2.10 Настройка аутентификации RIPv2 MD5 (несколько ключей)

В этом примере показана аутентификация MD5 в процессе обмена маршрутной информацией для RIP с использованием нескольких ключей. Коммутаторы Switch1 и 2 используют RIP и обмениваются обновлениями маршрутизации. Для настройки аутентификации на Switch1 определите цепочку ключей, укажите ключи в цепочке ключей, а затем определите строку аутентификации или пароли, которые будут использоваться для ключей. Затем установите период времени, в течение которого можно получать или отправлять ключ аутентификации, указав время действия приема и отправки. [необязательно]. После определения строки ключа укажите цепочку ключей (или набор ключей), которая будет использоваться для аутентификации на интерфейсе, и используемый режим аутентификации. Настройте Switch2 так, чтобы у них был тот же идентификатор ключа и строка ключа, что и у Switch1, на время обмена обновлениями.

При аутентификации по MD5 сопоставляются как идентификатор ключа, так и строка ключа. В следующем примере коммутатор Switch2 имеет тот же идентификатор ключа и строку ключа, что и коммутатор Switch1. Для дополнительной безопасности время действия приема и время действия отправки настроены таким образом, что идентификатор ключа и строка ключа меняются каждые пять дней. Для обеспечения непрерывности время действия приема должно перекрываться; однако время действия отправки не должно перекрываться.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# exit
```

```
Switch(config-if)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 10.10.11.10/24
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 2.2.2.2/24
Switch(config-if)# exit

Switch(config-if)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 10.10.11.50/24
Switch(config-if)# exit
```

Шаг 3. Включите процесс маршрутизации RIP и установите параметры.

```
Switch(config)# router rip
Switch(config-router)# network 10.10.11.0/24
Switch(config-router)# redistribute connected
Switch(config-router)# exit
```

Шаг 4. Создайте связку ключей и задайте строку ключа и время жизни.

```
Switch(config)# key chain SUN
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string key1
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 2 2012 14:00:00 Mar
7 2012
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 2 2012 12:00:00 Mar 7
2012
Switch(config-keychain-key)# exit
```

Еще один key (необязательно):

```
Switch(config-keychain)# key 2
Switch(config-keychain-key)# key-string Earth
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 7 2012 14:00:00 Mar
12 2012
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 7 2012 12:00:00 Mar
12 2012
Switch(config-keychain-key)# exit
```

Выйти из режима настройки связки ключей:

```
Switch(config-keychain)# exit
```

Шаг 5. Укажите строку аутентификации и режим.

```
Switch(config)# interface eth-0-9
Switch(config-if)# ip rip authentication key-chain SUN
Switch(config-if)# ip rip authentication mode md5
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config-if)# end
```

Шаг 7. Проверка.

Для отображения базы данных RIP используйте следующую команду:

```
Switch# show ip rip database

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

   Network            Next Hop         Metric From            If       Time
R  2.2.2.0/24         10.10.11.50           2 10.10.11.50     eth-0-9
00:01:10
Rc 10.10.11.0/24                            1                 eth-0-9
```

Для отображения состояния протокола RIP используйте следующую команду:

```
Switch# show ip protocols rip
Routing protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds, next due in 17 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
    connected  metric default
  Default version control: send version 2, receive version 2
    Interface        Send          Recv   Key-chain
    eth-0-9          2             2      SUN
  Routing for Networks:
    10.10.11.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 2
  Distance: (default is 120)
```

Для отображения интерфейса RIP используйте следующую команду:

```
Switch# show ip rip interface
eth-0-9 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.10/24
```

Для отображения маршрутов на устройстве используйте следующую команду:

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       Dc - DHCP Client
       [*] - [AD/Metric]
       * - candidate default

C        1.1.1.0/24 is directly connected, eth-0-1
C        1.1.1.1/32 is in local loopback, eth-0-1
R        2.2.2.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:02:27
C        10.10.11.0/24 is directly connected, eth-0-9
C        10.10.11.10/32 is in local loopback, eth-0-9
```

Для отображения связки ключей используйте следующую команду:

```
Switch# show key chain
key chain SUN:
    key 1 -- text "key1"
      accept-lifetime <12:00:00 Mar 02 2012> - <14:00:00 Mar 07 2012>
      send-lifetime <12:00:00 Mar 02 2012> - < 12:00:00 Mar 07 2012>
    key 2 -- text "Earth"
      accept-lifetime <12:00:00 Mar 07 2012> - <14:00:00 Mar 12 2012>
      send-lifetime <12:00:00 Mar 07 2012> - < 12:00:00 Mar 12 2012>
Switch#
```

5.3 Настройка списка префиксов Prefix-list

5.3.1 Общие положения

5.3.1.1 Описание функции

Политика маршрутизации — это механизм изменения информации о маршруте. Список префиксов — это разновидность политики маршрутизации, используемая для управления и

изменения информации о маршрутизации. Список префиксов идентифицируется по имени списка и содержит одну или несколько упорядоченных записей, которые обрабатываются последовательно. Каждая запись предоставляет соответствующий диапазон для сетевого префикса и имеет уникальный порядковый номер в списке. В процессе сопоставления коммутатор последовательно проверяет записи.

5.3.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте список префиксов.

Примечание: Создайте список префиксов. Если последовательность правил не указана, система должна автоматически присвоить им порядковый номер. Поддерживаются различные действия, такие как разрешение и запрет. Поддерживается добавление строки описания для списка префиксов.

```
Switch(config)# ip prefix-list test seq 1 deny 35.0.0.0/8 le 16
Switch(config)# ip prefix-list test permit any
Switch(config)# ip prefix-list test description this prefix list is fot test
Switch(config)# ip prefix-list test permit 36.0.0.0/24
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения списка префиксов используйте следующую команду:

```
Switch# show ip prefix-list detail
Prefix-list list number: 1
Prefix-list entry number: 3
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
   Description: this prefix list is fot test
   count: 3, range entries: 0, sequences: 1 - 10
     seq 1 deny 35.0.0.0/8 le 16 (hit count: 0, refcount: 0)
     seq 5 permit any (hit count: 0, refcount: 0)
     seq 10 permit 36.0.0.0/24 (hit count: 0, refcount: 0)
```

5.3.2.1 Настройка для протокола RIP

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте список префиксов.

```
Switch(config)# ip prefix-list aa seq 11 deny 35.0.0.0/8 le 16
Switch(config)# ip prefix-list aa permit any
```

Шаг 3. Примените список префиксов в режиме конфигурации маршрутизатора RIP.

```
Switch(config)# router rip
Switch(config-router)# distribute-list prefix aa out
Switch(config-router)# exit
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

Для отображения списка префиксов используйте следующую команду:

```
Switch# show ip prefix-list
ip prefix-list aa: 2 entries
      seq 11 deny 35.0.0.0/8 le 16
      seq 15 permit any
```

Для отображения конфигурации устройства используйте следующую команду:

```
Switch# show running-config
Building configuration...
…
ip prefix-list aa seq 11 deny 35.0.0.0/8 le 16
ip prefix-list aa seq 15 permit any
…
router rip
 distribute-list prefix aa out
```

5.4 Настройка маршрутизации на основе политик

5.4.1 Общие положения

5.4.1.1 Описание функции

Маршрутизация на основе политик (PBR) предоставляет гибкость при пересылке и маршрутизации пакетов в соответствии с определенными политиками, что выходит за рамки традиционных протоколов маршрутизации. Используя маршрутизацию на основе политик, возможно внедрять политики, которые выборочно направляют пакеты по разным путям.

5.4.2 Настройка PBR

На рисунке выше представлена типовая топология: после включения PBR на интерфейсе eth-0-1 коммутатора Switch1 пакеты от 172.16.6.1 должны перенаправляться на 172.16.4.2, а остальные пакеты должны перенаправляться в соответствии с исходными маршрутами.

Настройка на коммутаторе Switch1:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте список доступа по IP-адресу, соответствующий IP-адресу источника.

```
Switch(config)# ip access-list acl1
Switch(config-ip-acl)# 10 permit any 172.16.6.0 0.0.0.255 any
Switch(config-ip-acl)# exit
```

Шаг 3. Создайте карту маршрутов, соответствующую списку доступа по IP-адресу, и задайте IP-адрес следующего перехода.

```
Switch(config)# route-map rmap permit 10
Switch(config-route-map)# match ip address acl1
Switch(config-route-map)# set ip next-hop 172.16.4.2
Switch(config-route-map)# exit
```

Шаг 4. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес, а также примените карту маршрутов.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.16.5.2/24
Switch(config-if)# no shutdown
Switch(config-if)# ip policy route-map rmap
```

```
Switch(config-if)# exit
```

Шаг 5. Создайте статический маршрут с IP-адресом следующего перехода 172.16.4.3 (необязательно).

Для пересылки пакетов, не попавших в PBR, можно использовать как статическую маршрутизацию так и динамические протоколы, такие как RIP/OSPF.

```
Switch(config)# ip route 0.0.0.0/0 172.16.4.3
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

```
Switch# show ip policy route-map
Route-map                       interface
rmap                            eth-0-1
```

6 Руководство по настройке Multicast

6.1 Настройка маршрутизации IP Multicast трафика

6.1.1 Общие положения

6.1.1.1 Описание функции

Протоколы многоадресной рассылки позволяют нескольким станциям (клиентам) получать доступ к группе каналов, транслируемых через различные сети, для приема и передачи многоадресных данных.

Распространение котировок акций, видео трансляции, такие как новостные вещания и дистанционные учебные занятия, или же видеоконференции — все это примеры трафика, передаваемого при помощи многоадресной маршрутизации.

- Протокол IGMP (Internet Group Management Protocol) используется между хостами в локальной сети и маршрутизаторами (и многоуровневыми коммутаторами) в этой сети для отслеживания многоадресных групп, в которые входят хосты;

- Sparse-mode - применяется когда получатели многоадресного трафика распределены по сети относительно редко;

- Dense-mode - применяется когда получатели и группы многоадресного трафика распределены по сети относительно плотно.

6.1.2 Настройка

6.1.2.1 Настройка ограничения количества маршрутов многоадресной рассылки

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2: Установите ограничение.

```
Switch(config)# ip multicast route-limit 1000
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show ip mroute route-limit
Max Multicast Route Limit Number: 1000
Multicast Route Limit Warning Threshold: 1000
Multicast Hardware Route Limit: 1023
Current Multicast Route Entry Number: 0
```

6.2 Настройка IGMP

6.2.1 Общие положения

6.2.1.1 Описание функции

Для участия в IP-многоадресной рассылке хосты, маршрутизаторы и многоуровневые коммутаторы должны поддерживать протокол IGMP. Этот протокол определяет роли запрашивающего и хоста:

- устройство, отправляющее запросы, — это сетевое устройство, которое рассылает сообщения-запросы для определения того, какие сетевые устройства являются членами заданной многоадресной группы;

- хост — это получатель, который отправляет отчетные сообщения (в ответ на запросы), чтобы сообщить запрашивающему о принадлежности к той или иной сети;

- Группа, состоящая из запрашивающих устройств и хостов, получающих многоадресные потоки данных из одного источника, называется многоадресной (multicast) группой. Участники группы используют сообщения IGMP для присоединения к многоадресным группам и выхода из них. Любой хост, независимо от того, является ли он членом группы, может отправлять сообщения в группу. Однако получают сообщения только члены группы. Членство в многоадресной группе является динамическим; хосты могут присоединяться и выходить из группы в любое время. Нет никаких ограничений на местоположение или количество участников в многоадресной группе.

Хост может одновременно состоять в нескольких многоадресных группах. Многоадресная группа может быть активной в течение длительного отрезка времени или существовать недолго. Состав группы может постоянно меняться. Группа, в которой есть участники, может быть и неактивной.

IGMP использует следующие IP-адреса:

- общие запросы IGMP направляются по адресу 224.0.0.1 (все системы в подсети);

- запросы IGMP, специфичные для конкретной группы, направляются на IP-адрес группы;

- отчеты о членстве в группах IGMP отправляются на IP-адрес группы;

- сообщения IGMP версии 2 (IGMPv2) отправляются на адрес 224.0.0.2 (адрес всех многоадресных маршрутизаторов в подсети). В некоторых старых стеках IP-адресов сообщения могут отправляться на групповой IP-адрес, а не на адрес всех маршрутизаторов.

6.2.2 Настройка

Нет явной команды для включения IGMP, он всегда используется в сочетании с PIM-SM. Когда PIM-SM включен на интерфейсе, IGMP автоматически включается на этом же интерфейсе, и наоборот. Для работы IGMP необходимо сначала глобально включить маршрутизацию IP-многоадресной рассылки. В коммутаторе есть поддержка создания IGMP группы как путем изучения пакетов IGMP так и настройкой статической группы IGMP администратором.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите глобально маршрутизацию IP multicast.

```
Switch(config)# ip multicast-routing
```

Шаг 3. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.10/24
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.11.10/24
Switch(config-if)# exit
```

Шаг 4. Включите pim-sm на интерфейсе.

```
Switch(config)# interface eth-0-1
Switch(config-if)# ip pim sparse-mode
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# ip pim sparse-mode
Switch(config-if)# exit
```

Шаг 5. Установите атрибуты для IGMP.

```
Switch(config)# interface eth-0-1
Switch(config-if)# ip igmp version 2
Switch(config-if)# ip igmp query-interval 120
Switch(config-if)# ip igmp query-max-response-time 12
Switch(config-if)# ip igmp robustness-variable 3
```

```
Switch(config-if)# ip igmp last-member-query-count 3
Switch(config-if)# ip igmp last-member-query-interval 2000
Switch(config-if)# exit
```

Шаг 6. Установите максимальное количество групп IGMP (необязательно).

Максимальное количество групп IGMP ограничено глобально или для каждого интерфейса отдельно.

```
Switch(config)# ip igmp limit 2000

Switch(config)# interface eth-0-1
Switch(config-if)# ip igmp limit 1000
```

Шаг 7. Создайте статическую группу IGMP.

```
Switch(config-if)# ip igmp static-group 228.1.1.1
Switch(config-if)# exit
```

Шаг 8. Настройка IGMP-прокси (необязательно).

```
Switch(config)# interface eth-0-1
Switch(config-if)# ip igmp proxy-service
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# ip igmp mroute-proxy eth-0-1
Switch(config-if)# exit
```

Шаг 9. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 10. Проверка.

Для отображения информации об интерфейсах IGMP используйте следующую команду:

```
Switch# show ip igmp interface
Interface eth-0-1 (Index 1)
 IGMP Inactive, Version 2 (default) proxy-service
 IGMP host version 2
 IGMP global limit is 2000
 IGMP global limit states count is currently 0
 IGMP interface limit is 1000
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP query interval is 120 seconds
```

```
 IGMP querier timeout is 366 seconds
 IGMP max query response time is 12 seconds
 Last member query response interval is 2000 milliseconds
 Group Membership interval is 372 seconds
 Last memeber query count is 3
 Robustness Variable is 3
Interface eth-0-2 (Index 2)
 IGMP Inactive, Version 2 (default)
 IGMP mroute-proxy interface is eth-0-1
 IGMP global limit is 2000
 IGMP global limit states count is currently 0
 IGMP interface limit is 16384
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Last memeber query count is 2
 Robustness Variable is 2
```

Для отображения информации о группах используйте следующую команду:

```
Switch# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface       Uptime   Expires Last Reporter
228.1.1.1        eth-0-1          00:00:05 stopped  -
```

6.3 Настройка IGMP Snooping

6.3.1 Общие положения

6.3.1.1 Описание функции

Коммутаторы уровня 2 могут использовать IGMP snooping для ограничения распространения многоадресного трафика путем динамической настройки интерфейсов уровня 2 таким образом, чтобы многоадресный трафик перенаправлялся только на те интерфейсы, которые связаны с устройствами IP-многоадресной рассылки. Как следует из названия, IGMP snooping требует от коммутатора локальной сети отслеживать передачи IGMP между хостом и маршрутизатором, а также следить за многоадресными группами и входящими в них портами. Когда коммутатор получает от хоста отчет IGMP для определенной многоадресной группы, он добавляет номер порта в таблицу пересылки; когда он получает сообщение IGMP Leave Group от хоста, он удаляет порт хоста из таблицы. Маршрутизатор периодически отправляет общие запросы во все VLAN. Все хосты, заинтересованные в этом многоадресном трафике, отправляют запрос и добавляются в таблицу пересылки.

Многоадресные группы уровня 2, изученные с помощью IGMP snooping, являются динамическими. Если вы задаете членство в группе для многоадресного адреса статически, настройка имеет приоритет над любыми автоматическими изменениями, внесенными IGMP snooping. Списки членства в многоадресных группах могут содержать как заданные пользователем, так и полученные с помощью IGMP snooping параметры.

Ограничения:

Протокол RIP использytt многоадресные IP-адреса, поэтому следует избегать использования многоадресных IP-адресов, имеющих тот же многоадресный MAC-адрес, что и многоадресный IP-адрес, зарезервированный RIP.

RIP использует адрес многоадресной группы 224.0.0.9, поэтому при одновременной работе IGMP Snooping и RIP необходимо избегать использования такого адреса многоадресной группы.

6.3.2 Настройка

6.3.2.1 Включить глобально или для каждого VLAN

IGMP Snooping можно включить глобально или для каждого VLAN отдельно. Если IGMP Snooping отключен глобально, он не может быть активен ни в одном VLAN, даже если он включен для этого VLAN. Если IGMP Snooping включен глобально, его можно отключить для конкретного VLAN. По умолчанию IGMP Snooping включен глобально и для каждого VLAN отдельно.

Шаг 1. Войдите в режим настройки.

```
Switch#configure terminal
```

Шаг 2. Включите IGMP snooping глобально и для каждого VLAN.

```
Switch(config)# ip igmp snooping
Switch(config)# ip igmp snooping vlan 1
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения результатов IGMP-отслеживания в VLAN используйте следующую команду:

```
Switch # show ip igmp snooping vlan 1
Global Igmp Snooping Configuration
------------------------------------------------
Igmp Snooping                              :Enabled
Igmp Snooping Fast-Leave                   :Disabled
```

```
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Report-Suppression             :Enabled
Vlan 1
-----------
Igmp Snooping                                :Enabled
Igmp Snooping Fast-Leave                     :Disabled
Igmp Snooping Report-Suppression             :Enabled
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Group Access-list              :N/A
Igmp Snooping Mrouter Port                   :
Igmp Snooping Mrouter Port Aging Interval(sec) :255
```

6.3.2.2 Настройка функции быстрого выхода

При включении функции IGMP Snooping fast leave группа IGMP Snooping будет немедленно удалена после получения соответствующего отчета IGMP. В противном случае коммутатор отправит запрос IGMP, и если в течение указанного периода не получит ответа, группа будет удалена. По умолчанию функция IGMP Snooping fast leave отключена глобально и для каждого VLAN.

Шаг 1. Войдите в режим настройки.

```
Switch#configure terminal
```

Шаг 2. Включите функцию быстрого выхода (Fast Leave) глобально и для каждого VLAN.

```
Switch(config)#ip igmp snooping fast-leave
Switch(config)#ip igmp snooping vlan 1 fast-leave
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch # show ip igmp snooping vlan 1
Global Igmp Snooping Configuration
------------------------------------------------
Igmp Snooping                                :Enabled
```

```
Igmp Snooping Fast-Leave                    :Enabled
Igmp Snooping Version                       :2
Igmp Snooping Robustness Variable           :2
Igmp Snooping Max-Member-Number             :2048
Igmp Snooping Unknown Multicast Behavior    :Flood
Igmp Snooping Report-Suppression            :Enabled
Vlan 1
-----------
Igmp Snooping                               :Enabled
Igmp Snooping Fast-Leave                    :Enabled
Igmp Snooping Report-Suppression            :Enabled
Igmp Snooping Version                       :2
Igmp Snooping Robustness Variable           :2
Igmp Snooping Max-Member-Number             :2048
Igmp Snooping Unknown Multicast Behavior    :Flood
Igmp Snooping Group Access-list             :N/A
Igmp Snooping Mrouter Port                  :
Igmp Snooping Mrouter Port Aging Interval(sec) :255
```

6.3.2.3 Настройка параметров для запрашивающего устройства

Для корректной работы IGMP, а следовательно, и IGMP snooping, в сети должен существовать многоадресный маршрутизатор, генерирующий IGMP-запросы. Таблицы, созданные для snooping (содержащие порты-участники каждой многоадресной группы), связаны с запрашивающим устройством. Без запрашивающего устройства таблицы не создаются, и snooping работать не будет.

Шаг 1. Войдите в режим настройки.

```
Switch#configure terminal
```

Шаг 2. Установите глобальные атрибуты IGMP snooping.

```
Switch(config)# ip igmp snooping query-interval 100
Switch(config)# ip igmp snooping query-max-response-time 5
Switch(config)# ip igmp snooping last-member-query-interval 2000
Switch(config)# ip igmp snooping discard-unknown
```

Шаг 3. Настройте атрибуты IGMP snooping для каждого VLAN.

```
Switch(config)# ip igmp snooping vlan 1 querier address 10.10.10.1
Switch(config)# ip igmp snooping vlan 1 querier
Switch(config)# ip igmp snooping vlan 1 query-interval 200
Switch(config)# ip igmp snooping vlan 1 query-max-response-time 5
Switch(config)# ip igmp snooping vlan 1 querier-timeout 100
```

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 2000
Switch(config)# ip igmp snooping vlan 1 discard-unknown
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

```
Switch # show ip igmp snooping querier
Global Igmp Snooping Querier Configuration
-----------------------------------------------
Version                          :2
Last-Member-Query-Interval (msec) :2000
Last-Member-Query-Count           :2
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)              :100
Global Source-Address             :0.0.0.0
TCN Query Count                   :2
TCN Query Interval (sec)          :10
TCN Query Max Respose Time (sec)  :5
Vlan 1:   IGMP snooping querier status
-----------------------------------------
Elected querier is : 0.0.0.0
-----------------------------------------
Admin state                       :Enabled
Admin version                     :2
Operational state                 :Non-Querier
Querier operational address       :10.10.10.1
Querier configure address         :10.10.10.1
Last-Member-Query-Interval (msec) :2000
Last-Member-Query-Count           :2
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)              :200
Querier-Timeout (sec)             :100
```

6.3.2.4 Настройка порта Mrouter

Порт mrouter с поддержкой IGMP Snooping — это порт коммутатора, предназначенный для подключения многоадресного маршрутизатора. Порт mrouter настраивается в соответствии с VLAN или динамически. Когда на порту указанного VLAN поступает пакет общего запроса IGMP или пакет приветствия PIMv2, этот порт становится портом mrouter этого VLAN. Все запросы IGMP, полученные на этом порту, будут рассылаться в принадлежащий VLAN. Все запросы и ответы IGMP, полученные в этом VLAN, будут пересылаться на порт mrouter напрямую. Кроме того, весь многоадресный трафик в этом VLAN будет пересылаться на этот порт mrouter.

Шаг 1. Войдите в режим настройки.

```
Switch#configure terminal
```

Шаг 2. Включите глобальное подавление отчетов IGMP Snooping.

```
Switch(config)# ip igmp snooping report-suppression
```

Шаг 3. Настройте порт mrouter, включите подавление отчетов IGMP snooping и установите динамический интервал устаревания mrouter для IGMP snooping для VLAN.

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface eth-0-1
Switch(config)# ip igmp snooping vlan 1 report-suppression
Switch(config)# ip igmp snooping vlan 1 mrouter-aging-interval 200
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

```
Switch# show ip igmp snooping vlan 1
Global Igmp Snooping Configuration
------------------------------------------------
Igmp Snooping                              :Enabled
Igmp Snooping Fast-Leave                   :Disabled
Igmp Snooping Version                      :2
Igmp Snooping Robustness Variable          :2
Igmp Snooping Max-Member-Number            :2048
Igmp Snooping Unknown Multicast Behavior   :Flood
Igmp Snooping Report-Suppression           :Enabled
Vlan 1
-----------
Igmp Snooping                              :Enabled
Igmp Snooping Fast-Leave                   :Disabled
Igmp Snooping Report-Suppression           :Enabled
Igmp Snooping Version                      :2
Igmp Snooping Robustness Variable          :2
Igmp Snooping Max-Member-Number            :2048
Igmp Snooping Unknown Multicast Behavior   :Flood
Igmp Snooping Group Access-list            :N/A
Igmp Snooping Mrouter Port                 :eth-0-1
Igmp Snooping Mrouter Port Aging Interval(sec) :200
```

6.3.2.5 Настройка TCN для запрашивающих устройств

Система поддерживает адаптацию процесса обучения и обновления многоадресного маршрутизатора после сходимости STP путем настройки количества и интервала запросов TCN.

Шаг 1. Войдите в режим настройки.

```
Switch#configure terminal
```

Шаг 2. Настройка количества и интервала запросов TCN.

```
Switch(config)# ip igmp snooping querier tcn query-count 5
Switch(config)# ip igmp snooping querier tcn query-interval 20
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch # show ip igmp snooping querier
Global Igmp Snooping Querier Configuration
-----------------------------------------------
Version                          :2
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec)     :10
Query-Interval (sec)              :125
Global Source-Address             :0.0.0.0
TCN Query Count                   :5
TCN Query Interval (sec)          :20
Vlan 1:   IGMP snooping querier status
-----------------------------------------
Elected querier is : 0.0.0.0
-----------------------------------------
Admin state                       :Disabled
Admin version                     :2
Operational state                 :Non-Querier
Querier operational address       :0.0.0.0
Querier configure address         :N/A
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec)     :10
Query-Interval (sec)              :125
Querier-Timeout (sec)             :255
```

6.3.2.6 Настройка подавления отчетов

Коммутатор использует подавление отчетов IGMP, чтобы пересылать только один отчет IGMP на каждый запрос одного маршрутизатора. Когда подавление запросов IGMP включено (по умолчанию), коммутатор отправляет первый отчет IGMP от всех хостов группы всем многоадресным маршрутизаторам. Коммутатор не отправляет остальные отчеты IGMP для группы многоадресным маршрутизаторам. Эта функция предотвращает отправку дублирующих отчетов многоадресным устройствам.

Шаг 1. Войдите в режим настройки.

```
Switch#configure terminal
```

Шаг 2. Включите подавление отчетов глобально и для каждого VLAN.

```
Switch(config)# ip igmp snooping report-suppression
Switch(config)# ip igmp snooping vlan 1 report-suppression
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch # show ip igmp snooping
Global Igmp Snooping Configuration
------------------------------------------------
Igmp Snooping                              :Enabled
Igmp Snooping Fast-Leave                   :Disabled
Igmp Snooping Version                      :2
Igmp Snooping Robustness Variable          :2
Igmp Snooping Max-Member-Number            :2048
Igmp Snooping Unknown Multicast Behavior   :Flood
Igmp Snooping Report-Suppression           :Enabled
Vlan 1
-----------
Igmp Snooping                              :Enabled
Igmp Snooping Fast-Leave                   :Disabled
Igmp Snooping Report-Suppression           :Enabled
Igmp Snooping Version                      :2
Igmp Snooping Robustness Variable          :2
Igmp Snooping Max-Member-Number            :2048
Igmp Snooping Unknown Multicast Behavior   :Flood
Igmp Snooping Group Access-list            :N/A
```

```
Igmp Snooping Mrouter Port                    :
Igmp Snooping Mrouter Port Aging Interval(sec) :255
```

6.3.2.7 Настройка статической группы

Коммутатор может создавать группу IGMP Snooping при получении отчета IGMP на порту уровня 2 указанного VLAN. Поддерживается настройка статической группы IGMP Snooping с указанием группы IGMP, порта уровня 2 и VLAN.

Шаг 1. Войдите в режим настройки.

```
Switch#configure terminal
```

Шаг 2. Настройка статической группы.

```
Switch(config)# ip igmp snooping vlan 1 static-group 229.1.1.1 interface eth-
0-2
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show ip igmp snooping groups
VLAN    Interface       Group-Address       Uptime      Expires-time
1       eth-0-2         229.1.1.1           00:01:08    stopped
```

6.4 Настройка MVR

6.4.1 Общие положения

6.4.1.1 Описание функции

Регистрация многоадресных VLAN (MVR) предназначена для приложений, использующих широкомасштабное развертывание многоадресного трафика в сети поставщика услуг на основе кольцевой сети Ethernet (например, трансляция нескольких телевизионных каналов по сети поставщика услуг). MVR позволяет клиенту на порту подписываться и отписываться от многоадресного потока в общесетевой многоадресной VLAN. MVR обеспечивает возможность непрерывной отправки многоадресных потоков в многоадресной VLAN, но при этом изолирует потоки от VLAN абонентов по соображениям пропускной способности и безопасности.

Концепция MVR предполагает, что абонентские порты подписываются и отписываются (присоединяются и покидают) многоадресные потоки, отправляя сообщения IGMP join и leave. Эти сообщения могут исходить от хоста, совместимого с IGMP версии 2, с Ethernet-соединением. Хотя

MVR работает на основе механизма IGMP snooping, работа этих двух функций взаимосвязана. Включение или отключение одной из них влияет на поведение другой. Если IGMP snooping и MVR включены, MVR реагирует только на сообщения join и leave от многоадресных групп, настроенных в MVR. ЦП коммутатора идентифицирует многоадресные потоки IP MVR и связанные с ними MAC-адреса в таблице пересылки коммутатора, перехватывает сообщения IGMP и изменяет таблицу пересылки, чтобы включить или удалить абонента из списка получателей многоадресного потока, при этом получатели должны находиться в другой, отличной от источника, VLAN.

6.4.1.2 Основные термины

Терминология	Описание
MVR	Регистрация многоадресной VLAN.
VLAN источника	VLAN для приема многоадресного трафика для MVR.
Порт источника	Порт в исходной VLAN для отправки отчета или запроса на выход в вышестоящую сеть.
Порт приемника	Порт, который не находится в исходной VLAN для приема отчетов или для передачи данных нижестоящим пользователям.

6.4.2 Настройка

Включите IGMP в интерфейсе eth-0-1 коммутатора Switch1.

Настройте коммутатор Switch2: eth-0-1 в vlan111, eth-0-2 в vlan10 и eth-0-3 в vlan30.

При включении MVR на коммутаторе Switch2 требуется, чтобы на коммутатор Switch2 отправлялась только одна копия многоадресного трафика с коммутатора Switch1, но при этом хосты HostA и HostC могут принимать этот многоадресный трафик.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

Настройка на коммутаторе 1:

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 111,10,30
Switch(config-vlan)# quit
```

Шаг 3. Войдите в режим настройки интерфейса, задайте атрибуты и IP-адрес.

Switch1:

```
switch(config)# interface eth-0-1
switch(config-if)# no switchport
```

```
switch(config-if)# no shutdown
switch(config-if)# ip address 12.12.12.12/24
switch(config-if)# exit
```

Switch2:

```
 Switch(config)# interface vlan 111
 Switch(config-if)# exit
 Switch(config)# interface vlan 10
 Switch(config-if)# exit
 Switch(config)# interface vlan 30
 Switch(config-if)# exit
 Switch(config)# interface eth-0-1
 Switch(config-if)# switchport access vlan111
 Switch(config)# interface eth-0-2
 Switch(config-if)# switchport access vlan10
 Switch(config)# interface eth-0-3
 Switch(config-if)# switchport access vlan30
 Switch(config-if)# exit
```

Шаг 4. Включить MVR.

Switch2:

```
Switch(config)# no ip multicast-routing
Switch(config)# mvr
Switch(config)# mvr vlan 111
Switch(config)# mvr group 238.255.0.1 64
Switch(config)# mvr source-address 12.12.12.1
Switch(config)# interface eth-0-1
Switch(config-if)# mvr type source
Switch(config)# interface eth-0-2
Switch(config-if)# mvr type receiver vlan 10
Switch(config)# interface eth-0-3
Switch(config-if)# mvr type receiver vlan 30
Switch(config-if)# exit
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Switch1

```
Switch# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime   Expires  Last Reporter
238.255.0.1      eth-0-1              00:01:16 00:03:49 12.12.12.1
```

```
238.255.0.2       eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.3       eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.4       eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.5       eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.6       eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.7       eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.8       eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.9       eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.10      eth-0-1                00:01:16 00:03:49 12.12.12.1
......
238.255.0.64     eth-0-1               00:01:16 00:03:49 12.12.12.1
```

Switch2

```
Switch# show mvr
MVR Running: TRUE
MVR Multicast VLAN: 111
MVR Source-address: 12.12.12.1
MVR Max Multicast Groups: 1024
MVR Hw Rt Limit: 508
MVR Current Multicast Groups: 255

Switch# show mvr groups
VLAN    Interface       Group-Address       Uptime      Expires-time
10      eth-0-2         238.255.0.1         00:03:23    00:02:03
10      eth-0-2         238.255.0.2         00:02:16    00:02:03
10      eth-0-2         238.255.0.3         00:02:16    00:02:03
10      eth-0-2         238.255.0.4         00:02:16    00:02:03
10      eth-0-2         238.255.0.5         00:02:16    00:02:03
10      eth-0-2         238.255.0.6         00:02:16    00:02:04
10      eth-0-2         238.255.0.7         00:02:16    00:02:04
10      eth-0-2         238.255.0.8         00:02:16    00:02:04
10      eth-0-2         238.255.0.9         00:02:16    00:02:04
10      eth-0-2         238.255.0.10        00:02:16    00:02:04
......
10      eth-0-2         238.255.0.64       00:01:50    00:02:29
```

7 Руководство по настройке безопасности

7.1 Настройка безопасности портов

7.1.1 Общие положения

7.1.1.1 Описание функции

Функция безопасности порта используется для ограничения количества «безопасных» MAC-адресов, изучаемых на конкретном интерфейсе. Интерфейс будет пересылать пакеты только с MAC-адресами источника, которые соответствуют этим безопасным адресам. Безопасные MAC-адреса могут быть созданы вручную или изучены автоматически. После того, как количество безопасных MAC-адресов достигнет предела, новые MAC-адреса не могут быть изучены или настроены на интерфейсе. Если после этого интерфейс получает пакет с MAC-адреса, отличающимся от любого из безопасных адресов, такой пакет будет отброшен.

Поддерживаются два типа безопасных MAC-адресов:

- статические MAC-адреса: они настраиваются вручную с помощью команды конфигурации интерфейса «switchport port-security mac-address»;

- динамические MAC-адреса: они изучаются динамически.

В случае нарушения политик безопасности пересылаемые пакеты будут отброшены. Пользователь может настроить это действие с помощью команды «switchport port-security violation». Доступны три варианта действий:

- errdisable: отбросить пакет и установить для порта статус errdisable. См. руководство по настройке Ethernet, глава errdisable;

- protect: только отбрасывать;

- restrict: отбросить и записать событие в лог.

7.1.2 Настройка

Согласно приведенной выше топологии, после настройки принимаются только три записи MAC-адреса.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса, задайте атрибуты и включите защиту портов.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security mac-address 0000.0201.0101 vlan 1
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# exit
Switch(config)# interface eth-0-2
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# exit
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show port-security
Port Security Work Mode: Hardware

Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolationMode
               (Count)      (DynamicCount)
-------------------------------------------------------------
  eth-0-1           2             2       restrict
  eth-0-2           2             0       protect
Switch#
Switch# show mac address-table
          Mac Address Table
-----------------------------------------
(*)   - Security Entry      (M)   - MLAG Entry
(MO)  - MLAG Output Entry   (MI)  - MLAG Input Entry
(E)   - EVPN Entry          (EO)  - EVPN Output Entry
(EI)  - EVPN Input Entry
Vlan    Mac Address       Type         Ports
----    -----------       --------     -----
1       0000.0201.0103    dynamic(*)   eth-0-1
1       0000.020a.0a0b    static(*)    eth-0-2
1       0000.0201.0102    dynamic(*)   eth-0-1
1       0000.020a.0a0a    static(*)    eth-0-2
1       0000.0201.0101    static(*)    eth-0-1
11      00e0.4c02.172f    dynamic      eth-0-31
Switch#
```

```
Switch#
show port-security address-table
          Secure MAC address table
------------------------------------------------------------
Vlan    Mac Address       Type                Ports
----    -----------       -------             -------
1       0000.0201.0102    SecureLearned       eth-0-1
1       0000.0201.0101    SecureConfigured    eth-0-1
1       0000.020a.0a0b    StickyConfigured    eth-0-2
1       0000.020a.0a0a    StickyConfigured    eth-0-2
1       0000.0201.0103    SecureLearned       eth-0-1
Switch# show running-config interface eth-0-2
Building configuration...
!
interface eth-0-2
 switchport port-security mac-address sticky
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky 0000.020a.0a0a vlan 1
 switchport port-security mac-address sticky 0000.020a.0a0b vlan 1
!
Switch#
```

7.2 Настройка безопасности VLAN

7.2.1 Общие положения

7.2.1.1 Описание функции

Функция безопасности VLAN используется для ограничения общего количества MAC-адресов, изучаемых в конкретной VLAN. MAC-адреса могут добавляться вручную или изучаться автоматически. После того, как устройство достигнет лимита по количеству MAC-адресов, если VLAN получит пакет с неизвестным MAC-адресом источника, будет применено настроенное действие.

Поддерживаются два типа внесения MAC-адресов:

- статические MAC-адреса: они настраиваются пользователями вручную.

- динамические MAC-адреса: они изучаются динамически.

- пользователь может задать действие для пакетов с неизвестным MAC-адресом, используя команду «vlan *X* mac-limit action». Поддерживаются три типа действий:

- отбрасывание: Пакет с неизвестным MAC-адресом из этой VLAN будет отброшен, и MAC-адрес не будет изучен;

- предупреждение: Пакет с неизвестным MAC-адресом из этой VLAN будет отброшен, MAC-адрес не будет изучен, и в системный журнал будет выведено предупреждение;

- пересылка: Пакеты из VLAN будут пересылаться без обучения MAC-адресов и без записи предупреждений в журнал.

Функцию обучения MAC-адресов можно включать или отключать для каждого VLAN отдельно.

7.2.2 Настройка ограничения количества MAC-адресов для VLAN

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN, установите максимальное количество MAC-адресов и действие при превышении этого значения.

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 100
Switch(config-vlan)# vlan 2 mac-limit action discard
Switch(config-vlan)# exit
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show vlan-security
 Vlan  learning-en  max-mac-count  cur-mac-count  action
 ------------------------------------------------------
 2     Enable       100            0              Discard
```

7.2.2.1 Выключение изучения MAC-адресов внутри VLAN

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN, выключите изучение MAC-адресов.

```
Switch(config)# vlan database
Switch(config)# vlan 2
Switch(config-vlan)# vlan 2 mac learning disable
```

```
Switch(config-vlan)# exit
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show vlan-security
 Vlan  learning-en  max-mac-count  cur-mac-count  action
 ------------------------------------------------------
 2     Disable      100            0              Discard
```

7.3 Настройка временного диапазона Time-Range

7.3.1 Общие положения

7.3.1.1 Описание функции

Для реализации функций, основанных на времени, таких как списки контроля доступа (ACL), создается временной диапазон, определяющий конкретные периоды времени. Временной диапазон идентифицируется именем, на которое затем ссылается функция. Временной диапазон зависит от работы системных часов.

7.3.2 Настройка временного диапазона

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте временной диапазон и установите абсолютное время.

```
Switch(config)# time-range test-absolute
Switch(config-tm-range)# absolute start 1:1:2 jan 1 2012 end 1:1:3 jan 7
2012Switch(config-tm-range)# exit
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
DUT1# show time-range
time-range test-absolute
   absolute start 01:01:02 Jan 01 2012 end 01:01:03 Jan 07 2012
```

7.3.2.1 Настройка периодичного временного интервала

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте временной диапазон и установите периодичность по времени.

```
Switch(config)# time-range test-periodic
Switch(config-tm-range)# periodic 1:1 mon to 1:1 wed
Switch(config-tm-range)# exit
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
DUT1# show time-range
time-range test-periodic
   periodic 01:01 Mon to 01:01 Wed
```

7.4 Настройка ACL

7.4.1 Общие положения

7.4.1.1 Описание функции

Списки контроля доступа (ACL) классифицируют трафик по заданным характеристикам. ACL может содержать несколько записей контроля доступа (ACE), которые представляют собой команды, сопоставляющие поля пакета с заданными условиями. ACL могут фильтровать пакеты, полученные на интерфейсе, по м ногим полям, таким как IP-адрес, MAC-адрес.

Сегодня все больше внимания уделяется сетевой безопасности. Списки контроля доступа (ACL) могут обеспечить защиту сетевой безопасности во многих ситуациях, например:

- ограничение доступа к сети. Для обеспечения безопасности сети можно ограничить доступ пользователей к некоторым сервисам, настроив списки контроля доступа (ACL);
- предотвращение проникновения данных вируса во внутреннюю сеть возможно с помощью списков контроля доступа (ACL);
- контроль сетевого доступа пользователя и отслеживание сетевого трафика к контролируемому оборудованию с помощью стратегии ACL;
- применение стратегии ACL для перенаправления потока данных в инструменты межсетевого экрана и на указанный порт, для последующей проверки безопасности.

7.4.1.2 Основные термины

Запись контроля доступа (ACE): Каждая запись ACE включает действие (разрешить или запретить) и ряд фильтров, основанных на таких критериях, как адрес источника, адрес назначения, протокол и параметры, специфичные для протокола.

MAC ACL: MAC ACL позволяет фильтровать пакеты по полям mac-sa и mac-da, при этом MAC-адрес может быть замаскирован, настроен как идентификатор хоста или как любой другой для фильтрации всех MAC-адресов. MAC ACL также может фильтровать другие поля уровня L2, такие как COS, VLAN-ID, INNER-COS, INNER-VLAN-ID, тип L2, тип L3.

ACL для IPv4: ACL для IPv4 позволяет фильтровать пакеты по полям ip-sa и ip-da, при этом IP-адрес может быть замаскирован, настроен как идентификатор хоста или как любой другой параметр для фильтрации всех IPv4-адресов. ACL для IPv4 также может фильтровать другие поля уровня L3, такие как DSCP, протокол уровня L4 и такие поля уровня L4, как TCP-порт, UDP-порт и т. д.

Временной диапазон: Временной диапазон может определять период времени, в течение которого ACE действует.

7.4.1.3 Описание работы правила ACL

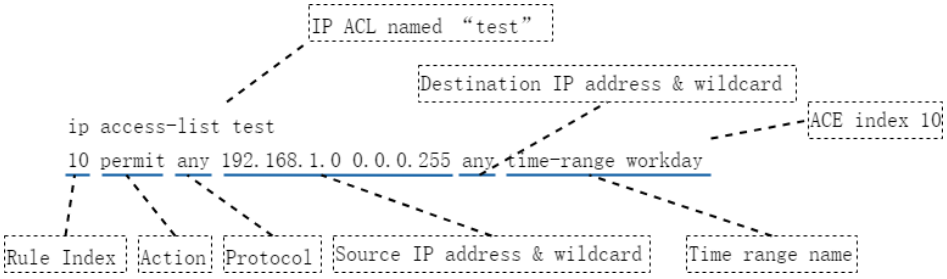


Рисунок 34 – Описание правил ACL

- [Название ACL] используется для различия между ACL;
- [ACE] — «Запись контроля доступа». Один ACL включает одну или несколько записей контроля доступа (ACE);
- [Идентификатор правила] Идентификатор правила выполняет две функции. Первая функция идентификатора правила — пометка записей ACE. Пользователи могут удалять записи ACE с указанным идентификатором правила. Вторая функция идентификатора правила — определение приоритета каждой записи ACE. Допустимый диапазон значений идентификатора правила — 1-131071; записи ACE с меньшим номером имеют более высокий приоритет и совпадают первыми;
- [Действие] включает в себя разрешения и запреты, указывает на то, разрешать или запрещать прохождение соответствующих кадров;

- [Поле] ACL предоставляет чрезвычайно большое количество полей для сопоставления, такие как информация заголовка кадра Ethernet (например, MAC-адрес источника, MAC-адрес назначения, тип Ethernet, VLAN), DSCP, TTL, номер порта TCP/UDP, флаги TCP и так далее.

7.4.1.4 Срабатывание правил

Два режима сработки для ACL: совпадение любого из условий и совпадение всех условий. Режим настраивается администратором.

Для кадров, не соответствующих критериям ACL, действие по умолчанию - прохождение кадров.

Кадры, перенаправляемые с одного и того же входящего устройства, не могут соответствовать списку контроля доступа (ACL) на исходящем канале этого же устройства.

Режим «совпадение всем» требует, чтобы кадры соответствовали всем записям ACE, поэтому записи ACE в списке ACL не допускают конфликтующих полей.

7.4.1.5 ACL анализируемые поля

ACL поддерживает очень большое количество полей для анализа, ниже приведены лишь некоторые из полей, которые используются наиболее часто:

IP-адрес источника/назначения и его маска подсети

В ACL используются три формата для сопоставления IP-адресов:

- любой: соответствует всем IP-адресам;
- host: соответствует только одному IP-адресу, нет необходимости настраивать маску подсети;
- A.B.C.D.: IP-адрес в заданном диапазоне; необходимо настроить маску подсети.

Пример: если вы хотите, чтобы все IP-адреса из сети 192.168.1.0/24 проходили, это можно настроить следующим образом:

```
permit any 192.168.1.0 0.0.0.255 any
```

Таблица 8 – Описания параметров ACL

Парамметр	Значение	Двоичный вид
Справочный адрес	192.168.1.0	11000000.10101000.00000001.00000000
Маска	0.0.0.255	00000000.00000000.00000000.11111111
Диапазон адресов	IP-адрес в диапазоне от 192.164.1.0 до 192.168.1.255	11000000.10101000.00000001.XXXXXXXX X может быть «0» или «1»

MAC-адрес источника/назначения и маска подстановки

MAC-адрес источника/назначения в ACL аналогичен IP-адресу, разница заключается в том, что MAC-адрес использует шестнадцатеричный формат и имеет 48 бит, а IP-адрес — десятичный формат и имеет 32 бита. Для получения информации о способах применения, пожалуйста, ознакомьтесь с инструкцией «IP-адрес источника/назначения и его маска подсети».

Тип IP-протокола.

В списках контроля доступа (ACL) существует три типа форматирования типов IP-протоколов:

- любой: соответствует всем типам IP-протоколов;
- номер IP-протокола: значение параметра, определяющего тип IP-протокола, заданное пользователем; диапазон значений должен быть от 0 до 255;
- Gre|icmp|igml|nvgre|tcp|udp: это некоторые часто используемые протоколы, которые поддерживает система.

Часто используемые типы протоколов, включая: ICMP (протокол 1), TCP (протокол 6), UDP (протокол 17), GRE (протокол 47), IGMP (протокол 2), IPinIP (протокол 4), OSPF (протокол 89).

Номер порта TCP/UDP.

Формат номера исходного порта: **src-port** { **eq** port | **gt** port | **lt** port | **range** port-start port-end}

Формат номера порта назначения: **dst-port** { **eq** port | **gt** port | **lt** port | **range** port-start port-end}

- eq port: значение, равное номеру порта источника или назначения;
- gt port: значение больше, чем номер порта в источнике или пункте назначения;
- lt port: значение меньше, чем номер порта в источнике или назначения.

Параметр `range port-start port-end`: задает диапазон номеров портов. `Port-start` — это начальное значение диапазона, `Port-end` — это конечное значение диапазона.

Таблица 9 – Соответствие TCP портов типам протоколов

Номер порта	Протокол	Пояснение
7	Echo	Эхо-протокол (RFC 862)
13	Daytime	Дата и время
19	Character generator	Сервис генерации символов; отправка неограниченного количества символов.
20	FTP-соединения для передачи данных	Порт данных FTP
21	Протокол передачи файлов (FTP)	Порт протокола передачи файлов (FTP)
23	Telnet	Telnet-сервис
25	Simple Mail Transport Protocol (SMTP)	Протокол SMTP

Номер порта	Протокол	Пояснение
37	Time	Временной протокол
43	Nickname（WHOIS）	Меню обслуживания
49	TAC Access Control System (TACACS)	Система доступа, используемая для тестирования и контроля, основана на протоколе TCP/IP (TACACS — протокол доступа хоста).
53	Служба доменных имен (DNS)	Служба доменных имен
80	World Wide Web (HTTP)	Протокол передачи гипертекста (HTTP). Применяется для просмотра веб-страниц.
101	NIC hostname server	Служба имен сетевой карты
109	Post Office Protocol v2	Пост протокол версии 2
110	Post Office Protocol v3	Пост протокол версии 3
111	Sun Remote Procedure Call (RPC)	Протокол удаленного вызова процедур (DPR) от компании SUN Inc.
119	Network News Transport Protocol (NNTP)	Протокол передачи сетевых новостей, сеть USENET
179	Border Gateway Protocol (BGP)	Протокол пограничного шлюза, маршрутизация
194	Internet Relay Chat (IRC)	протокол многоадресной рассылки IRC
512	Exec (rsh)	Используется для проверки хода выполнения удаленного запроса.
513	Login (rlogin)	Удаленный вход
514	Remote commands	Удаленные команды, не требующие входа в удаленную оболочку и удаленного копирования.
515	Printer service	Принтер
517	Talk	удаленная коммуникационная услуга для клиентов
540	Unix-to-Unix Copy Program	Служба копирования из Unix в Unix
543	Kerberos login	Kerberos версии 5 для удаленного входа в систему.
544	Kerberos shell	Kerberos версии 5 для удалённой программной оболочки

Таблица 10 – Соответствие UPD портов типам протоколов

Номер порта	Протокол	Пояснение
7	Echo	Эхо-служба

Номер порта	Протокол	Пояснение
9	Discard	Пустой сервис, используемый для тестирования подключения.
37	Time	Временной протокол
42	Host Name Server	служба имен хостов
53	Domain Name Service (DNS)	служба доменных имен
65	TACACS-Database Service	Сервис базы данных TACACS
67	Bootstrap Protocol Server	На стороне сервера используется протокол Bootstrap, а также DHCP-сервер.
68	Bootstrap Protocol Client	На стороне клиента используется протокол начальной загрузки (Bootstrap), а также DHCP-клиент.
69	Trivial File Transfer Protocol (TFTP)	Простой протокол передачи файлов
90	DNSIX Security Attribute Token Map	Атрибуты безопасности DNSIX
111	SUN Remote Procedure Call (SUN RPC)	Протокол удаленного вызова процедур (DPR) от компании SUN Inc
123	Network Time Protocol (NTP)	Протокол сетевого времени.
137	NETBIOS Name Service	Служба имен NETBIOS
138	NETBIOS Datagram Service	Служба датаграмм NETBIOS
139	NETBIOS Session Service	Служба сеансов связи NETBIOS
161	SNMP	Протокол управления сетью
162	SNMPTRAP	Протокол управления сетью
434	MobileIP-Agent	Агент мобильного IP
435	MobileIP-MN	Управление мобильными IP-адресами
512	Mail notify	Уведомление по электронной почте, оповещение пользователей о получении электронного письма.
513	Who	Список авторизованных пользователей
514	Syslog	Системный лог и жунал
517	Talk	Удалённая связь между сервером и клиентом.
520	Routing Information Protocol	Протокол маршрутизатора RIP

Условия совпадения условий для TCP

- режим «совпадение по любому параметру»: match-any { ack | fin | psh | rst | syn | urg } После «match-any» можно одновременно настроить несколько параметров для TCP, но если совпадение произойдет хотя бы с одним из них, то правило сработает;

- режим «Совпадение всех»: match-all { ack | fin | psh | rst | syn | urg };

- после выбора параметра «match-all» можно одновременно настроить несколько параметров идентификации P, и для успешного сопоставления кадры должны соответствовать всем этим параметрам.

7.4.2 Настройка

7.4.2.1 Базовая фильтрация MAC/IP-адресов

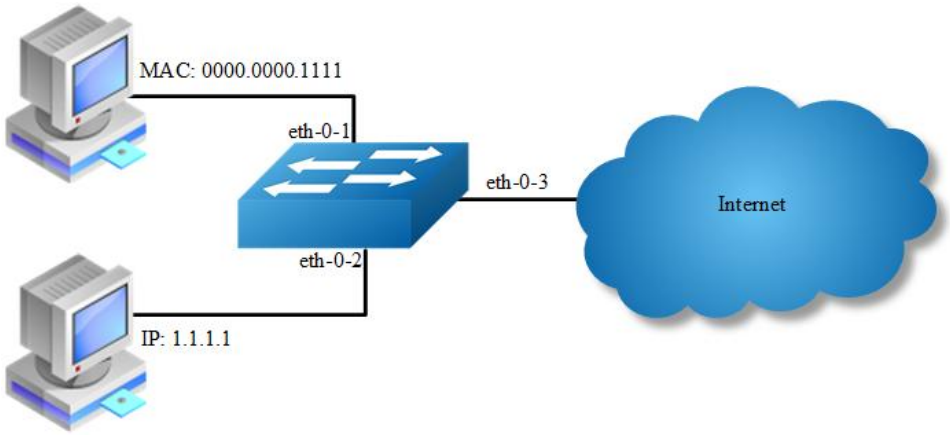


Рисунок 1-3 ACL

В этом примере используйте MAC ACL на интерфейсе eth-0-1, чтобы разрешить пакеты с MAC-адресом источника 0000.0000.1111 и запретить все остальные пакеты. Используйте IPv4 ACL на интерфейсе eth-0-2, чтобы разрешить пакеты с IP-адресом источника 1.1.1.1/24 и запретить все остальные пакеты.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте список доступа.

Список доступа по Mac:

```
Switch(config)# mac access-list mac
Switch(config-mac-acl)# permit src-mac host 0000.0000.1111 dest-mac any
Switch(config-mac-acl)# deny src-mac any dest-mac any
```

```
Switch(config-mac-acl)# exit
```

Список доступа по IP-адресам:

```
Switch(config)# ip access-list ipv4
Switch(config-ip-acl)# permit any 1.1.1.1 0.0.0.255 any
Switch(config-ip-acl)# deny any any any
Switch(config-ip-acl)# exit
```

Шаг 3. Создайте class-map и привяжите список доступа.

```
Switch(config)# class-map cmap1
Switch(config-cmap)# match access-group mac
Switch(config-cmap)# exit

Switch(config)# class-map cmap2
Switch(config-cmap)# match access-group ipv4
Switch(config-cmap)# exit
```

Шаг 4. Создайте policy-map и привяжите class-map.

```
Switch(config)# policy-map pmap1
Switch(config-pmap)# class cmap1

Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch(config)# policy-map pmap2
Switch(config-pmap)# class cmap2
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

Шаг 5. Примените политику к интерфейсу.

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy input pmap1
Switch(config-if)# exit

Switch(config-if)# interface eth-0-2
Switch(config-if)# service-policy input pmap2
Switch(config-if)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Результат выполнения команды «show running-config» выглядит следующим образом:

```
Switch# show running-config
mac access-list mac
  10 permit src-mac host 0000.0000.1111 dest-mac any
  20 deny src-mac any dest-mac any
!
ip access-list ipv4
  10 permit any 1.1.1.0 0.0.0.255 any
  20 deny any any any
!
class-map match-any cmap1
 match access-group mac
!
class-map match-any cmap2
 match access-group ipv4
!
policy-map pmap1
 class cmap1
!
policy-map pmap2
 class cmap2
!
interface eth-0-1
 service-policy input pmap1
!
interface eth-0-2
 service-policy input pmap2
!
```

7.4.2.2 Контроль доступа с заданным временным диапазоном

7.4.2.3 Топология

7.4.2.4 Требования к конфигурации

Сотрудники отдела исследований НЕ могут получить доступ к серверу запросов по заработной плате (IP-адрес 192.168.10.10) в рабочее время (с 9:00 до 18:00). Доступ есть от офиса CEO.

7.4.2.5 Этапы настройки

Шаг 1. Создайте VLAN 10, 20 и 30.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10,20,30
Switch(config-vlan)# exit
```

Шаг 2. Настройте порты 1-3 как транковые порты и подключите их к VLAN 10, 20 и 30.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10
Switch(config-if)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# interface eth-0-3
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 30
```

Шаг 3. Настройка IP-адреса для интерфейсов VLAN.

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.1.254/24
Switch(config-if)# interface vlan 20
Switch(config-if)# ip address 192.168.2.254/24
Switch(config-if)# interface vlan 30
Switch(config-if)# ip address 192.168.3.254/24
```

Шаг 4. Настройте порт 4 как switchport и задайте IP-адрес.

```
Switch(config-if)# interface eth-0-4
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.10.254/24
Switch(config-if)# exit
```

Шаг 5. Настройте временной диапазон с понедельника по пятницу, с 9:00 до 18:00, с периодическим интервалом.

```
Switch(config)# time-range time-1
Switch(config-tm-range)# periodic 09:00 weekdays to 18:00
```

Шаг 6. Настройте ACE для доступа отдела исследований и разработок к серверу запросов по заработной плате.

```
Switch(config)# ip access-list test
Switch(config-ip-acl)# deny any 192.168.1.0 0.0.0.255 host 192.168.10.10
time-range time-1
```

Шаг 7. Настройте ACE для доступа административного отдела к серверу запросов заработной платы.

```
Switch(config)# ip access-list test
Switch(config-ip-acl)# deny any 192.168.2.0 0.0.0.255 host 192.168.10.10
time-range time-1
```

Шаг 8. Создайте карту классов и привяжите ACL.

```
Switch(config)# class-map match-any cmap
Switch(config-cmap)# match access-group test
```

Шаг 9: Создайте tpolicy-map и привяжите к нему class-map. Включите функцию статистики для этого class-map.

```
Switch(config)# policy-map pmap
Switch(config-pmap)# class cmap
Switch(config-pmap-c)# statistics enable
```

Шаг 10. Примените карту политик к интерфейсу.

Отдел исследований и разработок будет получать доступ к серверу через интерфейс eth-0-1, поэтому следует применить ограничение трафика на eth-0-1 при входящем трафике..

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy input pmap
Switch(config)# interface eth-0-2
Switch(config-if)# service-policy input pmap
```

Шаг 11. Проверка.

Отобразить информацию о конфигурации ACL

```
Switch# show access-list ip
ip access-list test
  10 deny any 192.168.1.0 0.0.0.255 host 192.168.10.10 time-range time-1
  20 deny any 192.168.2.0 0.0.0.255 host 192.168.10.10 time-range time-1
```

Отображение информации о конфигурации class-map

```
Switch# show class-map
    CLASS-MAP-NAME: class-default (match-any)
    CLASS-MAP-NAME: cmap (match-any)
           match access-group: test
```

Отображение конфигурации policy-map

```
Switch# show policy-map
  POLICY-MAP-NAME: pmap
```

```
    State: attached
    CLASS-MAP-NAME: cmap
      match access-group: test
          statistics  : enable
```

Отобразить статистическую информацию о совпадениях по ACE.

```
Switch# show policy-map statistics interface eth-0-1 input ace-based
 Interface: eth-0-1
 Ingress service policy: pmap

Class name: cmap, operator : match-any
 access-group test
  10 deny any 192.168.1.0 0.0.0.255 host 192.168.10.10 time-range time-1 ( 0
match 0 bytes)
  20 deny any 192.168.2.0 0.0.0.255 host 192.168.10.10 time-range time-1 ( 0
match 0 bytes)
total 0 match 0 bytes
```

7.4.2.6 Конфигурация ACL коммутатора

```
vlan database
 vlan 10,20,30
   periodic 09:00 weekdays to 18:00
!
ip access-list test
  10 deny any 192.168.1.0 0.0.0.255 host 192.168.10.10 time-range time-1
  20 deny any 192.168.2.0 0.0.0.255 host 192.168.10.10 time-range time-1
!
class-map match-any cmap
 match access-group test
!
policy-map pmap
 class cmap
  statistics enable
!
interface eth-0-1
 switchport mode trunk
 switchport trunk allowed vlan add 10
 service-policy input pmap
!
time-range time-1
interface eth-0-2
 switchport mode trunk
 switchport trunk allowed vlan add 20
 service-policy input pmap
!
interface eth-0-3
 switchport mode trunk
```

```
 switchport trunk allowed vlan add 30
!
interface eth-0-4
 no switchport
 ip address 192.168.10.254/24
!
interface vlan10
ip address 192.168.1.254/24
!
interface vlan20
ip address 192.168.2.254/24
!
interface vlan30
ip address 192.168.3.254/24
!
```

7.4.2.7 Ограничьте доступ пользователей из разных VLAN друг к другу с помощью ACL.

7.4.2.8 Требование к конфигурации

Администратор сети разделяет отделы на разные VLAN, а разные VLAN — на разные IP-сегменты сети. Чтобы предотвратить разглашение секретной информации компании между отделами, ему предлагается запретить доступ к сети для разных отделов через коммутаторы, то есть запретить сетевое взаимодействие между различными VLAN.

7.4.2.9 Этапы настройки

Шаг 1. Создайте VLAN 10, 20 и 30.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10,20,30
Switch(config-vlan)# exit
```

Шаг 2. Настройте порты 1-3 как транковые интерфейсы и подключите их к VLAN 10, 20 и 30.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10
Switch(config-if)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# interface eth-0-3
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 30
```

Шаг 3. Настройка IP-адреса интерфейса VLAN.

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.1.254/24
Switch(config-if)# interface vlan 20
Switch(config-if)# ip address 192.168.2.254/24
Switch(config-if)# interface vlan 30
Switch(config-if)# ip address 192.168.3.254/24
```

Шаг 4: создайте список контроля доступа (ACL) «for-rd», чтобы запретить трафик из отдела исследований в административный/финансовый отдел.

```
Switch(config)# ip access-list for-rd
Switch(config-ip-acl)# deny any 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Switch(config-ip-acl)# deny any 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Шаг 5. Создайте список контроля доступа (ACL) «для административного отдела», чтобы запретить трафик из административного отдела в отдел исследований /финансовый отдел.

```
Switch(config)# ip access-list for-administrative
Switch(config-ip-acl)# deny any 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Switch(config-ip-acl)# deny any 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Шаг 6: создайте список контроля доступа (ACL) «для финансового отдела», чтобы запретить трафик из финансового отдела в отдел исследований /административный отдел.

```
Switch(config)# ip access-list for-finance
Switch(config-ip-acl)# deny any 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
Switch(config-ip-acl)# deny any 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Шаг 7. Создайте классификацию трафика «cmap-rd» и примените к ней параметр «for-rd».

```
Switch(config)# class-map match-any cmap-rd
Switch(config-cmap)# match access-group for-rd
```

Шаг 8. Создайте классификацию «camp-administrative» и примените к ней классификацию «for-administrative».

```
Switch(config)# class-map match-any cmap-administrative
Switch(config-cmap)# match access-group for-administrative
```

Шаг 9. Создайте "cmap-finance", примените "for-finance" к этой классификации трафика.

```
Switch(config)# class-map match-any cmap-finance
Switch(config-cmap)# match access-group for-finance
```

Шаг 10: создайте policy-map «pmap-rd», примените к ней «cmap-rd» и включите функцию статистики ACL.

```
Switch(config)# policy-map pmap-rd
Switch(config-pmap)# class cmap-rd
Switch(config-pmap-c)# statistics enable
```

Шаг 11. Создайте policy-map «pmap-administrative», примените к ней «cmap-administrative» и включите функцию статистики ACL.

```
Switch(config)# policy-map pmap-administrative
Switch(config-pmap)# class cmap-administrative
Switch(config-pmap-c)# statistics enable
```

Шаг 12: создайте policy-map «pmap-finance», примените «cmap-finance» к этой карте политик и включите функцию статистики ACL.

```
Switch(config)# policy-map pmap-finance
Switch(config-pmap)# class cmap-finance
Switch(config-pmap-c)# statistics enable
```

Шаг 13. Применить policy-map: команда `pmap-rd` к VLAN 10 (отдел исследований и разработок).

```
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input pmap-rd
```

Шаг 14. Применить policy-map: `traffic policy-map “pmap-administrative”` к VLAN 20 (административный отдел).

```
Switch(config)# interface vlan 20
Switch(config-if)# service-policy input pmap-administration
```

Шаг 15. Применить policy-map: команда `pmap-finance` к VLAN 30 (финансовый отдел).

```
Switch(config)# interface vlan 30
Switch(config-if)# service-policy input pmap-finance
```

7.4.2.10 Шаг 16. Проверка.

Отображение информации о конфигурации ACL

```
Switch# show access-list ip
ip access-list for-rd
  10 deny any 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
  20 deny any 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
ip access-list for-administrative
  30 deny any 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
  40 deny any 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
ip access-list for-finance
  30 deny any 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
      40 deny any 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Отображение конфигурации классификации трафика

```
Switch# show class-map
    CLASS-MAP-NAME: class-default (match-any)
    CLASS-MAP-NAME: cmap-rd (match-any)
       match access-group: for-rd
    CLASS-MAP-NAME: cmap-administrative (match-any)
       match access-group: for-administrative
    CLASS-MAP-NAME: cmap-finance (match-any)
           match access-group: for-finance
```

Отображение конфигурации политик для трафика

```
Switch# show policy-map
  POLICY-MAP-NAME: pmap-rd
    State: attached
    CLASS-MAP-NAME: cmap-rd
      match access-group: for-rd
        statistics   : enable
  POLICY-MAP-NAME: pmap-administrative
    State: attached
    CLASS-MAP-NAME: cmap-administrative
      match access-group: for-administrative
        statistics   : enable
  POLICY-MAP-NAME: pmap-finance
    State: attached
    CLASS-MAP-NAME: cmap-finance
      match access-group: for-finance
        statistics   : enable
```

7.4.2.11 Конфигурация ACL коммутатора

```
vlan database
 vlan 10,20,30
!
ip access-list for-rd
```

```
  10 deny any 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
  20 deny any 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
ip access-list for-administrative
  10 deny any 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
  20 deny any 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
ip access-list for-finance
  10 deny any 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
  20 deny any 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
!
class-map match-any cmap-rd
 match access-group for-rd
!
class-map match-any cmap-administrative
 match access-group for-administrative
!
class-map match-any cmap-finance
 match access-group for-finance
!
policy-map pmap-rd
 class cmap-rd
statistics enable
!
policy-map pmap-administrative
 class cmap-administrative
  statistics enable
!
policy-map pmap-finance
 class cmap-finance
  statistics enable
!
interface eth-0-1
 switchport mode trunk
 switchport trunk allowed vlan add 10
!
interface eth-0-2
 switchport mode trunk
 switchport trunk allowed vlan add 20
!
interface eth-0-3
 switchport mode trunk
 switchport trunk allowed vlan add 30
!
interface eth-0-4
 no switchport
 ip address 192.168.10.254/24
!
interface vlan10
 service-policy input pmap-rd
```

```
 ip address 192.168.1.254/24
!
interface vlan20
 service-policy input pmap-administrative
 ip address 192.168.2.254/24
!
interface vlan30
 service-policy input pmap-finance
 ip address 192.168.3.254/24
```

NOTE

- применение ACL к интерфейсу VLAN позволяет включить все физические интерфейсы в этой VLAN, это справедливо только для пакетов, пересылаемых на уровне 3;

- применение ACL к VLAN позволяет активировать все физические интерфейсы в этой VLAN и действует как для пакетов уровня 2, так и для пакетов уровня 3;

- пример конфигурации в этом разделе показывает различные списки контроля доступа (ACL), которые будут применяться к разным class-map и policy-map. Такая конфигурация позволяет сэкономить ресурсы ACL. Если экономия ресурсов ACL не важна, можно объединить все списки контроля доступа в одну class-map и policy-map для упрощения конфигурации.

7.4.2.12 Перенаправление потока при помощи ACL

7.4.2.13 Требования к конфигурации

Администратору сети необходимо направлять трафик из ненадежных сетей к защищенным серверам через межсетевые экраны; после завершения фильтрации межсетевые экраны отправят трафик обратно на коммутатор.

7.4.2.14 Этапы настройки

Шаг 1: Создайте VLAN 10 и 20.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10,20
```

Шаг 2. Настройте порты 1/2/3 как транковые порты и подключите их к соответствующему VLAN.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10
Switch(config-if)# ex
Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10
Switch(config-if)# ex
```

```
Switch(config)# interface eth-0-3
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
```

Шаг 3. Настройка IP-адреса VLAN.

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.1.254/24
Switch(config-if)# exit
Switch(config)# interface vlan 20
Switch(config-if)# ip address 192.168.2.254/24
```

Шаг 4. Создайте список контроля доступа (ACL) для сопоставления трафика из не доверенных сетей с защищаемым сервером.

```
Switch(config)# ip access-list test
Switch(config-ip-acl)# permit any any host 192.168.2.100
```

Шаг 5. Создайте class-map и привяжите ACL.

```
Switch(config)# class-map cmap
Switch(config-cmap)# match access-group test
```

Шаг 6. Создайте policy-map и привяжите class-map, включите функцию статистики и функцию перенаправления.

```
Switch(config)# policy-map pmap
Switch(config-pmap)# class cmap
Switch(config-pmap-c)# statistics enable
Switch(config-pmap-c)# redirect to interface eth-0-2
```

Шаг 7. Отключите функцию обучения MAC-адресов интерфейса eth-0-2.

```
Switch(config)# interface eth-0-2
Switch(config-if)# mac learning disable
```

Шаг 8. Примените карту политик к интерфейсу.

```
Switch(config)#interface eth-0-1
Switch(config-if) service-policy input pmap
```

7.4.2.15 Шаг 9. Проверка.

Проверьте информацию о конфигурации правил ACL и настроек классификации трафика

```
Switch# show access-list ip
ip access-list test
  10 permit any any host 192.168.2.100
Switch# show class-map
    CLASS-MAP-NAME: class-default (match-any)
    CLASS-MAP-NAME: cmap (match-any)
      match access-group: test
```

Отображение конфигурации политик для трафика

```
Switch# show policy-map
  POLICY-MAP-NAME: pmap
    State: detached
    CLASS-MAP-NAME: cmap
      match access-group: test
        statistics  : enable
        redirect    : interface eth-0-2
```

7.4.2.16 Конфигурация ACL коммутатора

```
vlan database
 vlan 10,20
!
ip access-list test
  10 permit any any host 192.168.2.100
!
class-map match-any cmap
 match access-group test
!
policy-map pmap
 class cmap
  statistics enable
  redirect to interface eth-0-2
!
interface eth-0-1
 switchport mode trunk
 switchport trunk allowed vlan add 10
 service-policy input pmap
!
interface eth-0-2
 switchport mode trunk
 switchport trunk allowed vlan add 10
 mac learning disable
!
interface eth-0-3
 switchport mode trunk
 switchport trunk allowed vlan add 20
!
interface vlan10
```

```
 ip address 192.168.1.254/24
!
interface vlan20
 ip address 192.168.2.254/24
```

NOTE

Поскольку межсетевой экран отправит сообщение обратно на коммутатор после его обработки, если интерфейс eth-0-2 не закроет функцию обучения MAC-адресов, это приведет к запоминанию одного и того же MAC-адреса для eth-0-1 и eth-0-2, что вызовет нестабильность; и сообщения, на которые отвечает сервер, не смогут корректно достичь порта eth-0-1. Поэтому необходимо закрыть функцию обучения MAC-адресов интерфейса eth-0-2.

Для включения функции мониторинга на основе списков контроля доступа (ACL) обратитесь к приведенным выше примерам конфигурации.

7.5 Настройка расширенного ACL

7.5.1 Общие положения

7.5.1.1 Описание Функции

Расширенный список контроля доступа IPv4 (Extended IPv4 ACL) объединяет MAC-фильтры с IP-фильтрами в одном списке доступа. В отличие от MAC- и IP-ACL, расширенный список контроля доступа может контролировать доступ ко всем пакетам (IP-пакетам и пакетам, не являющимся IP). Поддерживается расширенный список контроля доступа IPv4.

Ниже приведено краткое описание терминов и понятий, используемых для описания расширения ACL:

- расширение списка контроля доступа IPv4: Расширение списка контроля доступа IPv4 использует преимущества списков контроля доступа MAC и IPv4, объединяя их в одном списке контроля доступа для обеспечения более мощной функции контроля;
- MAC ACE: Фильтрация пакетов по MAC-SA и MAC-DA, при этом MAC-адрес может быть замаскирован, настроен как идентификатор хоста или как любой другой параметр для фильтрации всех MAC-адресов. Другие поля уровня L2, такие как COS, VLAN-ID, INNER-COS, INNER-VLAN-ID, тип L2, тип L3, также могут фильтроваться с помощью MAC ACE;
- IPv4 ACE: Фильтрация пакетов по IP-SA и IP-DA, при этом IP-адрес может быть замаскирован, настроен как идентификатор хоста или как любой другой параметр для фильтрации всех IPv4-адресов. Другие поля уровня L3, такие как DSCP, протокол уровня L4 и поля уровня L4, такие как TCP-порт, UDP-порт, также могут быть отфильтрованы с помощью IPv4 ACE.

Значения MAC ACE и IPv4 ACE в расширенном списке контроля доступа IPv4 могут быть настроены попеременно в произвольном порядке, который полностью определяется пользователем.

7.5.2 Настройка

В этом примере используйте расширенный список контроля доступа IPv4 на интерфейсе eth-0-1, чтобы разрешить пакеты с MAC-адресом источника 0000.0000.1111 и значением COS, равным 2, разрешить все пакеты TCP и запретить любые другие пакеты.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте список доступа.

```
Switch(config)# ip access-list ipxacl extend
Switch(config-ex-ip-acl)# permit src-mac host 0000.0000.1111 dest-mac any cos
2
Switch(config-ex-ip-acl)# permit tcp any any
Switch(config-ex-ip-acl)# deny src-mac any dest-mac any
Switch(config-ex-ip-acl)# end
```

Шаг 3. Создайте class-map и привяжите список доступа.

```
Switch(config)# class-map cmap
Switch(config-cmap)# match access-group ipxacl
Switch(config-cmap)# exit
```

Шаг 4. Создайте карту политик и привяжите class-map.

```
Switch(config)# policy-map pmap
Switch(config-pmap)# class cmap
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

Шаг 5. Примените политику к интерфейсу.

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy input pmap
Switch(config-if)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Результат выполнения команды «show running-config» выглядит следующим образом:

```
Switch# show running-config
ip access-list ipxacl extend
  10 permit src-mac host 0000.0000.1111 dest-mac any cos 2
  20 permit tcp any any
  30 deny src-mac any dest-mac any
!
class-map match-any cmap
 match access-group ipxacl
!
policy-map pmap
 class cmap
!
interface eth-0-1
 service-policy input pmap
!
Switch# show access-list ip
ip access-list ipxacl extend
  10 permit src-mac host 0000.0000.1111 dest-mac any cos 2
  20 permit tcp any any
  30 deny src-mac any dest-mac any
```

7.6 Настройка группы портов

7.6.1 Общие положения

7.6.1.1 Описание Функции

Функция Port-group предназначена для создания группы портов на основе правил ACL. В группу портов можно добавить несколько интерфейсов, поддерживаются как физические, так и агрегированные интерфейсы. Когда пользователь применяет политику ACL к группе портов, действие ACL имеет агрегированный эффект.

7.6.2 Настройка

7.6.2.1 Создайте группу портов

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте группу портов и добавьте в нее входящие в нее интерфейсы.

```
Switch(config)# port-group port_group_1
Switch(config-port-group)# member interface eth-0-1
Switch(config-port-group)# member interface agg 1
Switch(config-port-group)# exit
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
DUT1# show running-config port-group
port-group port_group_1
   member interface eth-0-1
   member interface agg1
```

7.7 Настройка группы VLAN

7.7.1 Общие положения

7.7.1.1 Описание Функции

Функция VLAN-group предназначена для создания группы VLAN на основе правил ACL. В группу VLAN можно добавить несколько VLAN. Когда пользователь применяет политику ACL к группе VLAN, действие ACL имеет совокупный эффект.

7.7.2 Настройка

Создайте группу VLAN

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте группу VLAN и добавьте в нее входящие в нее VLAN.

```
Switch(config)# vlan-group vlan_group_1
Switch(config-vlan-group)# member vlan 10
Switch(config-vlan-group)# member vlan 20
Switch(config-vlan-group)# exit
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
DUT1# show running-config vlan-group
vlan-group vlan_group_1
```

```
member vlan 10
member vlan 20
```

7.8 Настройка dot1x

7.8.1 Общие положения

7.8.1.1 Описание Функции

Локальные сети IEEE 802 часто развертываются в средах, допускающих физическое подключение неавторизованных устройств к инфраструктуре локальной сети или позволяющих неавторизованным пользователям пытаться получить доступ к локальной сети через уже подключенное оборудование.

Управление доступом к сети на основе портов обеспечивает аутентификацию и авторизацию устройств, подключенных к локальным портам, и предотвращает доступ к порту в случаях, когда процесс аутентификации и авторизации завершается неудачей.

При использовании аутентификации на основе портов 802.1X устройства в сети выполняют определенные роли:

- Клиент: устройство (ПК), которое запрашивает доступ к локальной сети и услугам коммутатора и отвечает на запросы от коммутатора. На ПК должно работать клиентское программное обеспечение, поддерживающее стандарт 802.1X. Для систем Linux мы рекомендуем приложение под названием «xsupplicant»;
- Сервер аутентификации: выполняет фактическую аутентификацию клиента. Сервер аутентификации проверяет личность клиента и уведомляет коммутатор о том, имеет ли клиент право доступа к локальной сети и услугам коммутатора. Поскольку коммутатор выступает в роли прокси-сервера, служба аутентификации прозрачна для клиента. В этой версии единственным поддерживаемым сервером аутентификации является система безопасности Remote Authentication Dial-In User Service (RADIUS) с расширениями Extensible Authentication Protocol (EAP). RADIUS работает в модели клиент/сервер, в которой защищенная информация для аутентификации обменивается между сервером RADIUS и одним или несколькими клиентами RADIUS;
- Коммутатор (граничный коммутатор или беспроводная точка доступа): управляет физическим доступом к сети на основе статуса аутентификации клиента. Коммутатор выступает в качестве посредника (прокси) между клиентом и сервером аутентификации, запрашивая у клиента информацию об идентификации, проверяя эту информацию с сервером аутентификации и передавая ответ клиенту. Коммутатор включает в себя RADIUS-клиент, который отвечает за инкапсуляцию и декапсуляцию кадров EAP и взаимодействие с сервером аутентификации. Когда коммутатор получает кадры EAPOL и передает их на сервер аутентификации, заголовок Ethernet удаляется, а оставшийся кадр EAP повторно инкапсулируется в формате RADIUS. Кадры EAP не

изменяются и не проверяются во время инкапсуляции, и сервер аутентификации должен поддерживать EAP в собственном формате кадра. Когда коммутатор получает кадры от сервера аутентификации, заголовок кадра сервера удаляется, остается кадр EAP, который затем инкапсулируется в Ethernet и отправляется клиенту. Поддерживается включение dot1x на маршрутизируемом порту и порту доступа.

7.8.2 Настройка

7.8.2.1 Базовая конфигурация dot1x

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите dot1x глобально.

```
Switch(config)# dot1x system-auth-ctrl
```

Шаг 3. Войдите в режим настройки интерфейса, задайте атрибуты интерфейса и включите dot1x.

```
Switch(config)# interface eth-0-25
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.100.1/24
Switch(config-if)# exit
```

Шаг 4. Задайте атрибуты интерфейса уровня 3 и настройте RADIUS-сервер.

```
Switch(config)# interface eth-0-26
Switch(config-if)# no switchport
Switch(config-if)# ip address 202.38.100.1/24
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# radius-server host 202.38.100.7
Switch(config)# radius-server host 2001:1000::1
Switch(config)# radius-server key test
Switch(config)# exit
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

```
Switch# show dot1x
802.1X Port-Based Authentication Enabled
  RADIUS server address: 2001:1000::1:1812
  Next radius message ID: 0
  RADIUS server address: 202.38.100.7:1812
  Next radius message ID: 0
Switch# show dot1x interface eth-0-25
802.1X info for interface eth-0-25
  portEnabled             : true
  portControl             : Auto
  portMode                : Port based
  portStatus              : Authorized
  Mac Auth bypass         : disabled
  reAuthenticate          : disabled
  reAuthPeriod            : 3600
  Max user number         : 255
  Current session number : 1
  Accept user number      : 1
  Reject user number      : 0
  Guest VLAN              : N/A
  Assign VLAN             : N/A
  QuietPeriod             : 60
  ReqMax                  : 2
  TxPeriod                : 30
  SuppTimeout             : 30
  ServerTimeout           : 30
  CD: adminControlledDirections : in
  CD: operControlledDirections  : in
  CD: bridgeDetected            : false
=======================================

session 1: 1 - 0011.0100.0001
---------------------------------------
 user name : admin
  abort:F fail:F start:F timeout:F success:T
  PAE: state: Authenticated - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 0
  BE: state: Idle - reqCount: 0 - idFromServer: 5
```

7.8.2.2 Включить dot1x на маршрутизируемом порту

В приведенном выше примере показано, как включить dot1x на порту доступа. Эта функция также может быть включена на маршрутизируемом порту. В следующем примере показано, как изменить eth-0-25 на маршрутизируемый порт и включить dot1x.

```
Switch(config)# interface eth-0-25
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.100.1/24
Switch(config-if)# dot1x port-control auto
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

7.8.2.3 Использование принудительного режима

В режиме настройки порта, dot1x может быть настроен на принудительную авторизацию или отклонение.

force-authorized (авторизован):

```
Switch(config)# interface eth-0-25
Switch(config-if)# dot1x port-control force-authorized
Switch(config-if)# exit
```

force-unauthorized (отклонен):

```
Switch(config)# interface eth-0-25
Switch(config-if)# dot1x port-control force-unauthorized
Switch(config-if)# exit
```

Пользователь может выбрать режим управления портами: принудительно авторизованный, принудительно неавторизованный или автоматический.

7.8.2.4 Включить учет сетевой активности dot1x

Функция учета dot1x позволяет отслеживать использование сети после аутентификации пользователя. По умолчанию dot1x отключен, его можно включить в режиме глобальной настройки.

Включить учет dot1x:

```
Switch(config)# dot1x accounting-mode radius
```

При включенной функции dot1x устройство отправляет запрос на запуск учета на сервер после аутентификации пользователя; если соответствующий ответ не получен, анализируется дополнительная политика запуска:

- Онлайн: чтобы избежать влияния сбоев сети на пользователей, можно настроить политику доступа в интернет, разрешающую пользователям находиться в сети;
- Офлайн: если запуск учета dot1x завершается неудачей, можно настроить политику офлайн, запрещающую пользователям подключаться к сети.

```
Switch(config)# dot1x accounting start-fail online
```

Пользователь может настроить учет таким образом, чтобы устройство периодически отправляло на сервер запрос на старт учета. Сервер продолжает вести учет пользователей только при получении запроса на старт учета.

Можно настроить максимальное количество попыток, когда на запрос учета не приходит ответ, а также действие в случае сбоя учета. По умолчанию максимальное количество попыток, когда запрос на учет не получает отклик, установлено на 3, и пользователю разрешается оставаться в сети даже после не подтверждённого запроса.

```
Switch(config)# dot1x accounting realtime 60
Switch(config)# dot1x accounting interim-fail max-times 2 offline
```

7.8.2.5 Необязательный параметр dot1x

Дополнительные параметры для RADIUS-сервера:

- установите время ожидания для повторной активации RADIUS-сервера;
- установите максимальное количество неудачных RADIUS-запросов, отправляемых на сервер;
- Установите значение тайм-аута отсутствия ответа от RADIUS-сервера.

```
Switch(config)# radius-server deadtime 10
Switch(config)# radius-server retransmit 5
Switch(config)# radius-server timeout 10
```

Атрибуты интерфейса:

- укажите количество попыток повторной аутентификации до потери авторизации;
- установите версию протокола;
- укажите период ожидания в состоянии HELD;
- включите повторную аутентификацию на порту;
- укажите количество секунд между попытками авторизации;
- укажите тайм-аут ответа сервера аутентификации;
- укажите тайм-аут ответа запрашивающей стороны;
- укажите количество секунд между попытками запроса с тем же ID.
- включить механизм рукопожатия dot1x с клиентом на порту;
- указать период для механизма рукопожатия.

```
Switch(config)# interface eth-0-25
Switch(config-if)# dot1x  max-req  5
Switch(config-if)# dot1x protocol-version 1
Switch(config-if)# dot1x quiet-period 120
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout re-authperiod 1800
Switch(config-if)# dot1x timeout server-timeout 60
Switch(config-if)# dot1x timeout supp-timeout 60
Switch(config-if)# dot1x timeout tx-period 60
```

```
Switch(config-if)# dot1x handshake
Switch(config-if)# dot1x timeout handshake-period 1
Switch(config-if)# exit
```

7.9 Настройка гостевой VLAN

7.9.1 Общие положения

7.9.1.1 Описание Функции

Для каждого порта 802.1x на коммутаторе можно настроить гостевую VLAN, чтобы предоставлять клиентам дополнительные услуги. Вот как это можно применять: некоторым клиентам может потребоваться обновить свою систему для аутентификации 802.1x, а некоторые хосты, например, системы Windows 98, могут и не поддерживать 802.1x. Если сервер аутентификации не получает ответа на свой запрос/кадр идентификации EAPOL, клиенты, не поддерживающие 802.1x, помещаются в гостевую VLAN для данного порта. При этом сервер не предоставляет доступ к сети клиентам, поддерживающим 802.1x, и которые не прошли аутентификацию. При перемещении порта коммутатора в гостевую VLAN доступ разрешается любому количеству хостов.

Функция гостевых VLAN не поддерживается на внутренних VLAN (маршрутизируемых портах) или транковых портах; она поддерживается только на портах доступа. Таким образом, гостевая VLAN поддерживается на порту доступа, но не поддерживается на маршрутизируемом порту или транковом порту.

7.9.2 Настройка

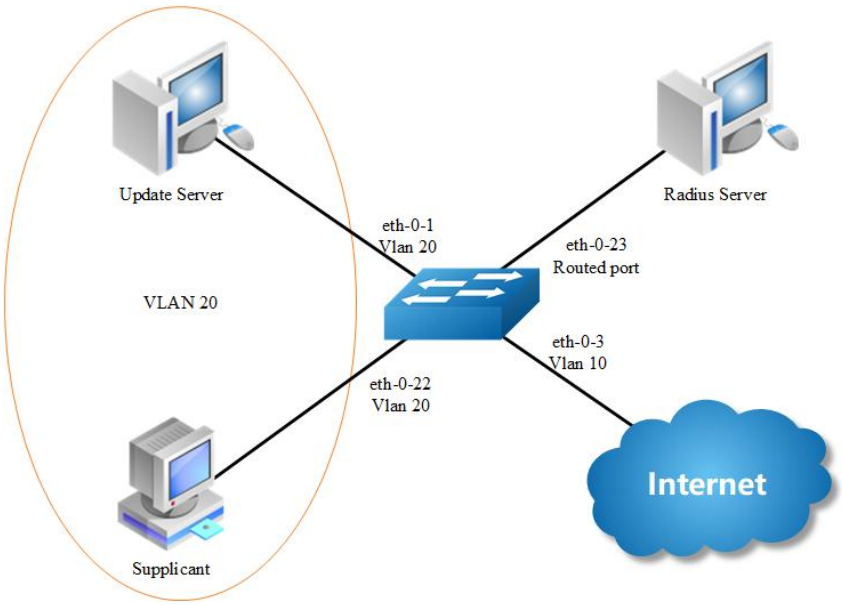


Рисунок 35 – Гостевая VLAN: до аутентификации

В приведенной выше топологии порт eth-0-22 поддерживает стандарт IEEE 802.1X и находится в собственном VLAN 10, а настроенная гостевая VLAN для этого порта — VLAN 20. Таким образом, клиенты, не поддерживающие 802.1X, будут помещены в VLAN 20 после того, как аутентификатор отправит максимальное количество запросов EAPOL/кадров идентификации, и не получит ответа.

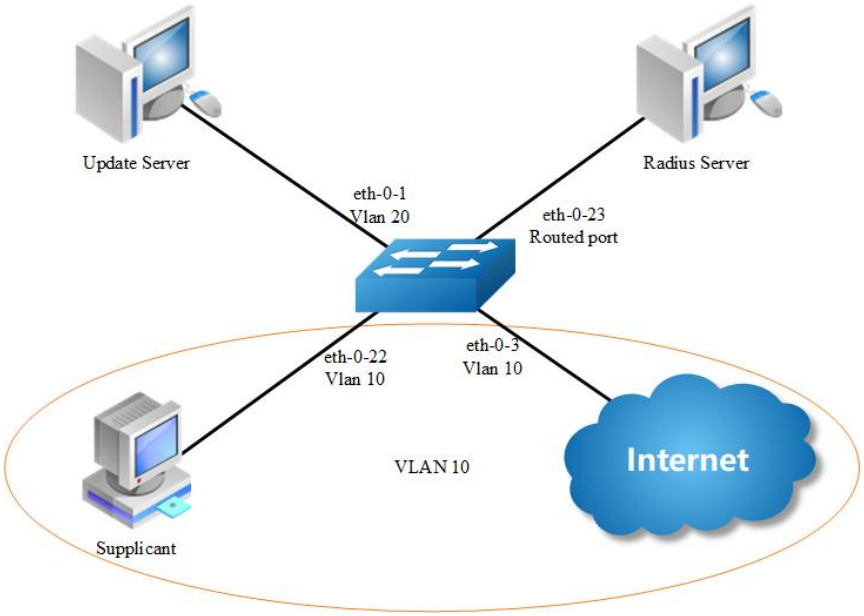


Рисунок 36 – Гостевая VLAN: после аутентификации

В качестве сервера аутентификации мы используем удаленный Linux RADIUS-сервер, адрес которого — 202.38.100.7, а IP-адрес подключенного маршрутизируемого порта eth-0-23 — 202.38.100.1. После аутентификации клиента RADIUS-сервером, он получает доступ к общедоступному интернету, который также находится в VLAN 10.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# vlan 20
Switch(config-vlan)# exit
```

Шаг 3. Включите dot1x глобально.

```
Switch(config)# dot1x system-auth-ctrl
```

Шаг 4. Войдите в режим настройки интерфейса, задайте атрибуты интерфейса, включите dot1x и настройте гостевой VLAN.

```
Switch(config)# interface eth-0-22
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# dot1x port-control auto
Switch( config-if)# no shutdown
Switch(config-if)# dot1x guest vlan 20
Switch(config-if)# exit
```

Шаг 5. Задайте атрибуты интерфейса уровня 3 и настройте RADIUS-сервер.

```
Switch(config)# interface eth-0-23
Switch(config-if)# no switchport
Switch(config-if)# ip address 202.38.100.1/24
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# radius-server host 202.38.100.7
Switch(config)# radius-server key test
Switch(config)#end
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Начальное состояние:

```
Switch# show running-config
dot1x system-auth-ctrl
radius-server host 202.38.100.7 key test
vlan database
 vlan 10,20
!
interface eth-0-22
 switchport access vlan 10
 dot1x port-control auto
 dot1x guest-vlan 20
!
interface eth-0-23
 no switchport
 ip address 202.38.100.1/24
!

Switch# show dot1x interface eth-0-22
```

```
802.1X info for interface eth-0-22
  portEnabled             : true
  portControl             : Auto
  portMode                : Port based
  portStatus              : Unauthorized
  Mac Auth bypass         : disabled
  reAuthenticate          : disabled
  reAuthPeriod            : 3600
  Max user number         : 255
  Current session number  : 0
  Accept user number      : 0
  Reject user number      : 0
  Guest VLAN              : 20
  Assign VLAN             : N/A
  QuietPeriod             : 60
  ReqMax                  : 2
  TxPeriod                : 30
  SuppTimeout             : 30
  ServerTimeout           : 30
  CD: adminControlledDirections : in
  CD: operControlledDirections  : in
  CD: bridgeDetected            : false
========================================

Switch# show vlan brief
VLAN ID  Name            State   STP ID  DSCP    Member ports
                                                 (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1       default          ACTIVE  0       Disable eth-0-1(u) eth-0-2(u)
                                                 eth-0-3(u) eth-0-4(u)
                                                 eth-0-5(u) eth-0-6(u)
                                                 eth-0-7(u) eth-0-8(u)
                                                 eth-0-9(u) eth-0-10(u)
                                                 eth-0-11(u) eth-0-12(u)
                                                 eth-0-13(u) eth-0-14(u)
                                                 eth-0-15(u) eth-0-16(u)
                                                 eth-0-17(u) eth-0-18(u)
                                                 eth-0-19(u) eth-0-20(u)
                                                 eth-0-21(u) eth-0-24(u)
                                                 eth-0-25(u) eth-0-26(u)
                                                 eth-0-27(u) eth-0-28(u)
                                                 eth-0-29(u) eth-0-30(u)
                                                 eth-0-31(u) eth-0-32(u)
                                                 eth-0-33(u) eth-0-34(u)
                                                 eth-0-35(u) eth-0-36(u)
                                                 eth-0-37(u) eth-0-38(u)
                                                 eth-0-39(u) eth-0-40(u)
                                                 eth-0-41(u) eth-0-42(u)
```

```
                                                    eth-0-43(u) eth-0-44(u)
                                                    eth-0-45(u) eth-0-46(u)
                                                    eth-0-47(u) eth-0-48(u)
10       VLAN0010          ACTIVE   0        Disable eth-0-22(u)
20       VLAN0020          ACTIVE   0        Disable
```

После настройки гостевой VLAN:

```
Switch# show dot1x interface eth-0-22
802.1X info for interface eth-0-22
  portEnabled             : true
  portControl             : Auto
  portMode                : Port based
  portStatus              : Unauthorized
  Mac Auth bypass         : disabled
  reAuthenticate          : disabled
  reAuthPeriod            : 3600
  Max user number         : 255
  Current session number  : 1
  Accept user number      : 0
  Reject user number      : 1
  Guest VLAN              : 20(Port Authorized by guest vlan)
  Assign VLAN             : N/A
  QuietPeriod             : 60
  ReqMax                  : 2
  TxPeriod                : 30
  SuppTimeout             : 30
  ServerTimeout           : 30
  CD: adminControlledDirections : in
  CD: operControlledDirections  : in
  CD: bridgeDetected            : false
=======================================

session 1: 1 - 0011.0100.0001
---------------------------------------
 user name : admin
  abort:F fail:T start:F timeout:F success:F
  PAE: state: Held - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  BE: state: Idle - reqCount: 0 - idFromServer: 92

Switch# show vlan brief
VLAN ID  Name            State    STP ID  DSCP    Member ports
                                                  (u)-Untagged, (t)-Tagged
======= ================ ======== ======= ======= ========================
1        default          ACTIVE   0       Disable eth-0-1(u) eth-0-2(u)
                                                    eth-0-3(u) eth-0-4(u)
                                                    eth-0-5(u) eth-0-6(u)
                                                    eth-0-7(u) eth-0-8(u)
```

```
                                                    eth-0-9(u) eth-0-10(u)
                                                    eth-0-11(u) eth-0-12(u)
                                                    eth-0-13(u) eth-0-14(u)
                                                    eth-0-15(u) eth-0-16(u)
                                                    eth-0-17(u) eth-0-18(u)
                                                    eth-0-19(u) eth-0-20(u)
                                                    eth-0-21(u) eth-0-24(u)
                                                    eth-0-25(u) eth-0-26(u)
                                                    eth-0-27(u) eth-0-28(u)
                                                    eth-0-29(u) eth-0-30(u)
                                                    eth-0-31(u) eth-0-32(u)
                                                    eth-0-33(u) eth-0-34(u)
                                                    eth-0-35(u) eth-0-36(u)
                                                    eth-0-37(u) eth-0-38(u)
                                                    eth-0-39(u) eth-0-40(u)
                                                    eth-0-41(u) eth-0-42(u)
                                                    eth-0-43(u) eth-0-44(u)
                                                    eth-0-45(u) eth-0-46(u)
                                                    eth-0-47(u) eth-0-48(u)
10      VLAN0010          ACTIVE  0       Disable
20      VLAN0020          ACTIVE  0       Disable eth-0-22(u)
    Client is authenticated

Switch# show dot1x interface eth-0-22
802.1X info for interface eth-0-22
  portEnabled             : true
  portControl             : Auto
  portMode                : Port based
  portStatus              : Authorized
  Mac Auth bypass         : disabled
  reAuthenticate          : disabled
  reAuthPeriod            : 3600
  Max user number         : 255
  Current session number  : 1
  Accept user number      : 1
  Reject user number      : 0
  Guest VLAN              : 20
  Assign VLAN             : N/A
  QuietPeriod             : 60
  ReqMax                  : 2
  TxPeriod                : 30
  SuppTimeout             : 30
  ServerTimeout           : 30
  CD: adminControlledDirections : in
  CD: operControlledDirections  : in
  CD: bridgeDetected            : false
=======================================
```

```
session 1: 1 - 0011.0100.0001
--------------------------------------
 user name : admin
  abort:F fail:F start:F timeout:F success:T
  PAE: state: Authenticated - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 0
  BE: state: Idle - reqCount: 0 - idFromServer: 207

Switch# show vlan brief
VLAN ID  Name            State   STP ID  DSCP    Member ports
                                                 (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1       default          ACTIVE  0       Disable eth-0-1(u) eth-0-2(u)
                                                 eth-0-3(u) eth-0-4(u)
                                                 eth-0-5(u) eth-0-6(u)
                                                 eth-0-7(u) eth-0-8(u)
                                                 eth-0-9(u) eth-0-10(u)
                                                 eth-0-11(u) eth-0-12(u)
                                                 eth-0-13(u) eth-0-14(u)
                                                 eth-0-15(u) eth-0-16(u)
                                                 eth-0-17(u) eth-0-18(u)
                                                 eth-0-19(u) eth-0-20(u)
                                                 eth-0-21(u) eth-0-24(u)
                                                 eth-0-25(u) eth-0-26(u)
                                                 eth-0-27(u) eth-0-28(u)
                                                 eth-0-29(u) eth-0-30(u)
                                                 eth-0-31(u) eth-0-32(u)
                                                 eth-0-33(u) eth-0-34(u)
                                                 eth-0-35(u) eth-0-36(u)
                                                 eth-0-37(u) eth-0-38(u)
                                                 eth-0-39(u) eth-0-40(u)
                                                 eth-0-41(u) eth-0-42(u)
                                                 eth-0-43(u) eth-0-44(u)
                                                 eth-0-45(u) eth-0-46(u)
                                                 eth-0-47(u) eth-0-48(u)
10      VLAN0010         ACTIVE  0       Disable eth-0-22(u)
20      VLAN0020         ACTIVE  0       Disable

Switch# show dot1x
802.1X Port-Based Authentication Enabled
  RADIUS server address: 202.38.100.7:1812
  Next radius message ID: 0
Switch# show dot1x statistics
=====================================
802.1X statistics for interface eth-0-22
  EAPOL Frames Rx: 52 - EAPOL Frames Tx: 4270
  EAPOL Start Frames Rx: 18 - EAPOL Logoff Frames Rx: 2
  EAP Rsp/Id Frames Rx: 29 - EAP Response Frames Rx: 3
```

```
EAP Req/Id Frames Tx: 3196 - EAP Request Frames Tx: 3
Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
EAPOL Last Frame Version Rx: 2 - EAPOL Last Frame Src: ae38.3288.f046
```

7.10 Настройка инспекции ARP пакетов

7.10.1 Общие положения

7.10.1.1 Описание Функции

Проверка. ARP — это функция безопасности, которая проверяет подлинность ARP-пакетов в сети. Проверка. ARP перехватывает, регистрирует и отбрасывает ARP-пакеты с недействительными привязками IP-адреса к MAC-адресу. Эта возможность защищает сеть от атак типа «злоумышленник посередине». Проверка. ARP гарантирует, что передаются только действительные ARP-запросы и ответы. Коммутатор выполняет следующие действия:

Перехватывать все ARP-запросы и ответы на ненадежных портах.

Перед обновлением ARP-кэша или перед пересылкой пакета соответствующему адресату проверяется, что каждый из перехваченных пакетов имеет действительную привязку IP-адреса к MAC-адресу. Недействительные ARP-пакеты отбрасываются.

Проверка. ARP выполняется на основе связок IP-адресов к MAC-адресам, хранящихся в базе данных привязок DHCP snooping. Эта база данных создается функцией DHCP snooping в то случае, если DHCP snooping включен на VLAN и на коммутаторе. Если ARP-пакет получен на доверенном интерфейсе, коммутатор пересылает пакет без каких-либо проверок.

7.10.1.2 Основные термины и понятия

Ниже приведено краткое описание терминов и понятий, используемых для описания проверки ARP:

- DHCP Snooping: функция безопасности, которая действует как брандмауэр между недоверенными хостами и доверенными DHCP-серверами. Эта функция создает и поддерживает базу данных привязок DHCP Snooping, которая содержит информацию о недоверенных хостах с арендованными IP-адресами.

- Протокол разрешения адресов (ARP): сопоставляет IP-адрес с MAC-адресом. Например, хост B хочет отправить информацию хосту A, но в его ARP-кэше отсутствует MAC-адрес хоста A. Хост B генерирует широковещательное сообщение для всех хостов в широковещательном домене, чтобы получить MAC-адрес, связанный с IP-адресом хоста A. Все хосты в широковещательном домене получают ARP-запрос, и хост A отвечает своим MAC-адресом.

7.10.2 Настройка

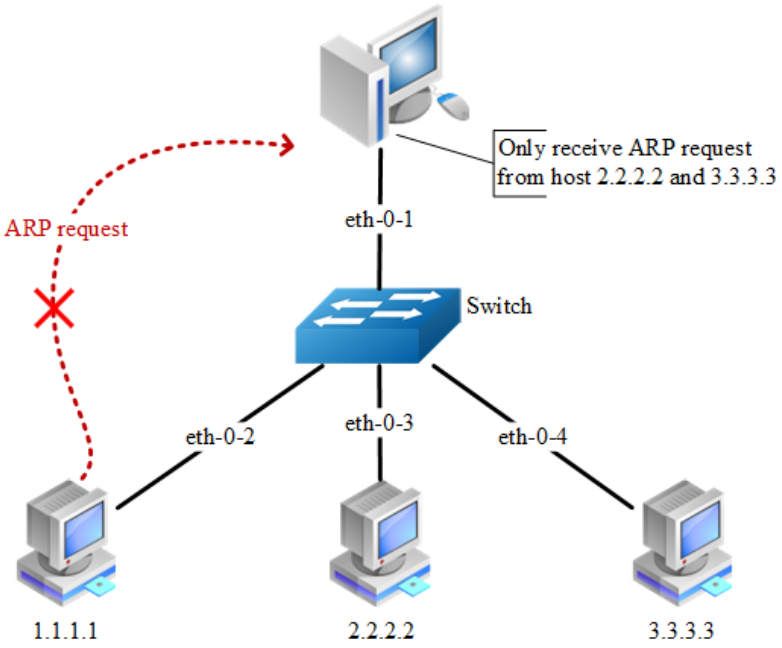


Рисунок 37 – ARP inspection

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# exit
Switch(config)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и добавьте интерфейс в VLAN.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit

Switch(config)# interface eth-0-3
Switch(config-if)# switchport access vlan 2
```

```
Switch(config-if)# exit

Switch(config)# interface eth-0-4
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
```

Шаг 4. Настройка проверки ARP.

```
Switch(config)# interface eth-0-1
Switch(config-if)# ip arp inspection trust
Switch(config-if)# exit
Switch(config)# ip arp inspection vlan 2
Switch(config)# ip arp inspection validate src-mac ip dst-mac
```

Шаг 5. Настройка списка доступа ARP.

```
Switch(config)# arp access-list test
Switch(config-arp-acl)# deny request ip host 1.1.1.1 mac any
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter test vlan 2
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# exit
```

Шаг 7. Проверка.

Проверьте конфигурацию ARP инспекции на коммутаторе:

```
Switch# show ip arp inspection
Source Mac Validation        : Enabled
Destination Mac Validation   : Enabled
IP Address Validation        : Enabled
Vlan     Configuration     ACL Match     Static ACL
================================================================
2        enabled             test
Vlan     ACL Logging     DHCP Logging
================================================================
2        deny              deny
Vlan     Forwarded       Dropped     DHCP Drops     ACL Drops
================================================================
2        0                 0             0               0
Vlan     DHCP Permits     ACL Permits     Source MAC Failures
================================================================
2        0                  0                  0
Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
```

```
================================================================
2       0                           0                                   0
```

Отобразить информацию из журнала проверки ARP на коммутаторе:

```
Switch# show ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 5 entries per 1 seconds.
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
```

7.11 Настройка функции DHCP Snooping

7.11.1 Общие положения

7.11.1.1 Описание Функции

Функция DHCP snooping — это функция безопасности, которая действует как брандмауэр между недоверенными хостами и доверенными DHCP-серверами.

Функция DHCP snooping выполняет следующие действия:

- проверяет сообщения DHCP, полученные из ненадежных источников, и отфильтровывает недействительные сообщения.

- создает и поддерживает базу данных привязки DHCP snooping, содержащую информацию о недоверенных хостах с арендованными IP-адресами.

- использует базу данных привязок DHCP snooping для проверки последующих запросов от недоверенных хостов.

Другие функции безопасности, такие как динамическая ARP инспекция (DAI), также используют информацию, хранящуюся в базе данных привязок DHCP snooping. DHCP snooping включается для каждой VLAN отдельно. По умолчанию эта функция неактивна для всех VLAN. Вы можете включить эту функцию для одной VLAN или для диапазона VLAN. Функция DHCP snooping реализована на программном уровне. Все сообщения DHCP перехватываются и направляются в ЦП для обработки.

7.11.2 Настройка

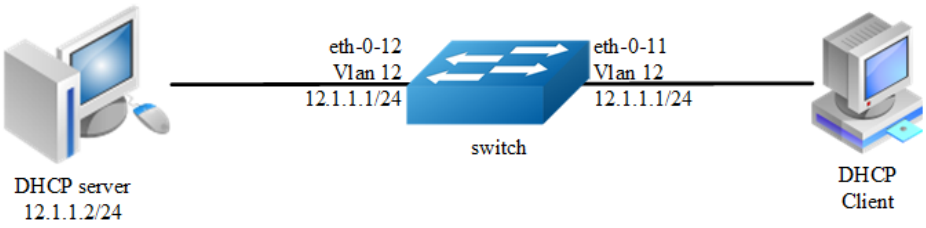


Рисунок 38 – DHCP snooping

На этом рисунке представлена сетевая топология для тестирования функций DHCP snooping. Для создания тестового стенда нам понадобятся два компьютера под управлением Linux и один коммутатор.

Компьютер A используется в качестве DHCP-сервера.

Компьютер B используется в качестве DHCP-клиента.

Коммутатор используется в качестве устройства для отслеживания DHCP-адресов.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 12
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и добавьте интерфейс в VLAN.

```
Switch(config)# interface eth-0-12
Switch(config-if)# switchport
Switch(config-if)# switchport access vlan 12
Switch(config-if)# dhcp snooping trust
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-11
Switch(config-if)# switchport
Switch(config-if)# switchport access vlan 12
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 12
Switch(config-if)# ip address 12.1.1.1/24
Switch(config-if)# exit
```

Шаг 4. Настройка атрибутов DHCP.

```
Switch(config)# dhcp snooping verify mac-address
Switch(config)# service dhcp enable
Switch(config)# dhcp snooping
Switch(config)# dhcp snooping vlan 12
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# exit
```

Шаг 6. Проверка.

Проверьте конфигурацию интерфейса.

```
Switch(config)# show running-config interface eth-0-12
!
interface eth-0-12
 dhcp snooping trust
 switchport access vlan 12
!

Switch(config)# show running-config interface eth-0-11
!
interface eth-0-11
 switchport access vlan 12
!
```

Проверьте состояние службы DHCP.

```
Switch# show services
Networking services configuration:
Service Name          Status
============================================================
dhcp                    enable
```

Чтобы проверить текущую конфигурацию, выведите на экран конфигурацию DHCP snooping.

```
Switch# show dhcp snooping config
dhcp snooping service: enabled
dhcp snooping switch: enabled
Verification of hwaddr field: enabled
Insertion of relay agent information (option 82): disable
Relay agent information (option 82) on untrusted port: not allowed
dhcp snooping vlan 12
```

Показать статистику перехвата DHCP.

```
Switch# show dhcp snooping statistics
DHCP snooping statistics:
```

```
============================================================
DHCP packets                                 17
BOOTP packets                                0
Packets forwarded                           30
Packets invalid                              0
Packets MAC address verify failed      0
Packets dropped                              0
```

Показать информацию о привязке DHCP snooping.

```
Switch# show dhcp snooping binding all
DHCP snooping binding table:
VLAN MAC Address    Interface  Lease(s)    IP Address
============================================================
12   0016.76a1.7ed9 eth-0-11   691190      12.1.1.65
```

7.12 Настройка функции IP source guard

7.12.1 Общие положения

7.12.1.1 Описание Функции

Защита IP-адреса источника предотвращает подмену IP-адресов, разрешая на определенном порту только те IP-адреса, которые получены с помощью DHCP snooping. Первоначально весь IP-трафик на порту блокируется, за исключением пакетов DHCP, перехваченных DHCP snooping. Когда клиент получает действительный IP-адрес от DHCP-сервера, на порт устанавливается список контроля доступа (ACL), разрешающий трафик только с этого IP-адреса. Этот процесс ограничивает IP-трафик клиента только теми IP-адресами, которые получены от DHCP-сервера; любой IP-трафик с IP-адреса, отличного от указанного в списке разрешенных ACL, отфильтровывается.

Фильтр IP-адреса на порту изменяется при создании или удалении новой записи привязки DHCP-snooping. Список контроля доступа (ACL) порта изменяется и повторно применяется, чтобы отразить изменение привязки IP Source. По умолчанию, если вы включаете IP Source Guard без каких-либо привязок DHCP-snooping, на порту устанавливается ACL по умолчанию, запрещающий весь IP-трафик. При отключении IP Source Guard любой ACL фильтра IP Source удаляется с порта.

Кроме того, функция IP Source Guard может использовать фильтрацию по IP-адресу и MAC-адресу. При включении этой опции IP-трафик фильтруется на основе IP-адреса и MAC-адреса источника. Коммутатор пересылает трафик только в том случае, если IP-адрес и MAC-адрес соответствуют записи в таблице привязки IP-адресов. В противном случае коммутатор отбрасывает все остальные типы пакетов, кроме пакетов DHCP.

Коммутатор также поддерживает фильтрацию по IP, MAC и VLAN. При включении опции IP-трафик фильтруется по исходным IP-адресам и MAC-адресам. Коммутатор пересылает трафик

только в том случае, если исходный IP-адрес, MAC-адрес и VLAN соответствуют записи в таблице привязки IP-источника.

Если на интерфейсе включена функция ip source guard, включите параметр «arp as-layer-3» в глобальном режиме конфигурации, чтобы пакеты ARP, соответствующие записям ip source guard, могли передаваться в обычном режиме. Если эта функция отключена, система будет отбрасывать ARP пакеты.

7.12.1.2 Основные термины и понятия

- Протокол динамической конфигурации хоста (DHCP): Протокол динамической конфигурации хоста (DHCP) — это протокол типа клиент-сервер, который автоматически предоставляет хосту его IP-адрес и другую информацию, такую как маска подсети и шлюз по умолчанию.

- DHCP Snooping: это функция безопасности, которая действует как брандмауэр между недоверенными хостами и доверенными DHCP-серверами. Эта функция создает и поддерживает базу данных привязок DHCP Snooping, которая содержит информацию о недоверенных хостах с арендованными IP-адресами.

- ACL: Список контроля доступа.

7.12.2 Настройка

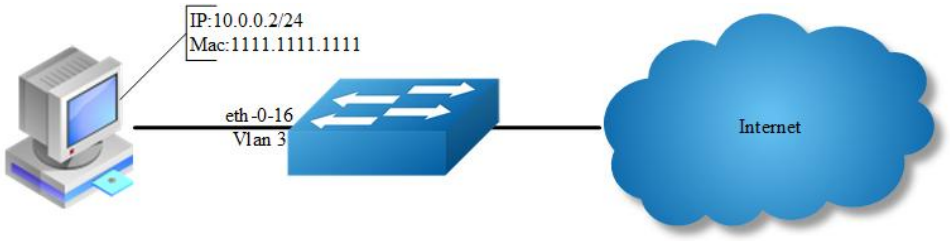


Рисунок 39 – IP Source Guard

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите ARP AS-Llayer-3.

```
Switch(config)# arp as-layer-3 enable
```

Шаг 3. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 3
Switch(config-vlan)# exit
```

Шаг 4. Войдите в режим настройки интерфейса и задайте атрибуты.

```
Switch(config)# interface eth-0-16
Switch(config-if)# switchport
Switch(config-if)# no shutdown
Switch(config-if)# switchport access vlan 3
Switch(config-if)# exit
```

Шаг 5. Добавьте записи защиты источника IP-адреса.

```
Switch(config)# ip source maximal binding number per-port 15
Switch(config)# ip source binding mac 1111.1111.1111 vlan 3 ip 10.0.0.2
interface eth-0-16
```

Шаг 6. Включите защиту IP-адреса на интерфейсе.

```
Switch(config)# interface eth-0-16
Switch(config-if)# ip verify source ip
Switch(config-if)# exit
```

Шаг 7. Выйдите из режима настройки.

```
Switch(config)# exit
```

Шаг 8. Проверка.

```
Switch#show running-config interface eth-0-16
!
interface eth-0-16
 ip verify source ip
 switchport access vlan 3
```

7.12.2.1 Удаление записи функции IP Source Guard

Удаление по записи:

```
Switch(config)# no ip source binding mac 1111.1111.1111 vlan 3 ip 10.0.0.2
interface eth-0-16
```

Удаление через интерфейс:

```
Switch(config)# no ip source binding entries interface eth-0-16
```

Удаление по VLAN:

```
Switch(config)# no ip source binding entries vlan 3
```

Удалить все:

```
Switch(config)# no ip source binding entries
```

7.13 Настройка Private VLAN

7.13.1 Общие положения

7.13.1.1 Описание Функции

Private-Vlan — это функция безопасности, используемая для предотвращения прямой связи уровня L2 между набором портов в VLAN.

Это позволяет создавать более безопасные и гибкие сетевые решения за счет изоляции портов, находящихся в одной и той же VLAN.

7.13.2 Настройка

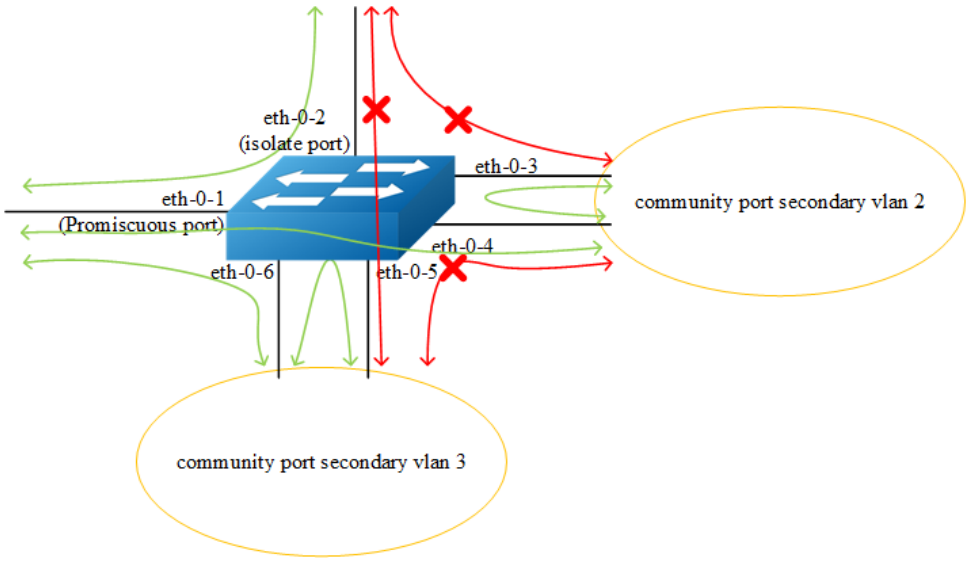


Рисунок 40 – Private VLAN

Как показано на рисунке выше:

- все порты находятся в одной и той же основной VLAN.

- порт 1 является портом, работающим в режиме promiscuous; он может взаимодействовать со всеми остальными портами.

- порт 2 является изолированным портом; он не может взаимодействовать со всеми остальными портами, кроме порта, работающего в режиме promiscuous (порт 1).

- порты 3 и 4 являются портами общего доступа во вторичном VLAN 2; они могут взаимодействовать друг с другом. Они не могут взаимодействовать со всеми остальными портами, кроме порта, работающего в режиме promiscuous.

- порты 5 и 6 являются портами общего доступа во вторичном VLAN 3; они могут взаимодействовать друг с другом. Они не могут взаимодействовать со всеми другими портами, кроме порта, работающего в режиме promiscuous.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch (config)# vlan database
Switch (config-vlan)# vlan 2
Switch (config-vlan)# quit
```

Шаг 3. Войдите в режим настройки интерфейса и задайте атрибуты.

Порт в режиме promiscuous: порт в режиме promiscuous в PVLAN может взаимодействовать с любыми другими портами в этом PVLAN.

```
Switch (config)# interface eth-0-1
Switch (config-if)# switchport mode private-vlan promiscuous
Switch (config-if)# switchport private-vlan 2
Switch (config-if)# quit
```

Изолированный порт: изолированный порт в PVLAN может взаимодействовать только с портом в режиме promiscuous в этом же PVLAN.

```
Switch (config)# interface eth-0-2
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport private-vlan 2 isolate
Switch (config-if)# quit
```

Community Порт: PVLAN может взаимодействовать с портом в режиме promiscuous и Community портами с тем же идентификатором VLAN

```
Switch (config)# interface eth-0-3
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport private-vlan 2 community-vlan 2
Switch (config-if)# quit

Switch (config)# interface eth-0-4
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport private-vlan 2 community-vlan 2
Switch (config-if)# quit

Switch (config)# interface eth-0-5
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport private-vlan 2 community-vlan 3
Switch (config-if)# quit

Switch (config)# interface eth-0-6
Switch (config-if)# switchport mode private-vlan host
```

```
Switch (config-if)# switchport private-vlan 2 community-vlan 3
Switch (config-if)# quit
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# exit
```

Шаг 5. Проверка.

Результат выполнения команды «show private-vlan» выглядит следующим образом:

```
switch # show private-vlan
Primary   Secondary Type            Ports
------------------------------------------------------------------------------
---
2         N/A       promiscuous     eth-0-1
2         N/A       isloate         eth-0-2
2         2         community       eth-0-3   eth-0-4
2         3         community       eth-0-5   eth-0-6
```

7.14 Настройка функций AAA

7.14.1 Общие положения

7.14.1.1 Описание Функции

Аутентификация проверяет пользователей, прежде чем им будет предоставлен доступ к сети и сетевым сервисам. Система может использовать методы аутентификации AAA и методы аутентификации, не относящиеся к AAA. Аутентификация RADIUS — один из методов аутентификации AAA. RADIUS — это распределенная клиент-серверная система, которая защищает сети от несанкционированного доступа. RADIUS — широко используемый протокол в сетевых средах. Он обычно встроен в сетевые устройства, такие как маршрутизаторы, модемы, серверы, коммутаторы и т. д. Клиенты отправляют запросы на аутентификацию на центральный сервер RADIUS, который содержит всю информацию об аутентификации пользователей и доступе к сетевым сервисам.

7.14.2 Настройка

На рисунке выше показана сетевая топология для функций аутентификации RADIUS. Для этого теста нам потребуется один коммутатор и два компьютера.

Один компьютер, работающий в качестве RADIUS-сервера, имеет IP-адрес интерфейса eth0 — 1.1.1.2/24.

Коммутатор имеет функцию аутентификации RADIUS. IP-адрес интерфейса eth-0-23 — 1.1.1.1/24. Управляющий IP-адрес коммутатора — 10.10.29.215, управляющий порт подключен к ПК, IP-адрес ПК — 10.10.29.10.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите AAA.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login radius-login radius local
```

Шаг 3. Настройка RADIUS-сервера.

```
Switch(config)# radius-server host 1.1.1.2 auth-port 1819 key keyname
Switch(config)# radius-server host 2001:1000::1 auth-port 1819 key keyname
```

Шаг 4. Настройте интерфейс уровня 3 и задайте IP-адрес.

```
Switch(config)# interface eth-0-23
Switch(config-if)# no switchport
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# quit
```

Шаг 5 Установите режим аутентификации

```
Switch(config)# line vty 0 7
Switch(config-line)#login authentication radius-login
Switch(config-line)#privilege level 4
Switch(config-line)#no line-password
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config-line)# end
```

Шаг 7. Проверка.

В коммутаторе можно использовать команду `show authentication status`:

```
Switch# show aaa status
aaa status:
     Authentication enable
```

Используйте команду `show keys`:

```
Switch# show aaa method-lists authentication
authen queue=AAA_ML_AUTHEN_LOGIN
    Name = default  state = ALIVE :   local
Name = radius-login  state = ALIVE :   radius  local
```

NOTE Не забудьте включить функцию аутентификации RADIUS.

Вы можете использовать команду для проверки сообщений журнала, если коммутатор не может выполнить аутентификацию RADIUS:

```
Switch# show logging buffer
```

7.15 Настройка TACACS+

7.15.1 Общие положения

7.15.1.1 Описание Функции

Аутентификация проверяет пользователей, прежде чем им будет предоставлен доступ к сети и сетевым сервисам. Система может использовать методы аутентификации AAA и методы аутентификации, не относящиеся к AAA. Аутентификация TACACS+ — один из методов аутентификации AAA. TACACS+ — это распределенная клиент-серверная система, которая защищает сети от несанкционированного доступа. TACACS+ — широко используемый протокол в сетевых средах. Он обычно встроен в сетевые устройства, такие как маршрутизаторы, модемы-серверы, коммутаторы и т. д. Клиенты отправляют запросы на аутентификацию на центральный сервер TACACS+, который содержит всю информацию об аутентификации пользователей.

7.15.2 Настройка

На рисунке выше представлена сетевая топология для функций аутентификации TACACS+. Для этого теста нам потребуется один коммутатор и два компьютера. Один компьютер будет выступать в качестве сервера TACACS+, его IP-адрес интерфейса eth0 — 1.1.1.2/24. Коммутатор также имеет функцию аутентификации TACACS+. IP-адрес интерфейса eth-0-23 — 1.1.1.1/24. Управляющий IP-адрес коммутатора — 10.10.29.215, управляющий порт подключен к ПК для тестового входа в систему, IP-адрес ПК — 10.10.29.10

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите AAA

```
Switch# configure terminal
Switch(config)# aaa new-model
```

```
Switch(config)# aaa authentication login tac-login tacacs-plus local
Switch(config)# aaa authorization exec default tacacs-plus
Switch(config)# aaa accounting exec default start-stop tacacs-plus
Switch(config)# aaa accounting commands default tacacs-plus
```

Шаг 3. Настройка сервера TACACS+.

```
Switch(config)# tacacs-server host 1.1.1.2 port 123 key keyname primary
```

Шаг 4. Настройте интерфейс уровня 3 и задайте IP-адрес.

```
Switch(config)# interface eth-0-23
Switch(config-if)# no switchport
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# quit
```

Шаг 5 Установите режим аутентификации

```
Switch(config)# line vty 0 7
Switch(config-line)#login authentication tac-login
Switch(config-line)#privilege level 4
Switch(config-line)#no line-password
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config-line)# end
```

Шаг 7. Проверка.

можно использовать команду `show authentication status`:

```
Switch# show aaa status
aaa stats: Authentication enable
```

можно использовать команду `show keys`:

```
Switch# show aaa method-lists authentication
authen queue=AAA_ML_AUTHEN_LOGIN Name = default state = ALIVE : localName =
tac-login state = ALIVE : tacacs-plus local
```

Вывод Telnet:

7.16 Настройка изоляции портов

7.16.1 Общие положения

7.16.1.1 Описание Функции

Изоляция портов (Port Isolation) — это функция безопасности, используемая для предотвращения прямой связи уровня L2/L3 между набором портов.

Позволяет создавать более безопасные и гибкие сетевые решения за счет изоляции портов, находящихся в одной и той же VLAN.

Как правило, используется на уровне доступа для изоляции пользователей.

7.16.2 Настройка

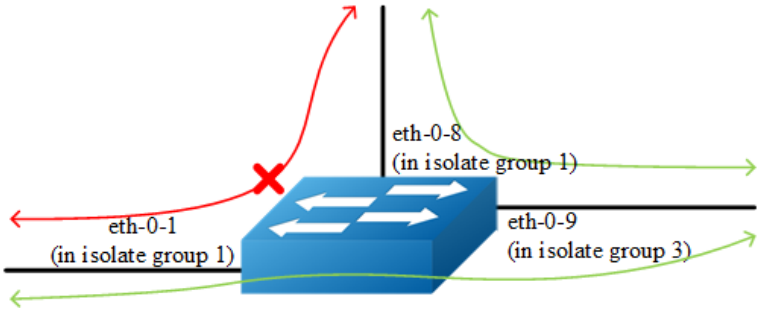


Рисунок 41 – Port Isolation

На рисунке выше представлена базовая топология для изолированного порта.

Порты 1 и 8 находятся в одной и той же изолированной группе 1, они изолированы. Следовательно, порт 1 не может взаимодействовать с портом 8. Порт 9 находится в другой изолированной группе 3, поэтому порт 9 может взаимодействовать с портами 1 и 8.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите режим изоляции портов глобально.

Режим «l2» означает, что изолированы только пакеты уровня 2. Режим «all» означает, что изолированы все пакеты, включая пакеты, пересылаемые в соответствии с маршрутами уровня 3.

```
Switch(config)# port-isolate mode l2
```

Шаг 3. Войдите в режим настройки интерфейса и установите группу изоляции.

```
Switch(config-if)# interface eth-0-1
Switch(config-if)# port-isolate group 1
Switch(config-if)# exit
```

```
Switch(config)# interface eth-0-8
Switch(config-if)# port-isolate group 1
Switch(config-if)# exit

Switch(config)# interface eth-0-9
Switch(config-if)# port-isolate group 3
Switch(config-if)# exit
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

Для отображения групп изоляции портов используйте следующую команду:

```
switch# show port-isolate
------------------------------------------------------------------
 Port Isolate Groups:
------------------------------------------------------------------
 Groups ID: 1
eth-0-1, eth-0-8
------------------------------------------------------------------
Groups ID: 3
eth-0-9
```

7.17 Настройка защиты от DDoS атак

7.17.1 Общие положения

7.17.1.1 Описание Функции

Атака типа «отказ в обслуживании» (DoS-атака) — это попытка сделать компьютерный ресурс недоступным для его предполагаемых пользователей. Атака, как правило, состоит из согласованных усилий одного или нескольких человек, направленных на полное прекращение работы интернет-сайта или сервиса, временно или на неопределенный срок. Злоумышленники, совершающие DoS-атаки, обычно нацеливаются на сайты или сервисы, размещенные на веб-серверах, таких как банки, платежные системы для кредитных карт.

Функция предотвращения DDoS-атак позволяет защитить коммутатор от следующих типов атак и перехватывать атакующие пакеты:

- ICMP-флуд: злоумышленники заваливают жертву ICMP-пакетами;
- атака «смурф»: злоумышленники перегружают целевую систему поддельными широковещательными ping-сообщениями;
- SYN-флуд: злоумышленники отправляют серию SYN-запросов в систему цели;

- UDP-флуд: злоумышленники отправляют большое количество UDP-пакетов на случайные порты удаленного хоста;

- атака Fraggle: злоумышленники отправляют большое количество UDP-эхо-трафика на широковещательные IP-адреса, при этом все адреса источника являются поддельными;

- малые пакеты: злоумышленники отправляют в систему большое количество небольших пакетов до тех пор, пока не исчерпаются ресурсы;

- некорректный перехват MAC-адресов: злоумышленники отправляют пакеты с одинаковыми MAC-адресами источника и назначения;

- "Подменный IP-адрес": злоумышленники отправляют пакеты с одинаковыми исходным и целевым IP-адресами.

7.17.2 Настройка

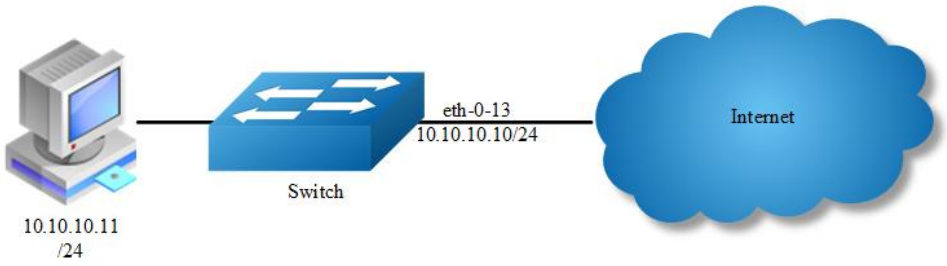


Рисунок 1-4 Топология схемы тестирования DDoS-атак

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка защиты от DDoS-атак.

Включите перехват ICMP-пакетов и установите максимальную скорость приема ICMP-пакетов на 100 пакетов в секунду.

```
Switch(config)# ip icmp intercept maxcount 100
```

Включите перехват UDP-пакетов и установите максимальную скорость приема UDP-пакетов на 100 пакетов в секунду.

```
Switch(config)# ip udp intercept maxcount 100
```

Включите перехват атаки типа Смурф

```
Switch(config)# ip smurf intercept
```

Включите перехват SYN-флуда и установите максимальную скорость приема SYN-пакетов на 100 пакетов в секунду.

```
Switch(config)# ip tcp intercept maxcount 100
```

Включите перехват атаки Fraggle

```
Switch(config)# ip fraggle intercept
```

Включите перехват атак с использованием небольших пакетов и установите длину принимаемого пакета равной или превышающей 32.

```
Switch(config)# ip small-packet intercept maxlength 32
```

Включите перехват пакетов с IP-адресом источника равным IP-адресу назначения

```
Switch(config)# ip ipeq intercept
```

Включите перехват пакетов с MAC-адресом источника, равным MAC-адресу назначения.

```
Switch(config)# ip maceq intercept
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show ip-intercept config
Current DDoS Prevent configuration:
============================================================
ICMP Flood Intercept              :Enable  Maxcount:500
UDP Flood Intercept               :Enable  Maxcount:500
SYN Flood Intercept               :Enable  Maxcount:500
Small-packet Attack Intercept     :Enable  Packet Length:45
Smurf Attack Intercept            :Enable
Fraggle Attack Intercept          :Enable
MAC Equal Intercept               :Enable
IP Equal Intercept                :Enable
Switch# show ip-intercept statistics
Current DDoS Prevent statistics:
============================================================
Resist Small-packet Attack packets number    :  1730
Resist ICMP Flood packets number             :  0
Resist SYN Flood packets number              :  0
Resist Fraggle Attack packets number         :  0
Resist UDP Flood packets number              :  0

Current DDoS Prevent mgmt-if statistics:
============================================================
Resist ICMP Flood packets number             :  0
Resist SYN Flood packets number              :  0
Resist Fraggle Attack packets number         :  0
Resist UDP Flood packets number              :  0
```

7.18 Настройка связки ключей (Key Chain)

7.18.1 Общие положения

7.18.1.1 Описание Функции

Key chain - это механизм обеспечения безопасности, который позволяет динамически управлять аутентификационными ключами (паролями) для протоколов маршрутизации или управления. Протоколы маршрутизации и сетевые приложения часто используют этот метод аутентификации для повышения безопасности при взаимодействии с другими узлами.

Вместо использования одного статического пароля, keychain позволяет создать последовательность ключей, которые автоматически сменяют друг друга по расписанию

Если в качестве метода обеспечения безопасности используются ключи, необходимо указать срок их действия и регулярно заменять их по истечении срока действия.

7.18.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте связку ключей и создайте сами ключи

```
Switch(config)# key chain test
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string ##test_keystring_1##
Switch(config-keychain-key)# accept-lifetime 0:0:1 1 jan 2012 infinite
Switch(config-keychain)# key 2
Switch(config-keychain-key)# key-string ##test_keystring_2##
Switch(config-keychain-key)# send-lifetime 0:0:1 2 jan 2012 infinite
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения конфигурации связки ключей используйте команду «show key chain» в привилегированном режиме EXEC

```
Switch # show key chain
key chain test:
    key 1 -- text "key-string ##test_keystring_1##"
      accept-lifetime <00:00:01 Jan 01 2012> - <infinite>
      send-lifetime <always valid> - <always valid> [valid now]
```

```
    key 2 -- text "key-string ##test_keystring_2##"
      accept-lifetime <always valid> - <always valid> [valid now]
      send-lifetime <00:00:01 Jan 02 2012> - <infinite>
```

7.19 Настройка блокировки портов

7.19.1 Общие положения

7.19.1.1 Описание Функции

По умолчанию коммутатор рассылает пакеты с неизвестными MAC-адресами назначения через все порты. Если неизвестный трафик перенаправляется на незащищенный порт, могут возникнуть проблемы с безопасностью. Чтобы предотвратить пересылку неизвестного трафика с одного порта на другой, можно заблокировать порт (защищенный или незащищенный), чтобы он не рассылал неизвестные одноадресные или многоадресные пакеты на другие порты.

7.19.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и заблокируйте неизвестные Unicast запросы.

```
Switch(config)# interface eth-0-1
Switch(config-if)# port-block unknown-unicast
Switch(config-if)# exit
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

Для отображения конфигурации блокировки портов используйте команду «show port-block» в привилегированном режиме EXEC：

```
Switch # show port-block interface eth-0-1
 Known unicast blocked: Enabled
 Known multicast blocked: Disabled
 Unknown unicast blocked: Disabled
 Unknown multicast blocked: Disabled
 Broadcast blocked: Disabled
```

7.20 Настройка ACL глобально

7.20.1 Общие положения

Описание функции

Система поддерживает создание глобальных списков ACL. Если одновременно существуют ACL на порту, ACL VLAN/VLANIF и глобальный ACL, приоритет будет следующим: ACL на порту > ACL VLAN/VLANIF > глобальный ACL.

Принцип работы следующий: при получении или отправке пакетов система определяет правило ACL по приоритету, и как только правило срабатывает, пакеты немедленно пересылаются. Если правило верхнего уровня ACL не сработало, система переходит к поиску правила следующего уровня ACL.

7.20.2 Варианты настройки

7.20.2.1 Создание ACL глобально

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите глобальный ACL, (он будет действовать до следующей перезагрузки).

```
Switch(config)# global-acl enable
```

Шаг 3. Примените политику к глобальному списку контроля доступа (ACL).

```
Switch(config)# service-policy global input pmap
```

Шаг 4. Примените группу доступа к глобальному списку контроля доступа.

```
Switch(config)# access-group global input aaa
```

Шаг 5. Проверка.

```
DUT1# show running-config
global-acl enable
service-policy global input pmap
access-group global input aaa
```

7.21 Насторйка MACsec

7.21.1 Общие положения

7.21.1.1 Описание Функции

MACSec (Media Access Control Security) — это защищенный метод связи, основанный на протоколах 802.1AE и 802.1X. Он обеспечивает безопасность кадров данных Ethernet за счет аутентификации, шифрования данных, проверки целостности данных, защиты от повторного воспроизведения и других функций, предотвращая возникновение угроз безопасности.

MACSec использует технологию шифрования L2 для обеспечения безопасной передачи данных между устройствами на каждом этапе, что подходит для ситуаций, требующих высокой конфиденциальности данных. После развертывания MACSec в сети, технология шифрования MACSec может обеспечить безопасную передачу данных на промежуточных устройствах передачи, снижая риск утечки информации и вредоносных сетевых атак.

Механизм работы MACsec, основные понятия и термины

- Установление и управление защищенными каналами MACsec, а также согласование ключей, используемых MACsec, являются обязанностью протокола MKA (MACsec Key Agreement).

- CA (Secure Connectivity Association) — это защищенное соединение, устанавливаемое и поддерживаемое протоколом согласования ключей, представляющее собой совокупность двух или более участников локальной сети, поддерживающих MACsec и использующих один и тот же ключ или набор ключей. Ключ, используемый участниками CA, называется SCAK (Secure Connectivity Association Key).

- MACsec в основном используется в одноранговых сетях (от интерфейса одного устройства к интерфейсу другого устройства), поэтому в основном используются парные CAK. Два подключенных устройства образуют CA и используют один и тот же CAK.

- SA (Secure Association) — это защищенное соединение, обеспечивающее безопасную передачу кадров данных между участниками CA. Каждый SA имеет один или несколько ключей шифрования для кадров данных, называемых SAK (Secure Association Key). SAK генерируется алгоритмами на основе CAK и используется для шифрования и дешифрования пакетов данных.

- Механизм обеспечения безопасности

- MACsec обеспечивает безопасную передачу бизнес-данных пользователя в локальной сети по следующим параметрам:

- Шифрование данных: Отправитель шифрует данные и передает их в зашифрованном виде по каналу локальной сети. Получатель расшифровывает полученные зашифрованные данные перед выполнением других операций.

- Проверка. целостности: Получатель выполняет проверку целостности полученных данных, чтобы определить, были ли они изменены. Отправитель вычисляет значение проверки целостности (ICV) на основе всего сообщения данных и алгоритма шифрования и добавляет его к сообщению. После получения сообщения получатель вычисляет ICV на основе сообщения данных без учета ICV и с использованием того же алгоритма шифрования и сравнивает его с ICV в сообщении. Если они совпадают, сообщение считается полным.

- Защита от повторного воспроизведения: чтобы предотвратить сетевые атаки злоумышленников путем многократной отправки перехваченных пакетов, получатель по умолчанию отбрасывает дублирующиеся или не порядковые пакеты. При передаче пакетов данных по сети может происходить перестановка порядка пакетов. Механизм защиты от повторного воспроизведения допускает определенную степень нарушения порядка кадров данных, и такие кадры, находящиеся вне этого порядка, могут быть приняты в пределах заданного пользователем диапазона смещения.

Механизм раздельных этапов

Процесс взаимодействия по протоколу MACsec делится на три этапа: согласование, защищенная связь и поддержание активности сессии.

1. Согласование

Устройства используют настроенные предварительно согласованные ключи (PSK) в качестве CAK для инициирования сеансов согласования посредством сообщений EAPOL-MKA. Интерфейс устройства с высоким приоритетом будет выбран в качестве сервера ключей, который генерирует SAK для шифрования пакетов данных на основе статически настроенного CAK и распространяет его среди других устройств. Устройства уведомляют друг друга о своих возможностях и различных параметрах, необходимых для установления сеанса, таких как приоритет и ожидается ли шифрование, через протокол MKA.

Пользователи могут настроить значение приоритета интерфейса. Чем ниже значение, тем выше приоритет. Интерфейс устройства с более высоким приоритетом будет выбран в качестве сервера ключей. Когда оба устройства имеют одинаковый приоритет, сравнивается значение SCI (идентификатор защищенного канала) интерфейса. SCI состоит из MAC-адреса и идентификатора порта интерфейса. Интерфейс с более низким значением SCI будет выбран в качестве сервера ключей.

2. Безопасная связь

Отправитель шифрует сообщение данных с помощью SAK, а получатель расшифровывает сообщение данных. Оба конечных устройства могут выступать как в роли отправителя, так и получателя. Для обеспечения безопасности пакетов данных, если количество зашифрованных пакетов с использованием одного и того же SAK превышает определенное значение или когда один

и тот же SAK используется в течение определенного периода времени, SAK рекомендуется заменить.

3. Поддержание соединения

Протокол MKA определяет таймер поддержания соединения. После успешного согласования сессии MKA оба устройства подтвердят установку соединения служебными сообщениями протокола MKA. После получения такого сообщения устройство запускает таймер. Если сообщение протокола MKA получено в течение периода ожидания, таймер перезапускается. Если в течение установленного времени ожидания от другой стороны не поступает сообщение, считается, что соединение больше не является безопасным, устройство на другой стороне удаляется, и возобновляется согласование MKA.

Описание параметров и команд

CKN (secure Connectivity Association Key Name): Имя CAK, которое должно быть настроено с тем же CKN на интерфейсах обоих устройств.

CAK (secure Connectivity Association Key): На интерфейсах обоих устройств должен быть настроен один и тот же CAK, который не используется напрямую для шифрования пакетов данных, а является производным от CKN.

SAK (Secure Association Key): Генерируется сервером ключей на основе CAK и CKN и используется для шифрования и расшифровки сообщений данных.

KEK (Key Encryption Key): Оба устройства генерируют один и тот же ключ KEK на основе одного и того же CAK и CKN, который используется для шифрования и расшифровки SAK для предотвращения утечки данных во время процесса передачи.

ICV (Integrity Check Value): Отправитель вычисляет ICV на основе сообщения и помещает его в конец сообщения. Приемник использует тот же алгоритм для вычисления ICV и сравнивает его с ICV, содержащимся в сообщении. Если эти два ICV совпадают, это означает, что сообщение не было изменено и Проверка. пройдена.

ICK (ключ проверки целостности): Оба устройства генерируют один и тот же ICK на основе одного и того же CAK и CKN, который используется для вычисления ICV сообщений протокола MKA. ICK требуется только для вычисления ICV сообщений протокола MKA.

Политика MKA: существует политика MKA по умолчанию («default-policy»), значения параметров которой соответствуют значениям по умолчанию на интерфейсе, и эту политику нельзя удалить или изменить. Используйте «show mka policy», чтобы отобразить существующие политики.

ICV-mode: Режим проверки ICV может быть настроен как обычный или только Проверка. целостности. Обычный: выполняется как шифрование данных, так и Проверка. целостности (по умолчанию — обычный). Только Проверка. целостности: выполняется только Проверка. целостности без шифрования данных.

Replay-protection: Настраивается для включения/отключения защиты от повторного воспроизведения. Защита от повторного воспроизведения включена по умолчанию. Предполагая, что настроенный размер окна защиты от повторного воспроизведения равен a, если получено сообщение с порядковым номером X, порядковый номер следующего разрешенного полученного сообщения должен быть больше или равен X+1-a (размер окна защиты от повторного воспроизведения по умолчанию равен 0 кадрам данных).

Validation-mode: Поддерживает 2 режима проверки. check: означает только проверку без отбрасывания недопустимых кадров данных (по умолчанию — режим check). strict: означает проверку полученных кадров данных и отбрасывание недопустимых данных.

Cipher-suite: Оба конца шифруют, проверяют и восстанавливают кадры данных на основе настроенного алгоритма шифрования. В настоящее время поддерживаются эти типы шифрования gcm-aes-128 и gcm-aes-256 (по умолчанию — gcm-aes-128).

MKA priority: Используется для согласования и выбора серверов ключей, при этом меньшие значения указывают на более высокий приоритет (значение по умолчанию — 0).

MacSec include-sci SCI (Secure Channel Identifier): Используется для идентификации источника сообщения и состоит из MAC-адреса интерфейса и индекса интерфейса. Необходимо, чтобы заголовок кадра MACsec обоих устройств содержал SCI. По умолчанию заголовок кадра MACsec содержит SCI.

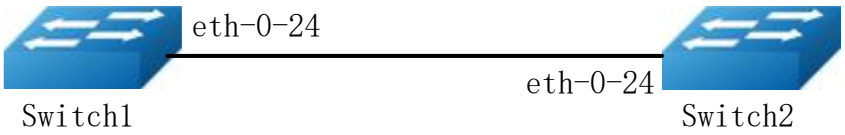
MKA apply: Применение политики. По умолчанию политика на порту не применяется.

MKA enable: Включение политики. По умолчанию отключена.

MacSec desire (включает защиту MACsec): По-умолчанию интерфейс не обеспечивает защиту MACsec для отправляемых кадров данных.

7.21.2 Пример настройки

Топология



7.21.2.1 Этапы настройки

Конфигурация на коммутаторе 1

Шаг 1. Войдите в режим настройки

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#
```

Шаг 2 Настройте IP-адрес интерфейса, чтобы обеспечить связь между двумя коммутаторами：

```
Switch1(config)# interface eth-0-24
Switch1(config-if)# no switchport
Switch1(config-if)# ip address 192.168.11.1/24
Switch1(config-if)# exit
```

Шаг 3 Настройте политику MKA (в системе используется политика по умолчанию)

```
Switch1(config)# mka policy mkatest
Switch1(config-mka-policy)# confidentiality-offset 30
Switch1(config-mka-policy)# exit
Switch1(config)#
```

Шаг 4 Настройте интерфейс MKA и включите его

```
Switch1(config)# interface eth-0-24
Switch1(config-if)# mka apply policy mkatest
Switch1(config-if)# mka psk ckn 112233 cak simple abcde1
Switch1(config-if)# macsec desire
Switch1(config-if)# mka priority 11
Switch1(config-if)# mka enable
```

Конфигурация на коммутаторе Switch2

Шаг 5 Выполните аналогичную настройку на Switch2, оставив значение приоритета MKA равным 0 по умолчанию (чем ниже значение, тем выше приоритет)

```
Switch2(config)# interface eth-0-24
Switch2(config-if)# no switchport
Switch2(config-if)# ip address 192.168.11.2/24
Switch2(config-if)# exit
Switch2(config)# mka policy mkatest
Switch2(config-mka-policy)# confidentiality-offset 30
Switch2(config-mka-policy)# exit
Switch2(config)# interface eth-0-24
Switch2(config-if)# mka apply policy mkatest
Switch2(config-if)# mka psk ckn 112233 cak simple abcde1
Switch2(config-if)# macsec desire
Switch2(config-if)# mka enable
```

Шаг 6. Проверка.

Отобразите результат согласования MKA сессии:

```
Switch1# show mka session interface
```

```
Interface eth-0-24:
 Tx-SCI              : 0001 0203 0606 0018
 Priority            : 11
 Capability          : 3
  CKN for participant : 1122 3300 0000 0000 0000 0000 0000 0000
   Key server                    : no
   MI (MN)                       : 40C0 4080 0080 0000 C040 0080 (430)
   Principal actor               : yes
   MKA session status            : succeeded
   Icv mode                      : normal
   Confidentiality offset        : 30 bytes
   Current SAK status            : rx & tx
   Current SAK AN                : 1
   Current SAK Cipher Suite      : gcm-aes-128
   Current SAK KI (KN)           : 0C44 40C8 044C 0404 C440 C484 0000 0002
(2)
   Previous SAK status           : rx
   Previous SAK AN               : 0
   Previous SAK Cipher Suite     : gcm-aes-128
   Previous SAK KI (KN)          : 1000 1040 5011 4000 1100 4000 0000 0001
(1)
   Peer list:
   MI                            MN         Priority Capability Rx-SCI

   0C44 40C8 044C 0404 C440 C484 428        0        3          D85B 2200
0401 0
018

Switch1#
```

```
Switch2# show mka session interface
Interface eth-0-24:
 Tx-SCI              : D85B 2200 0401 0018
 Priority            : 0
 Capability          : 3
  CKN for participant : 1122 3300 0000 0000 0000 0000 0000 0000
   Key server                    : yes
   MI (MN)                       : 0452 0202 4042 5216 1616 5614 (444)
   Principal actor               : yes
   MKA session status            : succeeded
   Icv mode                      : normal
   Confidentiality offset        : 30 bytes
   Current SAK status            : rx & tx
   Current SAK AN                : 0
   Current SAK Cipher Suite      : gcm-aes-128
   Current SAK KI (KN)           : 0452 0202 4042 5216 1616 5614 0000 0001
(1)
```

```
   Previous SAK status             : N/A
   Previous SAK AN                 : N/A
   Previous SAK Cipher Suite       : N/A
   Previous SAK KI (KN)            : N/A
   Peer list:
   MI                              MN          Priority Capability Rx-SCI

   A704 20A2 A203 0287 27A0 A182 414         11       3          0001 0203
0606 0
018

Switch2
```

8 Руководство по настройке функций управления

8.1 Настройка syslog

8.1.1 Общие положения

8.1.1.1 Описание функции

Программное обеспечение для регистрации служебных сообщений может сохранять лог в файл журнала или направлять его на другие устройства. Функция регистрации системных сообщений включает в себя следующие возможности:

- предоставляет информацию для мониторинга и устранения неполадок;
- позволяет выбрать типы информации, которая будет собираться в журнале;
- позволяет выбрать место назначения для собранной информации из журнала.

По умолчанию коммутатор записывает обычные, но важные системные сообщения во внутренний буфер. Вы можете указать, какие системные сообщения следует сохранять. Сообщения снабжены метками времени для повышения эффективности.

Доступ к системным сообщениям, регистрируемым в журнале, можно получить с помощью интерфейса командной строки коммутатора (CLI) или сохранив их на правильно настроенном сервере. Программное обеспечение коммутатора сохраняет сообщения журнала во внутреннем буфере, который может вместить до 1000 сообщений. Вы можете удаленно отслеживать системные сообщения, подключившись к коммутатору через Telnet, либо просматривая журналы на сервере Syslog.

8.1.1.2 Основные термины и команды

Наименование	Описание
Logging	Текущая конфигурация ведения журнала
Show	Показать конфигурацию логирования
Levels	Информация об уровне критичночсти
Enable	Включить запись лога в локальный файл
Disable	Отключить запись лога в локальный файл

Таблица 11 – Типы системных сообщений

Наименование	Описание
kern	Сообщения ядра
user	Случайные сообщения пользовательского уровня
mail	Почтовая система
auth	Сообщения безопасности/авторизации
syslog	Сообщения, генерируемые внутри системы syslog
news	Подсистема сетевых новостей
uucp	Подсистема UUCP
cron	Встроенное системное время
authpriv	Сообщения безопасности/авторизации (личные)
ftp	Агент FTP

Таблица 12 – Уровни критичности

Наименование	Описание
emergency	Система вышла из строя
alert	Необходимо незамедлительно принять меры
critical	Критическое событие
error	Ошибка
warning	Предупреждение
notice	Уведомление
information	Информация
debug	Сообщения уровня отладки

8.1.2 Насторйка

8.1.2.1 Настройка сервера логирования

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите сервер логирования и настройте атрибуты

```
Switch(config)# logging server enable
Switch(config)# logging server address 1.1.1.1
Switch(config)# logging server address 2001:1000::2
Switch(config)# logging server severity debug
Switch(config)# logging server facility mail
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show logging
Current logging configuration:
============================================================
logging buffer 500
logging timestamp bsd
logging file enable
logging level file warning
logging level module debug
logging server enable
logging server severity debug
logging server facility mail
logging server address 1.1.1.1
logging server address 2001:1000::2
logging alarm-trap enable
logging alarm-trap level middle
logging merge enable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable
```

8.1.2.2 Настройка размера буфера для логирования

По умолчанию количество сообщений, записываемых в буфер логирования, составляет 500. При желании вы можете установить это число в диапазоне от 10 до 1000.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите размер буфера для логирования.

```
Switch(config)# logging buffer 700
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show logging
Current logging configuration:
============================================================
logging buffer 700
logging timestamp bsd
logging file enable
logging level file warning
logging level module debug
logging server enable
logging server severity debug
logging server facility mail
logging server address 1.1.1.1
logging alarm-trap enable
logging alarm-trap level middle
logging merge enable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable
```

NOTE При настройке серверов Syslog убедитесь, что кабели подключены правильно и два компьютера могут пинговать друг друга. Прежде чем отправлять сообщения системного журнала на сервер, необходимо предварительно настроить программное обеспечение Syslog.

8.2 Настройка зеркалирования

8.2.1 Общие положения

8.2.1.1 Описание функции

Функция зеркалирования позволяет отправлять копии пакетов, проходящих через порты/VLAN, на один или несколько указанных интерфейсов. Также возможно отправлять копии процессору и сохранять их в памяти или файлах.

Копии пакетов используются для анализа и отладки. Функция зеркалирования не влияет на исходный сетевой трафик.

8.2.1.2 Основные понятия и термины

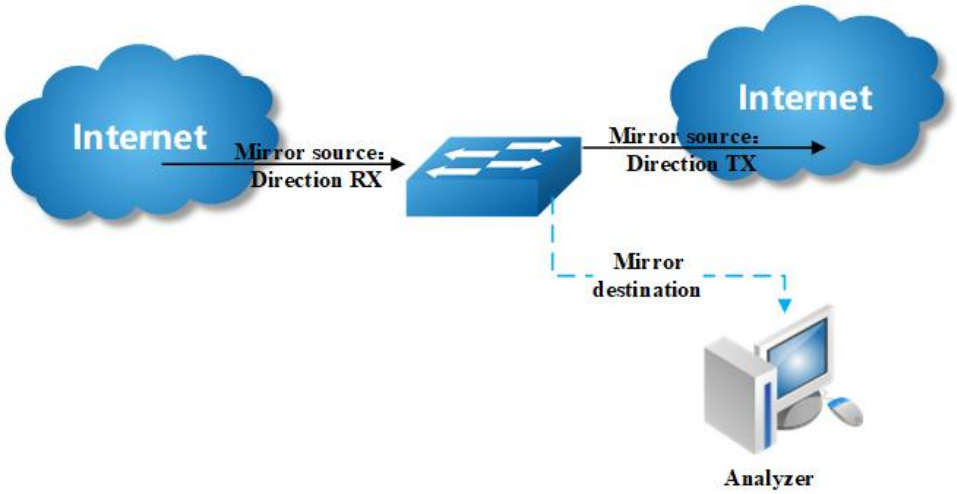


Рисунок 42 – Зеркалирование

1. Сессия зеркалирования

Связь между целевым портом и одним или несколькими портами источниками трафика. Устройство поддерживает до 3 сессий зеркалирования.

Сессии не мешают нормальной работе коммутатора. Однако перегрузка зеркального порта, например, порта 10 Гбит/с, зеркалирующего порт 100 Гбит/с, приводит к потере пакетов.

2. Направление зеркалирования

Устройство поддерживает настройку направления зеркального трафика, доступны 3 варианта на выбор: TX/RX/BOTH.

Зеркалирование приема (RX): позволяет отслеживать как можно больше пакетов, полученных исходным интерфейсом или VLAN, до того, как коммутатор выполнит какие-либо изменения или обработку. Копия каждого пакета, полученного источником (за исключением следующих пакетов: BPDU, LACPDU, BMGPDU, пакетов, отброшенных проверкой привязки IP-MAC на основе VLAN, пакетов с ошибками CRC), отправляется на целевой порт. Пакеты, измененные из-за маршрутизации, копируются без изменений; то есть копируется исходный пакет. Пакеты, измененные из-за качества обслуживания (QoS) — например, измененная точка кода дифференцированного обслуживания (DSCP) — копируются с изменениями. Пакеты, измененные из-за трансляции VLAN или классификации VLAN, копируются с изменениями. Некоторые функции, которые могут привести к потере пакета во время обработки приема, не влияют на зеркалирование, и целевой порт может получить копию пакета, даже если фактический входящий пакет был потерян. К таким функциям относятся: ACL входящего трафика, фильтр входящего трафика VLAN, MAC-

фильтр, STP, управление тегами VLAN, безопасность портов, неизвестные маршрутизируемые пакеты.

Зеркалирование передачи (TX): позволяет отслеживать как можно больше пакетов, отправленных исходным интерфейсом после того, как коммутатор выполнит все необходимые модификации и обработку. Копия каждого пакета, отправленного источником, отправляется на порт назначения для данной сессии зеркалирования.

Зеркалирование передачи и прием (BOTH): в режиме зеркалирования вы можете отслеживать как пакеты на приеме, так и на передаче.

3. Источник зеркалирования

Порт источник: интерфейс уровня 2, который необходимо отслеживать. В качестве исходного порта может выступать физический порт или линк-порт агрегации каналов. Порт-участник линка агрегации каналов не поддерживается в качестве зеркального источника.

VLAN источник: VLAN, которую необходимо отслеживать. Перед настройкой VLAN в качестве зеркальной исходной VLAN пользователь должен создать интерфейс VLAN.

ЦП: Пользователь может установить ЦП в качестве источника зеркалирования для мониторинга пакетов, отправляемых на ЦП или получаемых с него. Копии пакетов, отправляемые по назначению зеркалирования, создаются до обработки cpu-traffic-limit. В настоящее время только 1 сессия поддерживается при использовании ЦП в качестве источника зеркалирования.

4. Направление зеркалирования

Функция зеркалирования скопирует пакеты и отправит копии в место назначения. Это могут быть:

Локальный порт: порт назначения должен быть физическим портом или портом агрегации каналов; порт, входящий в состав порта агрегации каналов, не поддерживается. Порт назначения должен обладать следующими характеристиками:

- расположен на том же коммутаторе, что и исходный порт;
- не отключен;
- может участвовать только в одной зеркальной сессии (порт назначения в одной зеркальной сессии не может быть портом назначения во второй зеркальной сессии);
- это не может быть порт-источник сессии зеркалирования;
- порт не передает никакой другой трафик;
- не участвует в построении связующего дерева STP.

Порт во VLAN: целевой VLAN, в которой добавлен целевой порт. Копии пакетов должны отправляться на указанный порт с добавлением тега нужной VLAN.

- диапазон VLAN должен быть от 2 до 4094. Если VLAN не создан в системе, пользователь не сможет настроить этот VLAN для зеркалирования;

- исходящий порт должен быть физическим портом. Пользователь должен вручную проверить, может ли исходящий порт передавать зеркалированные пакеты;

- в пакеты мониторингового трафика добавляется метка с идентификатором VLAN, и они направляются через указанный исходящий порт на целевое устройство.

ЦП: отправка копий пакетов на ЦП устройства. Если анализатор недоступен, пользователь может использовать ЦП в качестве адреса назначения и сохранить результат для дальнейшего анализа пакетов. Поддерживается вывод пакетов с CPU через CLI и запись пакетов в текстовый файл. Зеркалирование не влияет на коммутацию сетевого трафика на исходных портах или исходных VLAN; копия пакетов, полученных или отправленных исходными интерфейсами, отправляется на CPU без изменений. Можно настроить ограничение скорости такого трафика для CPU. CPU может участвовать в качестве устройства назначения только в одной сессии зеркалирования session.

8.2.2 Настройка

8.2.2.1 Настройка зеркалирования локальных портов

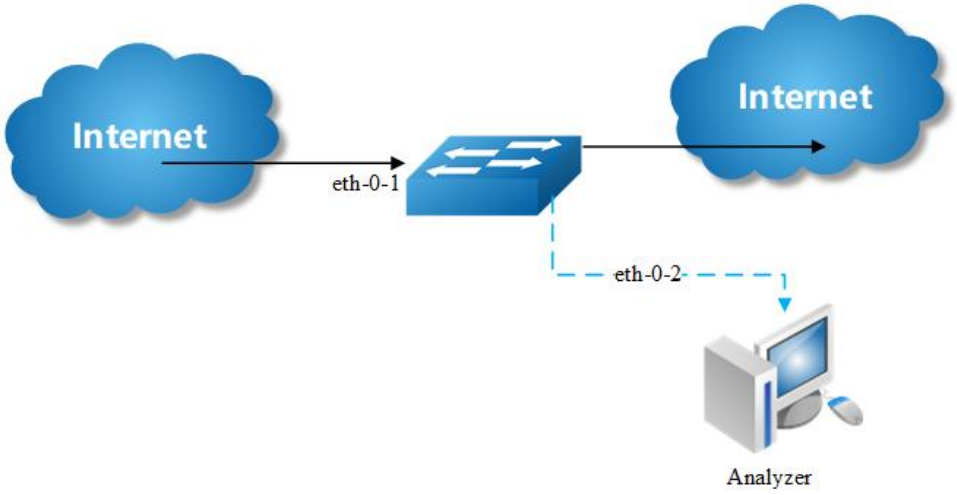


Рисунок 43 – Зеркалирование портов

Скопируйте пакеты с eth-0-1 и отправьте их на eth-0-2

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Укажите место назначения зеркалирования.

```
Switch(config)# interface eth-0-2
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# monitor session 1 destination interface eth-0-2
```

Шаг 3. Установите источник зеркалирования.

```
Switch(config)# monitor session 1 source interface eth-0-1 both
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

```
Switch# show monitor session 1
Session   1
----------
Status              : Valid
Type                : Local Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              : eth-0-1
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both              :
Destination Port    : eth-0-2
```

8.2.2.2 Настройка локального зеркалирования VLAN

Скопируйте пакеты из VLAN 10 и отправьте их на eth-0-2.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Укажите место назначения зеркалирования.

```
Switch(config)# interface eth-0-2
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# monitor session 1 destination interface eth-0-2
```

Шаг 3. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
```

Шаг 4. Создайте интерфейс VLAN.

```
Switch(config)# interface vlan10
Switch(config-if)# exit
```

Шаг 5. Установите источник зеркалирования.

```
Switch(config)# monitor session 1 source vlan 10 rx
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.n

```
Switch# show monitor session 1
Session   1
----------
Status              : Valid
Type                : Local Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              :
Source VLANs        :
  Receive Only      : 10
  Transmit Only     :
  Both              :
Destination Port    : eth-0-2
```

8.2.2.3 Настройка ЦП в качестве источника зеркалирования

Скопируйте пакеты с ЦП и отправьте их на eth-0-2.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Укажите место назначения зеркала.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# monitor session 1 destination interface eth-0-2
```

Шаг 3. Установите источник.

```
Switch(config)# monitor session 1 source cpu both
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

```
DUT1# show monitor session 1
Session   1
----------
Status              : Valid
Type                : Cpu Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              : cpu
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both              :
Destination Port    :eth-0-1
```

8.2.2.4 Настройка зеркалирования к нескольким адресатам Скопируйте пакеты с eth-0-1 и отправьте их на eth-0-2 и eth-0-3

Правила зеркалирования источника такие же, как и для одного целевого порта.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Укажите группу назначения для зеркала.

```
Switch(config)# interface eth-0-2
Switch(config-if)# no shutdown
```

```
Switch(config-if)# exit
Switch(config)# interface eth-0-3
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# monitor session 1 destination group 1
Switch(config-monitor-d-group)# member eth-0-2
Switch(config-monitor-d-group)# member eth-0-3
Switch(config-monitor-d-group)# exit
```

Шаг 3. Установите источник зеркалирования.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# monitor session 1 source interface eth-0-1
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

```
Session   1
----------
Status              :  Valid
Type                :  Local Session
Source Ports       :
  Receive Only      :
  Transmit Only     :
  Both              : eth-0-1
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both              :
Destination Port    : eth-0-2 eth-0-3
```

8.2.2.5 Настройка удалённого адресата сессии зеркалирования

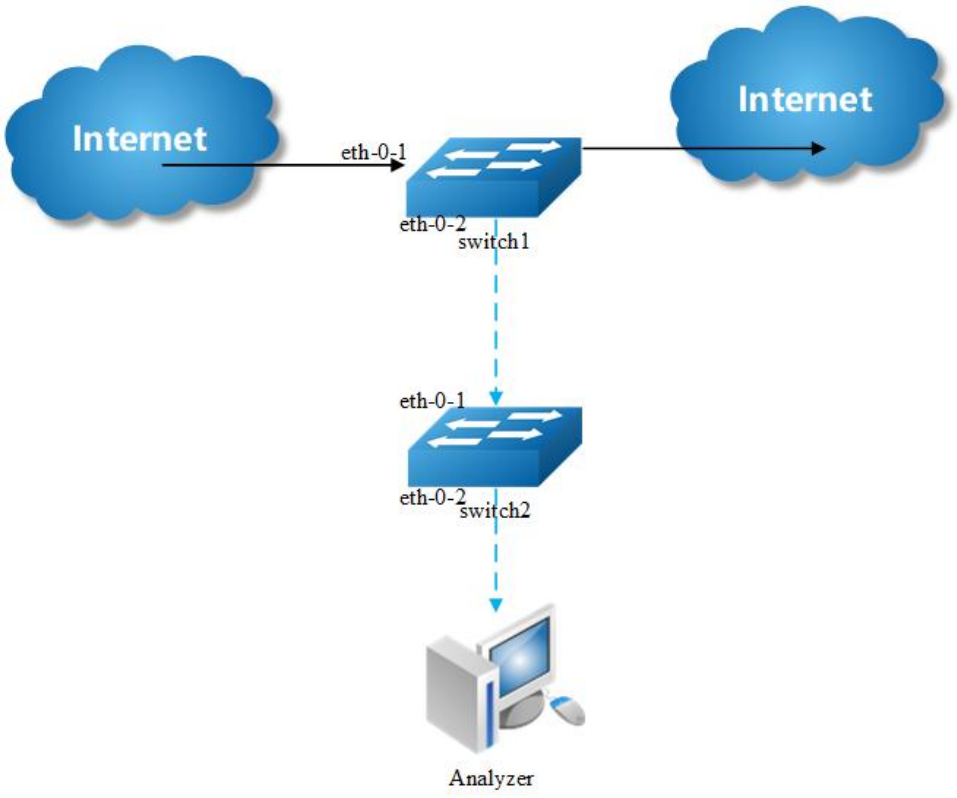


Рисунок 44 – Зеркалирование к удаленному ПК

Если локальное устройство не может напрямую подключиться к анализатору, пользователь может выбрать отправку копий пакетов с указанным тегом VLAN к удаленному устройству.

В следующем примере пакеты копируются с интерфейса eth-0-1 коммутатора Switch1 и отправляются на коммутатор Switch2 через интерфейс eth-0-2 коммутатора Switch1. Коммутатор Switch2 отправляет эти пакеты анализатору.

Конфигурация коммутатора Switch1:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Укажите место назначения для зеркала.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 15
Switch(config-vlan)# exit
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# no shutdown
```

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# exit
Switch(config)# monitor session 1 destination remote vlan 15 interface eth-0-
2
```

Шаг 3. Установите источник для зеркала.

```
Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config)# monitor session 1 source interface eth-0-1 both
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

```
SwitchA# show monitor session 1
Session   1
----------
Status              : Valid
Type                 :  Remote Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both                : eth-0-1
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both                :
Destination Port    : eth-0-2
Destination remote VLAN : 15
```

Конфигурация коммутатора Switch2:

Используйте эти методы на коммутаторе Switch2 для отправки пакетов анализатору через eth-0-2.

Метод 1: Использовать VLAN 15 в качестве источника зеркалирования, eth-0-2 в качестве назначения.

```
Switch # configure terminal
Switch (config)# vlan database
Switch (config-vlan)# vlan 15
Switch (config-vlan)# exit
```

```
Switch (config)# interface vlan15
Switch (config-if)# exit

Switch (config)# interface eth-0-2
Switch (config-if)# no shutdown

Switch (config)# interface eth-0-1
Switch (config-if)# no shutdown
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan add 15
Switch (config-if)# exit

Switch (config)# monitor session 1 destination interface eth-0-2
Switch (config)# monitor session 1 source vlan 15 rx
Switch (config)# end
```

Метод 2: Добавить оба порта в один и тот же VLAN (15) и настроить рассылку пакетов в этом VLAN.

```
Switch# configure terminal

Switch(config)# no spanning-tree enable

Switch(config)# vlan database
Switch(config-vlan)# vlan 15
Switch(config-vlan)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 15

Switch(config)# interface eth-0-1
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# exit
```

NOTE В данной конфигурации метка VLAN удаляется, поскольку eth-0-2 является портом доступа.

Метод 3: Рассылка во VLAN с сохранением тега VLAN 15.

Если пользователю необходимо сохранить тег VLAN 15, порт eth-0-2 должен быть транковым: (остальные настройки аналогичны методу 2)

```
Switch(config)# interface eth-0-2
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
```

8.2.2.6 Настройка зеркалирования в сторону CPU

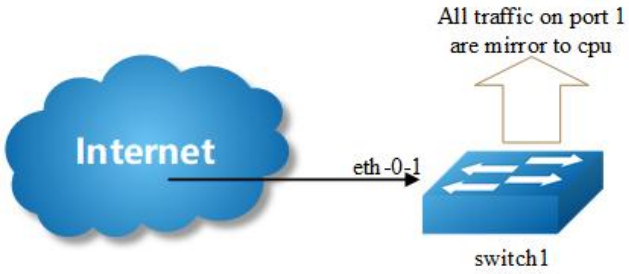


Рисунок 45 – Зеркалирование к CPU

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Укажите место назначения зеркала.

```
Switch(config)# monitor session 1 destination cpu
```

Установите размер буфера и значение, соответствующее частоте процессора:

```
Switch(config)# monitor cpu set packet buffer 100
Switch(config)# cpu-traffic-limit reason mirror-to-cpu rate 128
```

Шаг 3. Установите источник зеркального отображения.

```
Switch(config)# monitor session 1 source interface eth-0-1 both
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Дополнительные шаги

Включите или отключите запись пакетов в файлы флэш-памяти.

```
Switch# monitor cpu capture packet start
Switch# monitor cpu capture packet stop
```

Обменяйте файлы с расширения *.txt на *.pcap

```
Switch# pcap convert flash:/mirror/MirCpuPkt-2016-02-05-18-31-13.txt
flash:/MirCpuPkt-2016-02-05.pcap
```

Укажите действие после превышения размера буфера пакетов: «drop» отбросить последний пакет; «replace» отбросить самый старый пакет.

```
Switch(config)# monitor cpu capture strategy drop
Switch(config)# monitor cpu capture strategy replace
```

Шаг 5. Проверка.

В этом примере показано, как настроить зеркальную сессию (сессия 1) для мониторинга трафика с исходного порта на процессор. Для просмотра конфигурации можно использовать команду «show monitor session».

```
Switch# show monitor session 1
DUT1# show monitor session 1
Session   1
----------
Status              : Valid
Type                : Cpu Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              : eth-0-1
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both              :
Destination Port    : cpu
```

Отобразить пакеты зеркалируемые на процессор:

```
Switch# show monitor cpu packet all
-----------------show all mirror to cpu packet info-----------------
packet: 1
Source port: eth-0-1
MACDA:264e.ad52.d800, MACSA:0000.0000.1111
vlan tag:100
IPv4 Packet, IP Protocol is 0
IPDA:3.3.3.3, IPSA: 10.0.0.2
Data length: 47
Data:
 264e ad52 d800 0000 0000 1111 8100 0064
 0800 4500 001d 0001 0000 4000 6ad9 0a00
 0002 0303 0303 6365 6e74 6563 796f  75
```

Отобразить размер буфера зеркала:

```
Switch# show monitor cpu packet buffer
--------------------show packet buffer size ---------------------
The mirror-to-cpu packet buffer size of user set is: 100
```

Отобразить лимит для зеркального трафика на ЦП:

```
Switch# show cpu traffic-limit | include mirror-to-cpu
mirror-to-cpu               128           0
```

Отобразить файлы флэш-памяти:

```
Switch# ls flash:/mirror
Directory of flash:/mirror

total 8
-rw-r-----  1 2287 Dec 23 01:16 MirCpuPkt-2016-12-23-01-15-54.txt
-rw-r-----  1 2568 Jan  3 11:41 MirCpuPkt-2017-01-03-11-41-33.txt
14.8T bytes total (7.9T bytes free)

Switch# more flash:/mirror/ MirCpuPkt-2017-01-03-11-41-33.txt
sequence  srcPort
1          eth-0-1
++++++++1483443444:648884
8c 1d cd 93 51 00 00 00 00 00 11 11 08 00 45 00
00 26 00 01 00 00 40 00 72 d0 01 01 01 01 03 03
03 03 63 65 6e 74 65 63 79 6f 75 63 65 6e 74 65
63 79 6f 75
--------
sequence  srcPort
2          eth-0-1
++++++++1483443445:546440
8c 1d cd 93 51 00 00 00 00 00 11 11 08 00 45 00
00 26 00 01 00 00 40 00 72 d0 01 01 01 01 03 03
03 03 63 65 6e 74 65 63 79 6f 75 63 65 6e 74 65
63 79 6f 75
```

Файлы *.pcap можно открыть с помощью программ анализа пакетов, таких как Wireshark.

Для загрузки файлов обратитесь к разделам «ftp» и «tftp».

```
Switch#ls flash:/mirror
Directory of flash:/mirror

total 12
-rw-r-----  1 2287 Dec 23 01:16 MirCpuPkt-2016-12-23-01-15-54.txt
-rw-r-----  1 2568 Jan  3 11:41 MirCpuPkt-2017-01-03-11-41-33.txt
-rw-r--r--  1  704 Jan  3 13:07 test.pcap
14.8T bytes total (7.9T bytes free)
```

Отобразить действия после заполнения буфера

```
Switch# show monitor cpu capture strategy
The capture strategy of cpu mirror is: replace (add new packet and remove
oldest
 packet when buffer is full)
```

8.3 Интерфейсы управления устройством

8.3.1 Общие положения

8.3.1.1 Описание функции

Пользователь может управлять коммутатором через порт управления. Коммутатор имеет два порта управления: порт Ethernet и консольный порт.

8.3.2 Настройка

8.3.2.1 Настройка консольного порта для управления

Параметры консоли коммутатора по умолчанию следующие:

- скорость передачи данных составляет 115200.
- количество бит данных 8.
- стоп-биты 1.
- для четности установлено значение «нет».

Прежде чем подключить ПК или терминал к консольному порту, настройте соединение согласно параметрам выше. После входа в коммутатор вы можете изменить параметры консоли.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки «line console» и установите скорость консоли.

```
Switch(config)# line console 0
Switch(config-line)# speed 19200
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config-line)# end
```

Шаг 4. Проверка.

После выполнения вышеуказанных настроек будет необходимо обновить скорость консоли в ПК или терминала с 115200 до 19200, чтобы она соответствовала новому параметру, после чего настройка коммутатора через консольный порт станет возможной.

8.3.2.2 Настройка внешнего порта Ethernet для управления.

Для управления устройством через порт Ethernet необходимо сначала настроить управляющий IP-адрес через консольный порт.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка адреса управления коммутатором.

```
Switch(config)# management ip address 10.10.38.106/24
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show management ip address
  Management IP address is:  10.10.38.106/24
  Gateway: 0.0.0.0
```

8.3.2.3 Настройка порогов рабочей температуры

Коммутатор поддерживает управление сигналами тревоги о температуре работы. Можно настроить три температурных порога: низкий, высокий и критический. Если температура ниже низкого порога или выше высокого порога, будет выдан сигнал-сообщение тревоги. Если температура коммутатора выше критического порога, устройство автоматически отключит питание.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка температурного порога.

5℃ для низкого уровня; 70℃ для высокого уровня; 90℃ для критического уровня.

```
Switch(config)# temperature 5 70 90
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show environment
-------------------------------------------------------
Sensor status (Degree Centigrade):
```

```
Index Temperature  Lower_alarm  Upper_alarm Critical_limit
1     50           5            70          90
```

8.3.2.4 Вентиляторы охлаждения

Поддерживается автоматическое управление вентилятором охлаждения. В случае отказа вентилятора или отсутствия вентиляционного блока устройство подаст сигнал тревоги. Если вентиляционный блок поддерживает регулировку скорости, устройство может регулировать скорость вентилятора в зависимости от температуры. Устройство имеет три температурных порога: Tlow = 50, Thigh = 65 и Tcrit = 80 градусов Цельсия. Если температура < Tlow, вентилятор остановится; если Tlow <= температура < Thigh, вентилятор будет работать на 30% скорости; если Thigh <= температура < Tcrit, вентилятор будет работать на 70% скорости; если Tcrit >= температура, вентилятор будет работать на 100% скорости. Шаг для смены режимов – 2 градуса (Thyst). Если температура ранее превысила значения Tlow, Thigh или Tcrit, то для снижения скорости вращения вентилятора температура должна опуститься ниже соответствующих значений Thyst (Tlow-Thyst, Thigh-Thyst или Tcrit-Thyst). Например:

- температура составляет 58 градусов Цельсия, скорость вращения вентилятора — 30% (Tlow<58<Thigh).
- температура повышается до 65 градусов Цельсия, скорость вращения вентилятора составляет 70% (температура на уровне 65).
- температура понижается до 63 градусов Цельсия, скорость вращения вентилятора по-прежнему составляет 70% .
- температура понижается до 62 градусов Цельсия, скорость вращения вентилятора составляет 30%.

Значения Tlow, Thigh, Tcrit, Thyst и скорость вращения вентилятора для каждого температурного порога заданы жестко и не могут быть изменены.

```
Switch# show environment
Fan tray status:
Index     Status
1         PRESENT
FanIndex   Status SpeedRate Mode
1-1         OK      30%      Auto
1-2         OK      30%      Auto
1-3         OK      30%      Auto
1-4         OK      30%      Auto
-------------------------------------------------------
```

8.3.2.5 Питание коммутатора

Коммутатор поддерживает автоматическое управление состоянием питания. При отключении питания или неисправности работающего вентилятора устройство подаст сигнал тревоги. При отключении или подключении питания также уведомит пользователя.

Пользователь может отобразить состояние питания для проверки его работоспособности.

```
Switch# show environment
-------------------------------------------------------
Power status:
Index      Status     Power      Type       Fans       Control
1          PRESENT    OK         AC         -          -
2          ABSENT     -          -          -          -
3          PRESENT    OK         DC(PoE)    -          -
-------------------------------------------------------
```

8.3.2.6 Отображение данных о работе оптических приемо-передатчиков

Коммутатор поддерживает управление информацией о трансивере, которая включает основные и диагностические данные. Основные данные включают тип трансивера, название производителя, PN, S/N, длину волны и длину линии связи для поддерживаемых типов. Диагностические данные включают температуру, напряжение, ток, мощность оптического сигнала передачи, мощность оптического сигнала приема и пороговые значения для этих величин. Если при подключении или удалении трансивера параметры выходят за пределы пороговых значений, коммутатор уведомит пользователя.

Пользователь может отобразить информацию о приемопередатчике для проверки:

```
Switch# show transceiver detail
Port eth-1-2 transceiver info:
Transceiver Type: 10G Base-SR
Transceiver Vendor Name : OEM
Transceiver PN          : SFP-10GB-SR
Transceiver S/N         : 201033PST1077C
Transceiver Output Wavelength: 850 nm
Supported Link Type and Length:
      Link Length for 50/125um multi-mode fiber: 80 m
      Link Length for 62.5/125um multi-mode fiber: 30 m
-----------------------------------------------------------------------------
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
The threshold values are calibrated.
-----------------------------------------------------------------------------
             High Alarm   High Warn   Low Warn    Low Alarm
Temperature   Threshold    Threshold    Threshold     Threshold
```

```
Port   (Celsius)       (Celsius)      (Celsius)      (Celsius)       (Celsius)
--------- ------------------  ----------  ----------  ----------  ----------
eth-1-2  25.92        95.00          90.00       -20.00         -25.00
-------------------------------------------------------------------------------
---------------------
                   High Alarm    High Warn    Low Warn     Low Alarm
       Voltage     Threshold     Threshold    Threshold     Threshold
Port     (Volts)       (Volts)        (Volts)       (Volts)        (Volts)
--------- ----------------- ----------------  ----------------  -------------
--  ---------------
eth-1-2   3.32         3.80          3.70         2.90           2.80
-------------------------------------------------------------------------------
----------------------
                    High Alarm    High Warn    Low Warn     Low Alarm
         Current     Threshold     Threshold    Threshold     Threshold
Port    (milliamperes)   (mA)          (mA)         (mA)          (mA)
--------- ------------------  ---------------  ----------------  ------------
-----  -------------
eth-1-2    6.41         20.00        18.00        1.00            0.50
-------------------------------------------------------------------------------
------------------------
        Optical       High Alarm    High Warn    Low Warn     Low Alarm
     Transmit Power    Threshold     Threshold    Threshold     Threshold
Port    (dBm)           (dBm)         (dBm)          (dBm)         (dBm)
--------- ------------------  ---------------  ----------------  ------------
----  ---------------
eth-1-2    -2.41         2.01         1.00          -6.99          -7.96
-------------------------------------------------------------------------------
-------------------------
        Optical       High Alarm    High Warn     Low Warn     Low Alarm
     Receive Power     Threshold     Threshold     Threshold     Threshold
Port     (dBm)           (dBm)         (dBm)          (dBm)         (dBm)
--------- ------------------  ---------------  -----------------  -----------
-----  ----------------
eth-1-2     -12       -     1.00         0.00         -19.00       -20.00
-------------------------------------------------------------------------------
-------------------------
```

8.3.2.7 Обновление образа начальной загрузки

Коммутатор поддерживает обновление образа во время работы системы. После обновления необходимо перезагрузить коммутатор, чтобы изменения вступили в силу.

Шаг 1. Скопируйте файл загрузочного образа во флэш-память.

```
Switch# copy mgmt-if tftp://10.10.38.160/bootrom.bin flash:/boot/
```

Шаг 2. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 3. Обновите образ.

```
Switch(config)# update bootrom flash:/boot/bootrom.bin
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Перезагрузите систему.

```
Switch# reboot
```

Шаг 6. Проверка.

После выполнения указанных выше настроек вы сможете отобразить информацию о версии uboot:

```
Switch# show version
……
EPLD Version is 1
BootRom Version is 3.0.2
```

8.4 Настройка Bootrom

8.4.1 Общие положения

8.4.1.1 Описание функции

Основная функция Bootrom — инициализация старта аппаратной платы и загрузка образа ПО системы. В режиме Bootrom можно использовать некоторые служебные команды.

Bootrom может загружать образ системы как с TFTP-сервера, так и с постоянного носителя, например, ПЗУ. Можно настроить IP-адрес коммутатора и TFTP-сервера в режиме Bootrom для загрузки образа системы.

8.4.2 Настройка

8.4.2.1 Настройка загрузки с TFTP-сервера

Шаг 1: Загрузка системы с TFTP-сервера.

Сохраните конфигурацию и перезагрузите систему:

```
bootrom:> setenv bootcmd boot_tftp OS-ms-v3.1.9.it.r.bin
bootrom:> saveenvbootrom:> reset
```

Шаг 2: Загрузка системы с TFTP-сервера без пароля

Сохраните конфигурацию и перезагрузите систему:

```
bootrom:> setenv bootcmd boot_tftp_nopass OS-ms-v3.1.9.it.r.bin
bootrom:> saveenvbootrom:> reset
```

Шаг 3: Загрузите систему с TFTP-сервера и выполните автоматическую перезагрузку.

```
bootrom:> boot_tftp OS-ms-v3.1.9.it.r.bin
```

Шаг 4: Загрузите систему с TFTP-сервера и выполните автоматическую перезагрузку без пароля.

```
bootrom:> boot_tftp_nopass OS-ms-v3.1.9.it.r.bin
```

Проверка.

После выполнения указанных выше настроек отобразится следующая информация:

```
bootrom:> reset
……..
TFTP from server 10.10.29.160; our IP address is 10.10.29.118
Filename 'OS-ms-v3.1.9.it.r.bin'.
Load address: 0xaa00000
Loading: octeth0: Up 100 Mbps Full duplex (port  0)
#################################################################
####################
done
Bytes transferred = 12314539 (bbe7ab hex), 1829 Kbytes/sec
```

8.4.2.2 Настройка загрузки из FLASH-памяти

Шаг 1. Загрузите систему с флеш-накопителя.

Сохраните конфигурацию и перезагрузите систему:

```
bootrom:> setenv bootcmd boot_flash OS-ms-v3.1.9.it.r.bin
bootrom:> saveenvbootrom:> reset
```

Шаг 2. Загрузите систему без пароля.

Сохраните конфигурацию и перезагрузите систему:

```
bootrom:> setenv bootcmd boot_flash_nopass OS-ms-v3.1.9.it.r.bin
bootrom:> saveenvbootrom:> reset
```

```
Do you want to revert to default config file ? [Y|N|E]:Y
```

Шаг 3. Загрузите систему с флеш-накопителя и выполните автоматическую перезагрузку.

```
bootrom:> boot_flash OS-ms-v3.1.9.it.r.bin
```

Шаг 4. Загрузите систему с флеш-накопителя и перезагрузите её автоматически без пароля.

```
bootrom:> boot_flash_nopass OS-ms-v3.1.9.it.r.bin
Do you want to revert to default config file ? [Y|N|E]:Y
```

Шаг 5. Проверка.

После выполнения указанных выше настроек отобразится следующая информация:

```
bootrom:> reset
……
Do you want to  revert  to the default config file ? [Y|N|E]:Y
### JFFS2 loading '/boot/OS-ms-v3.1.9.it.r.bin' to 0xaa00000
Scanning JFFS2 FS: . done.
### JFFS2 load complete: 12314539 bytes loaded to 0xaa00000
## Booting image at 0aa00000 ...
   Verifying Checksum ... OK
   Uncompressing Kernel Image ... OK
……
```

8.4.2.3 Установка загрузочного IP-адреса коммутатора

Шаг 1. Установите IP-адрес коммутатора.

```
bootrom:> setenv ipaddr 10.10.29.101
bootrom:> saveenv
```

Шаг 2. Укажите IP-адрес TFTP-сервера.

```
bootrom:> setenv serverip 10.10.29.160
bootrom:> saveenv
```

Шаг 3 Проверка.

Отобразите информацию о конфигурации:

```
bootrom:> printenv
printenv
bootdelay=5
```

```
baudrate=9600
download_baudrate=9600
……
stderr=serial
ipaddr=10.10.29.101
serverip=10.10.29.160
Environment size: 856/2044 bytes
```

8.4.2.4 Обновление загрузочного образа Bootrom

Шаг 1. Обновите образ Bootrom с TFTP-сервера.

```
bootrom:> upgrade_uboot bootrom.bin
```

Шаг 2 Проверка.

```
bootrom:> version
versionBootrom 3.0.3 (Development build)
(Build time: Aug 4 2011 - 11:47:06)
```

8.4.2.5 Установить IP-адрес шлюза

Шаг 1. Установите IP-адрес шлюза коммутатора

```
bootrom:> setenv gatewayip 10.10.37.1
bootrom:> saveenv
```

Шаг 2. Установите сетевую маску

```
bootrom:> setenv netmask 255.255.255.0
bootrom:> saveenv
```

Шаг 3 Проверка.

```
bootrom:> printenv
printenv
bootdelay=5
baudrate=9600
download_baudrate=9600
……
stderr=serial
gatewayip=10.10.38.1
netmask=255.255.255.0
Environment size: 856/2044 bytes
```

8.5 Обновление ПО

8.5.1 Общие положения

Называют этот процесс по-разному - «обновлением прошивки», «обновлением версии» или «обновлением образа». ПО коммутатора описывает работу всех основных функции. В ходе технического обслуживания и развития, ПО регулярно обновляется и включает в себя новые функции, оптимизацию существующих функций или исправления ошибок. Поэтому рекомендуется пользователям использовать последнюю официальную версию. Обновление прошивки включает в себя два этапа: загрузку прошивки и применение.

8.5.2 Настройка

Обновление версии прошивки коммутатора можно выполнить через веб или с помощью командной строки. В качестве примера рассмотрим работу с командной строкой и обновление по TFTP.

Шаг 1. Настройте IP-адрес сетевой карты компьютера

Настройте IP-адрес 192.168.1.101 и маску 255.255.2555.0 для сетевой карты компьютера. Проверьте связь между коммутатором и компьютером.

Шаг 2. Войдите в режим конфигурации

```
Switch#configure terminal
```

Шаг 3. Настройте IP-адрес порта управления коммутатора.

По умолчанию все порты коммутатора являются членами VLAN 1. Для обеспечения связи между ними необходимо настроить IP-адрес VLAN 1 таким образом, чтобы он находился в том же сетевом сегменте, что и IP-адрес соответствующей сетевой карты на ПК.

```
Switch(config)# management ip address 192.168.1.1/24
```

Шаг 4. Прооверка связи при помощи ping

```
Switch# ping mgmt-if 192.168.1.101
ping: Warning: source address might be selected on device other than:
MANG_VRF
PING 192.168.1.101 (192.168.1.101) from 192.168.1.1 MANG_VRF: 56(84) bytes of
data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=128 time=0.607 ms
```

```
64 bytes from 192.168.1.101: icmp_seq=2 ttl=128 time=0.839 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=128 time=0.288 ms
64 bytes from 192.168.1.101: icmp_seq=4 ttl=128 time=0.790 ms
64 bytes from 192.168.1.101: icmp_seq=5 ttl=128 time=0.818 ms

--- 192.168.1.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4039ms
rtt min/avg/max/mdev = 0.288/0.668/0.839/0.207 ms
Switch#
```

Шаг 5. Включите службу TFTP на ПК

Запустите на своем ПК инструмент TftpServer (например, "Tftpd32"), на нем есть возможность передачи данных по протоколу TFTP. Поместите файл прошивки (образ), который необходимо загрузить в коммутатор, в каталог, и укажите к нему путь службе TFTP.

Шаг 6. Загрузите прошивку на коммутатор.

```
Switch# copy 329gmt.-if tftp://192.168.1.101/hos-vastlakes-v3.0.20.bin
flash:/boot/hos-vastlakes-v3.0.20.bin
```

Примечание: Прошивка (образ) должна быть сохранена в каталоге flash/boot.

Шаг 7. Настройте запуск с новой прошивкой.

```
Switch # boot system flash:/boot/hos-vastlakes-v3.0.20.bin
```

Нажмите Enter еще раз для подтверждения.

```
Are you sure to use flash:/boot/hos-vastlakes-v3.0.20.bin as the next boot
image? [confirm]
```

Шаг 8. Перезагрузите коммутатор для использования загруженной прошивки (ПО).

```
switch5# reboot
Building configuration...
Reboot system? [confirm]
```

8.6 Лог перезагрузки

8.6.1 Общие положения

8.6.1.1 Описание функции

Коммутатор поддерживает отображение лога перезагрузки. На основе этих данных пользователь может определить причины перезагрузки коммутатора. Причины перезагрузки могут включать как ручную перезагрузку, выключение питания так и другие причины.

Поддерживается хранение не более 50 записей. Термины и описания приведены в таблице:

Тип перезагрузки	Описание
POWER	Отключения электроэнергии
MANUAL	Команда CLI «reboot/reload».
HIGH-TMPR	Перезагрузка при аномально высокой температуре.
BHMDOG BHM	Таймер, функциональный модуль мониторинга
LCMDOG LCM	Таймер, контролирующий каждый LC
SCHEDULE	Запланированный перезапуск
SNMP-RELOAD	SNMP перезагрузка
HALFAIL	Перезапуск для связи HAGT с HSRV
ABNORMAL	Необычная перезагрузка, системный сбой ядра
CTCINTR	Кнопка перезагрузки
LCATTACH	Переподключенияе LC - CHSM
OTHER	Перезагрузка по неописанной причине

8.6.2 Настройка

Лог перезагрузки включен по умолчанию. Пользователь может просмотреть журнал командой:

Шаг 1. Отобразить журнал

```
Switch# show reboot-info
Times      Reboot Type     Reboot Time (UTC)
----------+---------------+--------------------
1          MANUAL          2023-01-04 20:54:22
2          MANUAL          2023-01-04 21:00:30
3          MANUAL          2023-01-04 21:06:53
4          MANUAL          2023-01-04 21:10:13
5          MANUAL          2023-01-04 21:14:16
6          MANUAL          2023-01-04 21:20:50
```

9 Руководство по настройке управления сетью

9.1 Инструменты и механизмы диагностики сети

9.1.1 Общие положения

9.1.1.1 Описание функции

Ping — это утилита для администрирования компьютерных сетей, используемая для проверки доступности хоста в сети IP и измерения времени отклика. Название происходит от терминологии активного гидролокатора.

Ping работает путем отправки пакетов запроса протокола ICMP (Internet Control Message Protocol) целевому хосту и ожидания ответа ICMP. При этом он измеряет время от передачи до приема (время кругового пути) [1] и регистрирует любые потери пакетов. Результаты теста выводятся в виде статистической сводки полученных ответных пакетов, включая минимальное, максимальное и среднее время отклика.

Traceroute — это сетевой инструмент для фиксирования пути следования и времени передачи пакетов в сети.

Программа Traceroute отправляет последовательность пакетов ICMP целевому хосту. Отслеживается и фиксируется каждый из пройденных промежуточных маршрутизаторов.

9.1.2 Настройка

9.1.2.1 Ping IP-адреса с использованием внутреннего порта.

```
Switch# ping 10.10.29.247
```

9.1.2.2 Ping IP-адреса с указанием порта управления.

```
Switch# ping mgmt-if 10.10.29.247
```

9.1.2.3 Ping IP-адреса с использованием VRF.

```
Switch# ping vrf vrf1 10.10.10.1
```

9.1.2.4 Трассировка маршрута к IP-адресу

```
Switch# traceroute 1.1.1.2
```

9.2 Настройка NTP

9.2.1 Общие положения

9.2.1.1 Описание функции

NTP — это сетевой протокол для синхронизации времени. NTP способен синхронизировать часы с точностью до миллисекунд при подключении к локальной сети и с точностью до сотен миллисекунд при подключении к глобальной сети. NTP позволяет пользователю выбирать необходимый ему уровень точности (страту) в дереве. Сервер времени, расположенный выше в дереве (с меньшим номером страты), обеспечивает более высокую вероятность соответствия стандарту времени UTC.

Некоторые хосты выступают в роли серверов-источников времени, то есть предоставляют другим хостам правильное время. Другие хосты выступают в роли клиентов, то есть узнают текущее время, запрашивая его у сервера-источника времени. Некоторые хосты выступают одновременно и в роли клиентов, и в роли серверов-источников времени, поскольку они являются звеньями в цепочке, по которой правильное время передается от одного хоста к другому. В рамках этой цепочки хост сначала выступает в роли клиента, чтобы получить правильное время, затем он, в свою очередь, начинает функционировать как сервер-источник времени, тогда как другие хосты, выступая в роли клиентов, отправляют ему запросы на получение времени.

9.2.2 Настройка

9.2.2.1 Настройка режима «клиент/сервер» для подключения к серверу через внутренний интерфейс.

Перед настройкой NTP-клиента убедитесь, что служба NTP включена на сервере.

Шаг 1. Войдите в режим настройки.

```
Switch#configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и подключитесь к VLAN.

```
Switch(config)# interface eth-0-26
Switch(config-if)# switch access vlan 10
Switch(config-if)# no shutdown
```

```
Switch(config-if)# exit
```

Шаг 4: создайте интерфейс VLAN и задайте IP-адрес.

```
Switch(config)# interface vlan10
Switch(config-if)# ip address 6.6.6.5/24
Switch(config-if)# exit
```

Шаг 5. Настройка атрибутов NTP-клиента.

Включите доверенный ключ; Настройте IP-адрес NTP-сервера; Включите аутентификацию; После включения аутентификации клиентский коммутатор будет отправлять запросы на получение точного времени только на доверенные NTP-серверы; Настройте NTP ACE.

```
Switch(config)# ntp key 1 serverkey
Switch(config)# ntp server 6.6.6.6 key 1
Switch(config)# ntp authentication enable
Switch(config)# ntp trustedkey 1
Switch(config)# ntp ace 6.6.6.6 none
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

```
Switch# show ntp
Current NTP configuration:
============================================================
NTP access control list:
  6.6.6.6 mask 255.255.255.255 none
Unicast peer:
Unicast server:
  6.6.6.6 key 1
Authentication: enabled
Local reference clock:
Disable management interface

Switch# show ntp status
Current NTP status:
============================================================
clock is synchronized
stratum:         7
reference clock: 6.6.6.6
frequency:       17.365 ppm
precision:       2**20
reference time:  d14797dd.70b196a2   ( 1:54:37.440 UTC   Thu Apr  7 2011)
```

```
root delay:       0.787 ms
root dispersion: 23.993 ms
peer dispersion: 57.717 ms
clock offset:    -0.231 ms
stability:        6.222 ppm
Switch# show ntp associations
Current NTP associations:
   remote           refid      st   when poll reach   delay   offset  disp
==============================================================================
*6.6.6.6         127.127.1.0     6   50  128   37      0.778   -0.234  71.945
synchronized, + candidate, # selected, x falsetick, . excess, - outlier
```

9.2.2.2 Настройка клиент-серверного режима подключения от интерфейса управления

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка атрибутов NTP-клиента

```
Switch(config)# ntp key 1 serverkey
Switch(config)# ntp server mgmt-if 192.168.100.101 key 1
Switch(config)# ntp authentication enable
Switch(config)# ntp trustedkey 1
Switch(config)# ntp ace 192.168.100.101 none
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show ntp
Current NTP configuration:
============================================================
NTP access control list:
  192.168.100.101 mask 255.255.255.255 none
Unicast peer:
Unicast server:
  192.168.100.101(mgmt-if) key 1
Authentication: enabled
Local reference clock:
Only management interface
Switch# show ntp associations
Current NTP associations:
remote           refid      st when poll reach   delay   offset  disp
```

```
==============================================================================
=
*192.168.100.101 127.127.1.0      3   27   64    1    1.328    2.033 433.075
* sys.peer, + candidate, # selected, x falsetick, . excess, - outlyer
```

9.3 Настройка PTP

9.3.1 Общие положения

9.3.1.1 Краткий обзор

PTP (Precision Time Protocol) — это протокол синхронизации компьютерного времени, определенный стандартом IEEE 1588. Цель PTP — обеспечить точную синхронизацию часов в распределенных системах по сети для достижения высокой точности и синхронизации времени. Широко используется в промышленной автоматизации, транспорте, энергетических системах и других областях, требующих высокоточной синхронизации по времени.

Протокол PTP основан на архитектуре «ведущий-ведомый», где одно устройство выступает в роли ведущего генератора времени, а остальные — в роли ведомых. Протокол PTP в основном состоит из следующих важных компонентов и этапов:

- процесс синхронизации: Главные часы передают информацию о времени в сеть. После получения этой информации ведомые часы корректируются для соответствия времени главных;
- измерение задержки передачи: Главный тактовый генератор измеряет задержку распространения собственной временной информации до ведомого, чтобы тот смог скорректировать свое время;
- расчет смещения времени: смещение между своим временем и временем главных часов на основе информации о времени от главных часов;
- коррекция времени на основе рассчитанного смещения относительно основных часов.

Протокол PTP включает две версии: 1588 и G.8275.1. Версия 1588 включает 1588v1 и 1588v2. Версия 1588v1 обеспечивает точность синхронизации времени до долей миллисекунды, тогда как версия 1588v2 — до долей микросекунды. Стандарт G.8275.1 — это точный стандарт синхронизации времени, разработанный ITUT, аналогичный стандарту IEEE 1588. Оба стандарта предназначены для решения проблемы синхронизации по времени во всей сети.

Как высокоточный протокол синхронизации времени, PTP обеспечивает повышенную точность, более широкую область применения, более быструю обработку, масштабируемость и гибкость по сравнению с предыдущими технологиями. Эти преимущества сделали PTP важной технологией синхронизации времени в различных областях.

Основные термины и понятия

Сокращение	Описание
GPS	Глобальная система позиционирования
NTP	Протокол сетевого времени
PTP	Протокол точного времени
UTC	Всемирное координированное время
TAI	Международное атомное время

Ниже приведены некоторые важные понятия в PTP, которые помогут понять функции PTP и корректно настроить его на основе этих знаний.

Домен PTP

В домене PTP существует только один главный тактовый генератор, и все устройства синхронизируются с ним. Устройства в домене PTP могут обмениваться информацией о времени через протокол PTP, а также выполнять калибровку и синхронизацию времени.

Поддерживаемый диапазон доменов PTP — 0–255. Домен PTP можно настроить с помощью команды. Домен по умолчанию — 0.

Часы

В протоколе PTP существует три типа часов (или генераторов времени):

- Boundary Clock (BC): В одном и том же домене PTP устройства с двумя или более портами, участвующие в синхронизации времени PTP, называются «граничными часами». Устройство синхронизирует время с вышестоящих устройств через один порт и распределяет время на нижестоящие устройства через другие порты$

- Ordinary Clock (OC): В рамках одного домена PTP устройства с одним портом, участвующие в синхронизации времени PTP, называются «обычными часами»$

- Transparent Clock (TC): В качестве промежуточного узла «транзитные часы» принимают пакет PTP без обработки. Вносится корректировка на смещение перед передачей его дальше.

Порт

Порты с включенным протоколом PTP называются PTP-портами. Существует три типа PTP-портов:

- Главный порт: Порты, используемые для распределения времени на нижестоящие устройства на устройствах BC или OC$

- Ведомый порт: Порт, используемый для приема времени от вышестоящего устройства на устройствах BC или OC$

- Пассивный порт: Порт не принимает и не передает время на устройства BC.

Главные часы (время)

Главные часы (Grandmaster Clock, GM) — это часы самого высокого уровня в домене PTP и эталонное время для всего домена PTP. Все тактовые узлы в домене PTP организованы в определенную иерархию, и время оптимальных часов в конечном итоге синхронизируется со всем доменом PTP посредством взаимодействия сообщений протокола PTP между тактовыми узлами. Поэтому их также называют источником времени.

Алгоритм BMC

В алгоритме BMC «оптимальные часы» выбираются динамически посредством сообщений протокола PTP между узлами синхронизации. Каждый узел синхронизации обменивается информацией, такой как приоритет часов, точность времени, передаваемой в сообщении Announce, и в конечном итоге выбирает узел в качестве главных часов для домена PTP.

BMC алгоритм учитывает следующие поля:

- Приоритет 1: Допустимый диапазон значений — 0–255. Меньшее число указывает на более высокий приоритет. Значение по умолчанию — 128$
- Класс часов: Допустимый диапазон: 6/7/13/14/52/58/187/193/248. Меньшее число указывает на более высокий приоритет. Значение по умолчанию: 248$
- Точность синхронизации: допустимый диапазон — 0x20–0x31/0xFE. Меньшее число указывает на более высокий приоритет. Значение по умолчанию — 0xFE$
- Приоритет 2: Допустимый диапазон значений — от 0 до 255. Меньшее число указывает на более высокий приоритет. Значение по умолчанию — 128.

Инкапсуляция пакетов

Устройство, передающее PTP-пакеты, вычисляет смещение и задержку относительно ведущего устройства по метке времени в пакетах и корректирует локальные часы для синхронизации с часами ведущего устройства.

Метка времени PTP добавляется микросхемой ASIC для обеспечения точности времени. Микросхема ASIC обладает высокой производительностью.

Пакеты PTP поддерживают инкапсуляцию MAC и инкапсуляцию UDP.

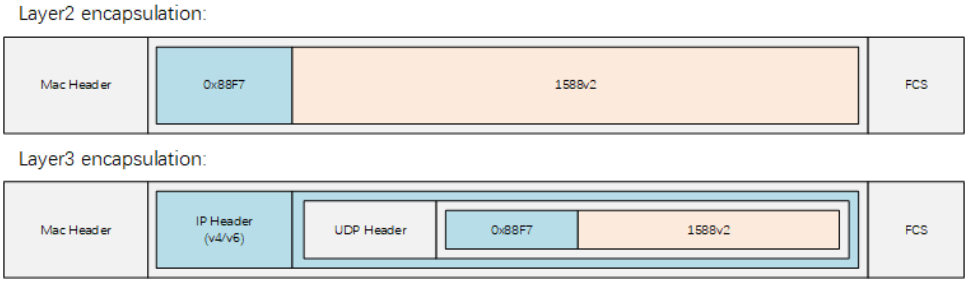


Рисунок 46 – структуара PTP пакета

Процесс синхронизации

Процесс синхронизации времени по протоколу PTP включает следующие этапы:

- Выбор ведущего и ведомого источника времени: В процессе синхронизации PTP один узел выбирается в качестве ведущего (Master clock), а остальные узлы служат в качестве ведомых (Slave clock). Ведущий (Master clock) имеет высокоточный источник времени и сообщает точное время ведомым (Slave clock) по сети, ведомые устройства, в свою очередь, синхронизируют свои часы.

- Компенсация и коррекция задержек: В процессе синхронизации PTP требуется компенсация задержек, возникающих при передаче сообщений. После расчета времени передачи сообщений точность времени восстанавливается путем учета рассчитанных значений задержки.

- В процессе синхронизации PTP крайне важно учитывать механизмы отказоустойчивости для повышения стабильности системы. Условия сети могут быть оптимизированы для синхронизации PTP.

- Проверка. согласованности времени: Проверка. согласованности времени также имеет важное значение в процессе синхронизации PTP. Распространенные методы проверки включают мониторинг разницы во времени между ведущими и ведомыми часами.

Этот процесс можно подробно описать с помощью механизма запроса-ответа с задержкой, описанного в стандарте IEEE 1588. Главные часы периодически отправляют сообщения синхронизации и записывают точное время t1; ведомые часы записывают точное время t2, когда сообщение синхронизации поступает; главные часы отправляют сообщение Follow_up, содержащее t1; ведомые часы отправляют сообщение Delay_Req, записывая точное время t3, когда сообщение отправляется; главные часы записывают точное время t4, когда сообщение Delay_Req поступает; затем главные часы отправляют ведомым часам сообщение Delay_Resp, содержащее t4. Таким образом, главные и ведомые часы могут синхронизировать время.

Конфигурация по умолчанию

Таблица 13 – Значения конфигурации по умолчанию

Наименование	Значение/режим
PTP протокол	Выключено
PTP тип устройства	Транзитные часы
PTP приоритет 1/PTP приоритет 2	128
PTP режим шага	2
PTP интервал анонса	1 сек
PTP таймаут анонса	3 сек

9.3.2 Примеры конфигурации

9.3.2.1 Настройка «Граничных часов» и «Обычных часов»

Топология

Рисунок 1-5 PTP Домен

Как показано на рисунке выше, Switch1 является главным устройством в домене и распределяет время между нижестоящими устройствами. Switch2 получает время от Switch1 и отправляет его на Switch3.

Этапы настройки

Конфигурация коммутатора 1

Шаг 1. Войдите в режим конфигурации

```
Switch1# configure terminal
```

Шаг 2. Включите PTP глобально и задайте приоритет 1.

Switch1 — это обычные часы с одним интерфейсом для распределения времени.

Установите priority1 равным 0. Это обеспечит коммутатору наивысший приоритет в данном домене синхронизации PTP, то есть он будет являться главным тактовым генератором этого домена.

```
Switch1(config)# ptp priority1 0
```

Шаг 3. Настройка типа устройства.

```
Switch1(config)# ptp device-type oc
```

Примечание: По умолчанию коммутатор работает в режиме TC, для включения PTP в режиме BC требуется как минимум 2 интерфейса. В этом примере коммутатор Switch1 имеет только один интерфейс для включения PTP и должен быть настроен в режиме OC.

Шаг 4. Настройка шага синхронизации (необязательно).

В PTP-пакетах для меток времени поддерживается одношаговый и двухшаговый режимы добавления. По-умолчанию используется двухшаговый режим.

Одношаговый процесс: добавление метки времени в пакет синхронизации.

Двухэтапный процесс: в пакет Follow_Up добавляется метка времени из пакета синхронизации.

Рекомендуется использовать один и тот же режим в одном домене PTP.

```
Switch1(config)# ptp clock-step two-step
```

Шаг 5. Настройка механизма задержки (необязательно).

Существует два режима работы механизма: E2E/P2P

По умолчанию используется режим e2e.

```
Switch1(config)# ptp delay-mechanism p2p
```

Шаг 6. Включите PTP на интерфейсе.

```
Switch1(config)# interface eth-0-9
Switch1(config-if)# ptp enable
```

Шаг 7 Включение PTP глобально

```
Switch1(config)# ptp start
```

Конфигурация коммутатора Switch2

Шаг 1. Войдите в режим конфигурации

```
Switch2# configure terminal
```

Шаг 2. Установите тип устройства как «Граничные часы» и включите PTP глобально.

Switch2 получает время от Switch1 и отправляет информацию о точном времени на Switch3. Установите тип устройства на «граничные часы».

```
Switch2(config)# ptp device-type bc
```

Шаг 3. Настройка механизма задержки (необязательно).

Примечание: используйте ту же конфигурацию, что и у Switch1.

```
Switch2(config)# ptp delay-mechanism p2p
```

Шаг 4. Включите PTP на интерфейсе.

```
Switch2(config)# interface eth-0-9
Switch2(config-if)# ptp enable
Switch2(config-if)# exit
Switch2(config)# interface eth-0-18
```

```
Switch2(config-if)# ptp enable
Switch2(config-if)# exit
```

Шаг 5. Глобальная активация PTP.

```
Switch1(config)# ptp start
```

Конфигурация коммутатора Switch3

Шаг 1. Войдите в режим конфигурации

```
Switch3# configure terminal
```

Шаг 2: настройте тип устройства как OC.

```
Switch3(config)# ptp device-type oc
```

Шаг 3. Настройка механизма задержки (необязательно).

Примечание: используйте ту же конфигурацию, что и для Switch2.

```
Switch3(config)# ptp delay-mechanism p2p
```

Шаг 4. Включите PTP на интерфейсе.

```
Switch3(config)# interface eth-0-18
Switch3(config-if)# ptp enable
Switch3(config-if)# exit
```

Шаг 5. Глобальная настройка PTP.

```
Switch1(config)# ptp start
```

Проверка.

Проверьте состояние PTP на коммутаторе Switch1

```
Switch1# show ptp
------------------  Global Config  ------------------
PTP State                   : enable
Port Number                 : 1
Domain                      : 0
Step Mode                   : two
Priotity1                   : 0
Priotity2                   : 128
Clock Type                  : ordinary clock
```

```
Delay Machanism              : P2P
------------------  Time Status  ------------------
        000102.fffe.030d02-0 seq 0 RESPONSE MANAGEMENT TIME_STATUS_NP
master_offset(ns)           0
ingress_time(ns)            0
gmPresent                   false
gmIdentity                  000102.fffe.030d02
Switch1#
```

Проверьте состояние PTP-порта на коммутаторе Switch1

```
Switch1# show ptp interface
        000102.fffe.030d02-9 seq 0 RESPONSE MANAGEMENT PORT_DATA_SET
portIdentity            000102.fffe.030d02-9
portState               MASTER
logMinDelayReqInterval  0
peerMeanPathDelay       924
logAnnounceInterval     1
announceReceiptTimeout  3
logSyncInterval         0
delayMechanism          2
logMinPdelayReqInterval 0
versionNumber           2
Switch1#
```

Проверьте состояние PTP на коммутаторе Switch2

```
Switch2# show ptp
------------------  Global Config  ------------------
PTP State                    : enable
Port Number                  : 2
Domain                       : 0
Step Mode                    : two
Priotity1                    : 128
Priotity2                    : 128
Clock Type                   : binary clock
Delay Machanism              : P2P
------------------  Time Status  ------------------
        d85b22.fffe.0bba84-0 seq 0 RESPONSE MANAGEMENT TIME_STATUS_NP
master_offset(ns)           -2
ingress_time(ns)            1732806452900546058
gmPresent                   true
gmIdentity                  000102.fffe.030d02
Switch2#
```

Проверьте состояние порта PTP на коммутаторе Switch2

```
Switch2# show ptp interface
        d85b22.fffe.0bba84-9 seq 0 RESPONSE MANAGEMENT PORT_DATA_SET
portIdentity            d85b22.fffe.0bba84-9
portState               SLAVE
```

```
logMinDelayReqInterval  0
peerMeanPathDelay       921
logAnnounceInterval     1
announceReceiptTimeout  3
logSyncInterval         0
delayMechanism          2
logMinPdelayReqInterval 0
versionNumber           2
        d85b22.fffe.0bba84-18 seq 0 RESPONSE MANAGEMENT PORT_DATA_SET
portIdentity            d85b22.fffe.0bba84-18
portState               MASTER
logMinDelayReqInterval  0
peerMeanPathDelay       1282
logAnnounceInterval     1
announceReceiptTimeout  3
logSyncInterval         0
delayMechanism          2
logMinPdelayReqInterval 0
versionNumber           2
Switch2#
```

Проверьте состояние PTP на коммутаторе 3.

```
Switch# show ptp
-------------------  Global Config  ------------------
PTP State                    : enable
Port Number                  : 1
Domain                       : 0
Step Mode                    : two
Priotity1                    : 128
Priotity2                    : 128
Clock Type                   : ordinary clock
Delay Machanism              : P2P
-------------------  Time Status  -------------------
        d85b22.fffe.000401-0 seq 0 RESPONSE MANAGEMENT TIME_STATUS_NP
master_offset(ns)           -7
ingress_time(ns)            1732805307622102495
gmPresent                   true
gmIdentity                  000102.fffe.030d02
Switch#
```

Проверьте состояние порта PTP на коммутаторе 3

```
Switch# show ptp interface
        d85b22.fffe.000401-18 seq 0 RESPONSE MANAGEMENT PORT_DATA_SET
portIdentity            d85b22.fffe.000401-18
portState               FAULTY
logMinDelayReqInterval  0
peerMeanPathDelay       1284
logAnnounceInterval     1
```

```
announceReceiptTimeout  3
logSyncInterval         0
delayMechanism          2
logMinPdelayReqInterval 0
versionNumber           2
Switch#
```

9.4 Настройка функции L2 ping

9.4.1 Общие положения

9.4.1.1 Описание функции

Инструмент L2 ping предназначен для проверки соединения между двумя коммутаторами. L2 ping отличается от хорошо известной команды 'ping IP-ADDRESS'. Обычная команда 'ping' реализуется по протоколу ICMP, который зависит от уровня IP, поэтому она может быть неприменима, если целевым устройством является коммутатор уровня 2. L2 ping основан на пакетах Ethernet уровня 2.

При запуске L2 ping пакет протокола L2 ping (с типом '36873(0x9009)') отправляется с указанного физического порта на другой указанный порт. На принимающей стороне пакет L2 ping отправляется обратно через интерфейс обратной связи (не 802.1ag), или через конфигурируемый «ответ ping L2». Устройство, выполняющее ping, получает пакет ответа на ping и выводит результат.

9.4.2 Настройка

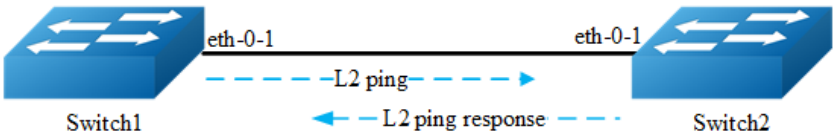


Рисунок 47 – Ping до порта коммутатора

Конфигурации коммутаторов Switch1 и Switch2 практически одинаковы, за исключением некоторых моментов, которые специально отмечены.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и включите интерфейс.

```
Switch (config)# interface eth-0-1
Switch (config-if)# no shutdown
```

Шаг 3. Включите функцию ответа на ping L2.

Настройка на Switch2:

```
Switch (config-if)# l2 ping response enable
```

Шаг 4. Выйдите из режима настройки.

```
Switch (config-if)# end
```

Шаг 5. Использование L2-ping.

Настройка коммутатора Switch1

```
Switch1# l2 ping 001e.0808.58f1 interface eth-0-1 count 10 interval 1000
timeout 2000

 Sending 10 L2 ping message(s):
 64 bytes from 001e.0808.58f1: sequence = 0, time = 10ms
 64 bytes from 001e.0808.58f1: sequence = 1, time = 15ms
 64 bytes from 001e.0808.58f1: sequence = 2, time = 13ms
 64 bytes from 001e.0808.58f1: sequence = 3, time = 12ms
 64 bytes from 001e.0808.58f1: sequence = 4, time = 20ms
 64 bytes from 001e.0808.58f1: sequence = 5, time = 21ms
 64 bytes from 001e.0808.58f1: sequence = 6, time = 12ms
 64 bytes from 001e.0808.58f1: sequence = 7, time = 16ms
 64 bytes from 001e.0808.58f1: sequence = 8, time = 14ms
 64 bytes from 001e.0808.58f1: sequence = 9, time = 17ms
 L2 ping completed.
 ---------------------------------
 10 packet(s) transmitted, 10 received, 0 % packet loss
```

001e.0808.58f1 — это MAC-адрес интерфейса на коммутаторе Switch2. Его можно получить с помощью команды “show interface eth-0-1” на коммутаторе Switch2.

9.5 Настройка RMON

9.5.1 Общие положения

9.5.1.1 Описание функции

RMON — это стандарт мониторинга, разработанный группой (IETF), который позволяет различным сетевым агентам обмениваться данными мониторинга по сети. Функцию RMON можно использовать совместно с Simple Network Management Protocol (SNMP) для мониторинга всего трафика, проходящего между всеми сегментами локальной сети.

RMON — это стандартная спецификация мониторинга, определяющая набор данных и функций, которыми можно обмениваться между совместимыми с RMON консольными системами

и сетевыми устройствами. RMON предоставляет исчерпывающую информацию для диагностики сетевых неисправностей и их устранения для повышения производительности сети.

9.5.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и создайте разделы статистики и истории.

```
Switch(config)# interface eth-0-1
Switch(config-if)# rmon collection stats 1 owner test
Switch(config-if)# rmon collection history 1 buckets 100 interval 1000 owner
test
Switch(config-if)# exit
```

Шаг 3. Создайте событие, в котором установлены параметры log и trap.

```
Switch(config)# rmon event 1 log trap public description test_event owner
test
```

Шаг 4. Создайте оповещение, используя событие 1, созданное ранее, и отслеживайте его на eth-0-1.

```
Switch(config)# rmon alarm 1 etherStatsEntry.6.1 interval 1000 delta rising-
threshold 1000 event 1 falling-threshold 1 event 1 owner test
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

```
Switch# show rmon statistics
  Rmon collection index 1
        Statistics ifindex = 1, Owner: test
        Input packets 0, octets 0, dropped 0
        Broadcast packets 0, multicast packets 0, CRC alignment errors 0,
collisions 0
        Undersized packets 0, oversized packets 0, fragments 0, jabbers 0
        # of packets received of length (in octets):
        64: 0,  65-127: 0, 128-255: 0
        256-511: 0,  512-1023: 0, 1024-max: 0
```

```
Switch# show rmon history
  History index = 1
        Data source ifindex = 1
        Buckets requested = 100
        Buckets granted = 100
        Interval = 1000
        Owner: test

Switch# show rmon event
  Event Index = 1
        Description: test_event
        Event type Log & Trap
        Event community name: public
        Last Time Sent = 00:00:00
        Owner: test

Switch# show rmon alarm
  Alarm Index = 1
  Alarm status = VALID
  Alarm Interval = 1000
  Alarm Type is Delta
  Alarm Value = 00
  Alarm Rising Threshold = 1000
  Alarm Rising Event = 1
  Alarm Falling Threshold = 1
  Alarm Falling Event = 1
  Alarm Owner is test
```

9.6 Настройка SNMP

9.6.1 Общие положения

9.6.1.1 Описание функции

SNMP — это протокол уровня приложений, предоставляющий формат сообщений для связи между менеджерами и агентами. Система SNMP состоит из менеджера SNMP, агента SNMP и MIB. Менеджер SNMP может быть частью системы управления сетью (NMS). Агент и MIB находятся на коммутаторе. Агент SNMP содержит переменные MIB, значения которых менеджер SNMP может запрашивать или изменять. Менеджер может получить значение от агента или прописать значение в агенте. Агент собирает данные из MIB и может отвечать на запросы менеджера на получение или запись данных. Агент может отправлять оповещения менеджеру. Это сообщения, оповещающие менеджер SNMP о состоянии сети или о событии как например: ошибка аутентификации, перезапуски, состояние канала связи (активен или неактивен), отслеживание MAC-адреса, закрытие TCP-соединения, потеря связи с соседом или другие значимые события.

9.6.1.2 Описание принципа

Модуль SNMP основан на следующем стандарте RFC:

- SNMPv1: RFC 1157;
- SNMPv2C: RFC 1901;
- SNMPv3: RFC 2273–2275.

Ниже приведено краткое описание терминов, используемых для описания протокола SNMP:

- Агент: модуль программного обеспечения для управления сетью. Агент преобразует данные о сети и устройстве в форму, совместимую с SNMP.
- База информации (MIB): это иерархическая текстовая база данных, описывающая параметры сетевого устройства.
- Идентификатор: уникальный идентификатор узла сети.
- Оповещение: используется управляемыми устройствами для передачи информации о событиях в систему управления сетью (NMS).

9.6.2 Настройка

Как показано на рисунке, агент SNMP собирает данные из MIB. Агент может отправлять уведомления об определенных событиях менеджеру SNMP. Такие сообщения оповещают менеджер SNMP о состоянии сети. Агент SNMP также отвечает на запросы, связанные с MIB, отправляемые менеджером SNMP в формате get-request, get-next-request и set-request.

9.6.2.1 Включение SNMP

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите SNMP глобально.

```
Switch(config)# snmp-server enable
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show running-config
snmp-server enable
```

9.6.2.2 Настройка Community String

Community string — это текстовый пароль (строка аутентификации), используемый в версиях SNMPv1 и SNMPv2c для разграничения доступа между менеджером (системой мониторинга) и агентом (сетевым устройством: коммутатор, роутер, сервер). Если строка совпадает, устройство принимает запрос, если нет — игнорирует его. Для строки можно указать:

- Какое подмножество объектов MIB доступно данному сообществу.
- Права доступа (чтение/запись) к объектам MIB, доступным данному сообществу.

Для настройки строки сообщества на коммутаторе выполните следующие действия в привилегированном режиме EXEC.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройка строки сообщества.

Настройте представление с именем «DUT»; настройте сообщество с именем «public» с правами на чтение «DUT».

```
Switch(config)# snmp-server view DUT included 1
Switch(config)# snmp-server community public read-write (view DUT)
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.n

```
Switch# show running-config
snmp-server enable
snmp-server view DUT included .1
snmp-server community public read-only view DUT
```

9.6.2.3 Configuring SNMPv3 Groups, Users and Accesses

Вы можете указать идентификационное имя для локального SNMP-сервера на коммутаторе. Можно настроить группу SNMP-серверов, которая сопоставляет пользователей SNMP с отчетами/ответами SNMP, можно добавлять новых пользователей в эту группу SNMP и предоставлять права доступа этой группе SNMP.

Для настройки в привилегированном режиме EXEC выполните следующие действия.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройте глобальные параметры конфигурации SNMP.

- Установить EngineID;
- Установить имя пользователя, пароль и тип аутентификации;
- Создать SNMP-сервер;
- Установить права доступа для членов группы.

```
Switch(config)# snmp-server engineID 8000123456
Switch(config)# snmp-server usm-user usr1 authentication md5 mypassword
privacy des yourpassword
Switch(config)# snmp-server group grp1 user usr1 security-model usm
Switch(config)# snmp-server access grp1 security-model usm noauth
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show running-config
snmp-server engineID 8000123456
snmp-server usm-user usr1 authentication md5 mypassword privacy des
yourpassword
snmp-server group grp1 user usr1 security-model usm
snmp-server access grp1 security-model usm noauth
```

9.6.2.4 Настройка уведомлений SNMPv1 и SNMPv2

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройте глобальные параметры SNMP.

- Включите все поддерживаемые оповещения;
- Настройте удаленный менеджер оповещений с IP-адресом «10.0.0.2»;

```
Switch(config)# snmp-server trap enable all
Switch(config)# snmp-server trap target-address 10.0.0.2 community
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show running-config
snmp-server trap target-address 10.0.0.2 community public
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

9.6.2.5 Настройка уведомлений SNMPv3

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Настройте глобальные параметры SNMP.

- включить все поддерживаемые оповещения;
- настроить уведомления версии SNMPv3;
- настроить IP-адрес удаленного менеджера оповещений;
- добавить локального пользователя SNMPv3.

```
Switch(config)# snmp-server trap enable all
Switch(config)# snmp-server notify notif1 tag tmptag trap
Switch(config)# snmp-server target-address targ1 param parm1 10.0.0.2 taglist
tmptag
Switch(config)# snmp-server target-params parm1 user usr1 security-model v3
message-processing v3 noauth
```

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show running-config
snmp-server notify notif1 tag tmptag trap
snmp-server target-address targ1 param parm1  10.0.0.2 taglist tmptag
snmp-server target-params parm1 user usr1 security-model v3 message-
```

```
processing v3 noauth
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

9.7 Настройка SFLOW

9.7.1 Общие положения

9.7.1.1 Описание функции

sFlow (sampled flow) — это отраслевой стандарт (протокол) для мониторинга производительности высокоскоростных сетей в реальном времени, основанный на случайной выборке пакетов и периодическом опросе счетчиков интерфейсов. Он позволяет получать точную статистику о типах трафика, загрузке каналов и аномалиях без высокой нагрузки на оборудование.

Архитектура и методы выборки, используемые в системе мониторинга sFlow, обеспечивают непрерывный мониторинг трафика высокоскоростных коммутируемых и маршрутизируемых сетей.

Агент sFlow использует два метода выборки: статистическую выборку пакетов из коммутируемых потоков и выборку статистики сетевых интерфейсов.

Таблица 14 – Конфигурация по умолчанию

Параметр	Настройки по умолчанию
sFlow глобально	Выключено
sFlow на порту	Выключено
UDP порт коллектора	6343
Временной интервал счетчика	20 seconds

9.7.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите sFlow глобально.

```
Switch(config)# sflow enable
```

Шаг 3. Установите глобальный атрибут для sFlow.

Укажите IP-адрес агента, IP-адрес сборщика и UDP-порт. Если UDP-порт не указан, используется порт по умолчанию 6364.

```
Switch(config)# sflow agent ip 3.3.3.1
Switch(config)# sflow collector 3.3.3.2 6342
```

NOTE Для работы с sFlow необходимо настроить как минимум один агент и один сборщик.

Установите интервал отправки данных со счетчиков интерфейса (необязательно):

```
Switch(config)# sflow counter interval 15
```

Шаг 4. Войдите в режим настройки интерфейса и задайте атрибуты интерфейсов

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 15.1.1.1/24
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)#no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 16.1.1.1/24
Switch(config-if)# exit

Switch(config)# interface eth-0-3
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 3.3.3.1/24
Switch(config-if)# exit
```

Шаг 5. Включите sFlow для входящих пакетов на eth-0-1

```
Switch(config)# interface eth-0-1
Switch(config-if)# sflow flow-sampling rate 8192
Switch(config-if)# sflow flow-sampling enable input
Switch(config-if)# sflow counter-sampling enable
Switch(config-if)# exit
```

Шаг 6. Проверка.

Для отображения конфигурации sFlow используйте следующую команду：

```
Switch# show sflow
sFlow Version: 5
sFlow Global Information:
 Agent IPv4 address             : 3.3.3.1

 Counter Sampling Interval      : 15 seconds
 Collector 1:
  IPv4 Address: 3.3.3.2
  vrf: N/A
  Port: 6342

  vrf: N/A
  Port: 6343

sFlow Port Information:
                                  Flow-Sample    Flow-Sample
 Port         Counter    Flow      Direction      Rate
 ---------------------------------------------------------
 eth-0-1      Enable     Enable    Input          8192
```

9.8 Настройка LLDP

9.8.1 Общие положения

9.8.1.1 Описание функции

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевому оборудованию оповещать другое оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, и получать от него аналогичные сведения. Описание протокола приводится в стандарте IEEE 802.1AB-2009 Обнаружение на уровне 2 позволяет точно определять интерфейсы, подключенные к устройствам, и информацию о соединении уровня 2, такую как атрибуты VLAN порта, пути между коммутатором, маршрутизатором, серверами. Это подробное описание помогает быстро получить информацию для диагностики сети.

9.8.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Включите LLDP глобально.

```
Switch(config)# lldp enable
```

Шаг 3. Войдите в режим настройки интерфейса и установите атрибуты LLDP на интерфейсе.

```
Switch(config)# interface eth-0-9
Switch(config)# no shutdown
Switch(config-if)# no lldp tlv 8021-org-specific vlan-name
Switch(config-if)# lldp tlv med location-id ecs-elin 1234567890
Switch(config-if)# lldp enable txrx
Switch(config-if)# exit
```

Шаг 4. Настройка таймеров LLDP (необязательно).

Установите интервал передачи LLDP-пакета на 40 секунд; установите задержку передачи LLDP-пакета на 3 секунды; установите задержку повторной инициализации функции LLDP на 1 секунду.

```
Switch(config)# lldp timer msg-tx-interval 40
Switch(config)# lldp timer tx-delay 3
Switch(config)# lldp timer reinitDelay 1
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Для отображения конфигурации LLDP используйте следующую команду:

```
Switch# show lldp local config
LLDP global configuration:
============================================================
LLDP function global enabled : YES
LLDP msgTxHold     : 4
LLDP msgTxInterval : 40
LLDP reinitDelay   : 1
LLDP txDelay       : 3
Switch# show lldp local config interface eth-0-9
LLDP configuration on interface eth-0-9 :
============================================================
LLDP admin status : TXRX
Basic optional TLV Enabled:
    Port Description TLV
    System Name TLV
    System Description TLV
    System Capabilities TLV
    Management Address TLV
IEEE 802.1 TLV Enabled:
```

```
    Port Vlan ID TLV
    Port and Protocol Vlan ID TLV
    Protocol Identity TLV
IEEE 802.3 TLV Enabled:
    MAC/PHY Configuration/Status TLV
    Power Via MDI TLV
    Link Aggregation TLV
    Maximum Frame Size TLV
LLDP-MED TLV Enabled:
    Med Capabilities TLV
    Network Policy TLV
    Location Identification TLV
    Extended Power-via-MDI TLV
    Inventory TLV
Switch# show running-config
!
lldp enable
lldp timer msg-tx-interval 40
lldp timer reinit-delay 1
lldp timer tx-delay 3
!
interface eth-0-9
lldp enable txrx
 no lldp tlv 8021-org-specific vlan-name
 lldp tlv med location-id ecs-elin 1234567890
!
Switch# show lldp neighbor
Local Port eth-0-1 has 0 neighbor(s)

Local Port eth-0-2 has 0 neighbor(s)
…
Local Port eth-0-9 has 2 neighbor(s)

Remote LLDP Information of port eth-0-9
============================================================
Neighbor Index : 1
Chassis ID type: Mac address
Chassis ID     : 48:16:be:a4:d7:09
Port ID type   : Interface Name
Port ID        : eth-0-9
TTL : 160
Expired time: 134
…
Location Identification :
ECS ELIN: 1234567890
```

9.9 Настройка IPFIX

9.9.1 Общие положения

9.9.1.1 Описание функции

Трафик в сети передачи данных можно рассматривать как потоки, проходящие через сетевые элементы. В административных или иных целях часто бывает необходимо иметь доступ к информации об этих потоках, проходящих через сетевые элементы. Это требует единообразия в методе представления информации о потоках и средствах передачи этих данных о потоках от сетевых элементов к точке сбора. Именно это и обеспечивает IPFIX.

До появления IPFIX существовал патентованный протокол Cisco — NetFlow. IPFIX похож на NetFlow и основан на версии NetFlow 9.

9.9.2 Настройка

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите время устаревания (необязательно).

Установите время устаревания 300 секунд. По умолчанию время устаревания составляет 1800 секунд.

```
Switch(config)# ipfix global
Switch(Config-ipfix-global)# flow aging 300
```

Шаг 3. Настройка интерфейса уровня 3

```
Switch(config)# interface eth-0-2
Switch(config-if)# no shutdown
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.2/24
Switch(config-if)# exit
```

Шаг 4. Настройка регистратора.

Пользователь может указать характеристики для разделения потоков в «Рекордере». В следующем примере пакеты с заданными MAC-адресом источника, IPv4 адресами назначения и источника и VXLAN-vni относятся к одному потоку.

Следует настроить параметр «счетчик сбора». В следующем примере включены параметры «счетчик сбора байтов» и «счетчик сбора пакетов», что означает, что должны записываться как байты, так и пакеты.

```
Switch(config)# ipfix recorder recorder1
Switch(Config-ipfix-reocrder)# match mac source address
Switch(Config-ipfix-reocrder)# match ipv4 source address mask 32
Switch(Config-ipfix-reocrder)# match ipv4 destination address mask 32
Switch(Config-ipfix-reocrder)# match vxlan-vni
Switch(Config-ipfix-reocrder)# collect counter bytes
Switch(Config-ipfix-reocrder)# collect counter packets
Switch(Config-ipfix-reocrder)# exit
```

Шаг 5. Настройка сэмплера

```
Switch(config)# ipfix sampler sampler1
Switch(Config-ipfix-sampler)# 1 out-of 100
Switch(Config-ipfix- sampler)# exit
```

Шаг 6. Настройка экспортера.

Настройте параметры инкапсуляции и отправки пакетов IPFIX.

В следующем примере адрес назначения пакетов — 10.10.10.1 (совпадает с адресом сборщика), отправка осуществляется с eth-0-2, интервал между пакетами составляет 200 секунд.

"Тайм-аут окончания потока событий" означает, что при истечении времени ожидания потока пакет IPFIX должен быть немедленно отправлен сборщику.

```
Switch(config)# ipfix exporter exporter1
Switch(Config-ipfix-exporter)# destination 10.10.10.1
Switch(Config-ipfix-exporter)# source interface eth-0-2
Switch(Config-ipfix-exporter)# flow data timeout 200
Switch(Config-ipfix-exporter)# event flow end timeout
Switch(Config-ipfix-exporter)# exit
```

Шаг 7. Настройка мониторинга

```
Switch(config)# ipfix monitor monitor1
Switch(Config-ipfix-monitor)# recorder recorder1
Switch(Config-ipfix-monitor)# exporter exporter1
Switch(Config-ipfix-monitor)# exit
```

Шаг 8. Войдите в режим настройки интерфейса и примените конфигурацию ipfix.

```
Switch(config)# interface eth-0-1
Switch(config-if)# ipfix monitor input monitor1
Switch(config-if)# exit
```

Вы можете указать монитор и сэмплер в одной команде, используя команду для сэмплера с целью определения частоты сэмплирования. (Если сэмплер не указан, частота дискретизации должна быть 100%).

```
Switch(config)# interface eth-0-1
Switch(config-if)# ipfix monitor input monitor1 sampler sampler1
Switch(config-if)# exit
```

Шаг 9. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 10. Проверка.

Для проверки конфигурации используйте следующие команды:

```
Switch# show ipfix global
IPFIX global informaition:
     Current flow cache number                          : 0(ingress: 0,
egress: 0)
     Flow cache aging interval                          : 300 seconds
     Flow cache export interval                         : 5 seconds
     Flow cache memory usage threshold                  : 90%
     Flow cache sampler mode                            : all flow
     Flow cache packet wraparound threshold             : 67108863
     Flow cache byte wraparound threshold               : 4294967295
     Flow cache dropped packet wraparound threshold     : 1023
     Flow cache jitter threshold                        : 65535
     Flow cache latency threshold                       : 16777215

Switch# show ipfix recorder recorder1
IPFIX recorder information:
    Name            : recorder1
    Description     :
    Match info      :
        match Source Mac Address
        match IPv4 Source Address
        match IPv4 Destination Address
        match Vxlanvni
    Collect info    :
        collect Flow Byte Number
        collect Flow Packet Number

Switch# show ipfix exporter exporter1
IPFIX exporter information:
    Name                            : exporter1
    Description                     :
    Exporter Interface              : eth-0-2
    Domain ID                       : 0
    Collector Name                  : 10.10.10.1
    IPFIX message protocol          : UDP
    IPFIX message destination Port  : 2055
```

```
    IPFIX message TTL value           : 255
    IPFIX message DSCP value          : 63
    IPFIX data interval               : 200
    IPFIX template interval           : 1800
    IPFIX exporter events             :
        Flow aging event

Switch# show ipfix sampler sampler1
IPFIX sampler information:
    Name                              : sampler1
    Description                       :
    Rate                              : 100

Switch# show ipfix monitor monitor1
IPFIX monitor information:
    Name                              : monitor1
    Description                       :
    Recorder                          : recorder1
    exporter                          : exporter1
    flow mirror packet                : 0
    flow mirror destination           : NA
```

10 Руководство по настройке системы управления трафиком

10.1 Настройка QoS

10.1.1 Общие положения

10.1.1.1 Описании функции

Механизм Quality of Service (QoS) позволяет предоставлять определенным видам трафика приоритет над другими. Без QoS весь трафик в сети имеет одинаковый приоритет и время доставки. При возникновении перегрузки любой трафик имеет одинаковую вероятность быть отброшенным. С QoS можно установить приоритет для определенных видов сетевого трафика. Такая сеть более эффективно использует полосу пропускания.

Классификационная информация может передаваться в заголовке IP-пакета уровня 3 или в кадре уровня 2. В заголовках IP-пакетов информация передается с использованием 6 или 3 бит из устаревшего поля типа обслуживания IP (TOS). В кадрах 802.1Q уровня 2 информация передается с использованием 2-байтового поля информации управления тегом (Tag Control Information).

Все коммутаторы и маршрутизаторы используют информацию о классификации трафика для установления соответствующего приоритета. Пакеты в сети можно классифицировать как:

- Пакет с конечного устройства или коммутатора (в соответствии с настроенной политикой).
- Детальный анализ пакета будет проводиться ближе к границе сети, (позволит предотвратить перегрузку магистральных коммутаторов и маршрутизаторов).
- Сочетание двух вышеуказанных методов

Информация о классификации трафика может использоваться коммутаторами и маршрутизаторами на пути прохождения для ограничения объема выделяемых ресурсов для обработки каждого класса.

QoS (Quality of Service) обеспечивает разное качество обслуживания в соответствии с различными требованиями. Например, предоставление заданной полосы пропускания, снижение частоты потери пакетов для голосового трафика. Для достижения этих целей QoS часто использует различные методы, например, классификацию и распределение трафика. Вот основные методы и функции QoS:

- классификация трафика по ряду признаков;
- контроль и надзор за определенным трафиком, поступающим в сетевое оборудование. Принятие мер по защите такого особого трафика от потерь;

- регулировка скорости выходящих потоков трафика (активная регулировка скорости передачи данных). Обычно используется для адаптации нижестоящего маршрутизатора, предоставляющего сетевые ресурсы, и предотвращения ненужной потери пакетов;

- управление перегрузкой сети при возникновении сетевых перегрузок и конкуренции за ресурсы. Пакеты помещаются в буфер очереди, для определения порядка пересылки пакетов используется определенный алгоритм;

- снижение вероятности перегрузки сети. При обнаружении тенденции к быстрому росту трафика система предпримет действия по отбрасыванию пакетов, корректируя объемы трафика.

Среди этих методов обеспечения качества обслуживания (QoS) классификация трафика является основополагающей. Распознавание пакетов в соответствии с определенными правилами и является необходимым условием для работы QoS.

10.1.1.2

Краткое описание терминов и понятий, используемых для описания функции QoS

Списки контроля доступа (ACL) классифицируют трафик по одинаковым характеристикам. IP-трафик классифицируется с помощью IP ACL, не IP-трафик — с помощью MAC ACL. ACL может содержать несколько записей контроля доступа (ACE), которые представляют собой команды, сопоставляющие поля с содержимым пакета.

Класс обслуживания (CoS) — это 3-битное значение, используемое для классификации приоритета кадров второго уровня.

QoS классифицирует кадры, присваивая им значения CoS с индексацией по приоритету, и отдает предпочтение трафику с более высоким приоритетом.

Заголовки кадров 802.1Q второго уровня содержат 2-байтовое поле Tag Control Information, в котором значения CoS хранятся в трех старших битах, называемых битами приоритета. На интерфейсах, настроенных как транки 802.1Q второго уровня, весь трафик передается в кадрах 802.1Q, за исключением трафика собственной VLAN.

Другие типы кадров не могут передавать значения CoS уровня 2. Значения CoS варьируются от 0 до 7.

Код дифференцированного обслуживания (DSCP) — это 6-битное значение, используемое для классификации пакетов уровня 3.

Значения DSCP варьируются от 0 до 63.

IP-Precedence — это 3-битное значение, используемое для классификации приоритета пакетов третьего уровня.

Значения IP-Precedence варьируются от 0 до 7.

Значение EXP — это 3-битное значение, используемое для классификации пакетов MPLS.

Значения MPLS EXP варьируются от 0 до 7.

Классификация трафика происходит за счет анализа полей пакета. В результате процесса генерируется внутренний приоритет для пакета, который определяет все будущие действия QoS с этим пакетом.

На входе пакет проверяется, и его приоритет определяется на основе списков контроля доступа (ACL) или конфигурации. Затем значение CoS уровня 2 сопоставляется со значением приоритета.

Класс передается в заголовке IP-пакета с использованием 6 бит или 3 бит из устаревшего поля IP TOS. Классификация также может происходить и в кадре уровня 2. Классификация происходит на входящем физическом порту.

Классификация может основываться на CoS/внутреннем CoS/DSCP/приоритетности IP-адресов, а также на картах классов и политик, настроенных в коммутаторе.

Оформление – изменение скорости входящего трафика для регулирования скорости исходящего трафика. Если входящий трафик имеет высокую интенсивность и скачкообразный характер, его необходимо буферизовать, чтобы выходные данные из буфера были менее прерывистыми.

Маркировка определяет способ дальнейшей обработки пакета, когда он не попал под созданные правила. Анализируется нагрузка трафика и конфигурация, чтобы определить необходимые действия для пакета:

- пропустить пакет и маркировать его;
- отбросить пакет.

Маркировка может производиться на входных и выходных интерфейсах.

Очередь

Пакеты помещаются в определенную очередь. Каждый исходящий порт может вмещать до 8 очередей для unicast, 1 для multicast и 1 очередь SPAN.

Внутренний приоритет пакета может быть сопоставлен с одной из исходящих очередей. Единицей измерения размера очереди является буферная ячейка. Буферная ячейка — это 288 байт.

После того как пакеты помещены в очередь, планируется их отправка.

Отбрасывание пакетов в конце очереди

Отбрасывание пакетов в конце очереди (tail drop) — это стандартный метод предотвращения перегрузки на интерфейсе. Пакеты с разным приоритетом и цветом имеют разный приоритет отбрасывания. Сопоставление приоритета трафика с приоритетами очереди можно настроить. Таким образом можно управлять очередностью отброса пакетов при перегрузке

выходных буферов. Используется команда настройки интерфейса для определения пороговых значений очереди. Каждое пороговое значение связано с размером буфера интерфейса.

WRED

Метод Weighted Random Early Detection (WRED) отличается от других методов предотвращения перегрузки тем, что он направлен на прогнозирование перегрузки, а не на управление ими в момент их возникновения.

WRED снижает вероятность потери пакетов в конце очереди, выборочно отбрасывая пакеты, когда выходной интерфейс начинает демонстрировать признаки перегрузки. Отбрасывая часть пакетов на ранних этапах, не дожидаясь заполнения очереди, WRED избегает одновременной потери большого количества пакетов. Таким образом, WRED позволяет постоянно использовать линию передачи в полном объеме. WRED также отбрасывает больше пакетов от крупных потоков, чем от мелких.

Вы можете включить WRED и настроить два пороговых значения для приоритета отбрасывания, назначенных каждой исходящей очереди. Каждое минимальное пороговое значение показывает, с какого момента WRED начинает случайным образом отбрасывать пакеты. По мере приближения к максимальному пороговому значению очереди WRED продолжает случайным образом отбрасывать пакеты. Когда достигается максимальное пороговое значение, WRED отбрасывает все пакеты. По умолчанию WRED отключен.

Планирование

При планировании пересылки пакетов используется комбинация алгоритмов WDRR и SP. Каждая очередь принадлежит к определенному классу. Классы варьируются от 0 до 7, где 7 — наивысший приоритет. Несколько очередей могут принадлежать к одному классу. Планирование происходит с помощью алгоритма SP между классами и алгоритма WDRR между очередями внутри класса.

Строгая система приоритезации (SP), при которой сначала передаются пакеты с высоким приоритетом. Пакеты с более низким приоритетом передаются только тогда, когда очереди с более высоким приоритетом пусты.

Взвешенное распределение (Deficit Round Robin, WDRR) — метод, при котором каждой очереди присваивается вес для регулирования количества пакетов, отправляемых из каждой очереди.

Карта классов

Изолирует определенный трафик от остального трафика. Карта классов определяет критерии, используемые для дальнейшей классификации. Критерии могут соответствовать

нескольким группам доступа, определенным в списке контроля доступа (ACL). После сопоставления пакета с критериями карты классов он дополнительно классифицируется с помощью карты политик.

Карта политик

Карта политик определяет, к какому классу трафика следует применять следующие действия:

- задайте конкретный приоритет и цвет для класса трафика;
- задайте конкретную политику для сопоставления приоритета и цвета;
- укажите ограничения пропускной способности трафика для каждого соответствующего класса трафика и действия, которые необходимо предпринять, когда трафик выходит за рамки;
- перенаправьте соответствующий класс трафика на конкретный физический интерфейс;
- зеркалирование конкретного класса трафика в конкретную сессию мониторинга;
- включите статистику для каждой карты классов.

Временной диапазон

Используя временной диапазон, можно применять правила карты классов в зависимости от времени суток или недели. Таким образом вы можете использовать временной диапазон для определения того, когда действуют правила в карте классов (например, в течение указанного периода времени или в указанные дни недели).

Вот лишь некоторые из многочисленных преимуществ использования временного диапазона:

- Вы можете управлять разрешением или запретом доступа пользователя к ресурсам.
- Статистику трафика можно получать строго в назначенное время.
- Вы можете определить, когда действие для определенного класса трафика вступает в силу.

10.1.1.3 Краткое пояснение процесса настройки функции MQC (Modular QoS)

Коммутатор предоставляет простые шаблоны настройки MQC (модульное QoS). Сетевым администраторам не нужно беспокоиться о том, как отдельно решать вопросы импорта или экспорта команд. Нужно лишь настроить карту политик, а затем применить её к определённому интерфейсу. Это снижает требования к обслуживающему сетевое оборудование персоналу.

Процесс настройки системы MQC выглядит следующим образом:

- для настройки QOS в class-map можно использовать COS, DSCP, IP-Precedence или ACL.
- примените QoS типа class-map к QoS типа policy-map. Для разных типов class-map настройте разные очереди, управление трафиком, перемаркировку и другие операции. Пакеты,

которые не совпадают ни с одной картой классов, будут классифицироваться как class-default, связанному с очередью по умолчанию 0 (не могут быть настроены с использованием WDRR).

- для различных классов трафика (после применения class-map), поддерживаются очереди от 1 до 7, 0 зарезервировано для системы и не может быть настроено пользователем.

- одна и та же карта политик может применяться к нескольким интерфейсам.

- только одна карта политик входящего трафика и одна карта политик исходящего трафика могут быть одновременно настроены на интерфейсе.

10.1.2 Настройка

Ниже приведены данные, которые следует учитывать при настройке QoS:

- На интерфейсе Linkagg невозможно настроить политики QoS;

- Классификация трафика возможна только на входящих портах;

- В каждой карте классов (class-map) может быть несколько списков ACL. Список ACL может содержать несколько записей контроля доступа;

- Применение политик классификации на уровне виртуального интерфейса коммутатора невозможно.

Для настройки политики QoS обычно требуется следующее:

- Разделите трафик на категории/классы;

- Настройте политики, применяемые к классам трафика;

- Привяжите политики к интерфейсам.

10.1.2.1 Классификация трафика с помощью списков ACL

Классифицировать IP-трафик можно с помощью списков контроля доступа (ACL). Ниже показано, как создать ACL для IP-трафика. Выполните шаги в режиме привилегированной консоли Exec.

- Настройте терминал;

- «ip access-list ACCESS-LIST-NAME», где ACCESS-LIST-NAME - имя списка ACL IP;

- Создайте записи ACE. Повторяйте этот по мере необходимости (для получения более подробной информации обратитесь к руководству по настройке ACL).

В следующем примере показано, как разрешить доступ только хостам в трех указанных подсетях. Если IP-адрес источника хоста не соответствует данным в списке доступа, доступ отклоняется.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте списки ACL и записи контроля доступа ACE.

```
Switch(config)# ip access-list ip-acl
Switch(config-ip-acl)# permit any 128.88.12.0 0.0.0.255 any
Switch(config-ip-acl)# permit any 28.88.0.0 0.0.255.255 any
Switch(config-ip-acl)# permit any 11.0.0.0 0.255.255.255 any
Switch(config-ip-acl)# exit
```

NOTE Для удаления списка контроля доступа (ACL) используйте команду «no ip access-list» в глобальном режиме настройки. Для удаления записи о доступе (ACE) используйте команду «no sequence-num» в режиме настройки ACL.

Терминология:

- ACL: Список контроля доступа;
- ACE: Запись внутри списка контроля доступа.

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show access-list ip ip-acl
ip access-list ip-acl
  10 permit any 128.88.12.0 0.0.0.255 any
  20 permit any 28.88.0.0 0.0.255.255 any
  30 permit any 11.0.0.0 0.255.255.255 any
```

10.1.2.2 Создание class-map (карты классов)

Ниже показана классификация IP-трафика по физическим портам с использованием карт классов. Это включает в себя создание карты классов и определение критерия соответствия. В данном случае это настройка карты классов с именем cmap1 с одним критерием: список доступа IP ip-acl, который разрешает трафик от любого источника в любое место назначения.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте списки контроля доступа (ACL) и записи контроля доступа (ACE).

```
Switch(config)# ip access-list ip-acl
Switch(config-ip-acl)# permit any any any
Switch(config-ip-acl)# quit
```

Шаг 3. Создайте карту классов и сопоставьте ее с ACL.

```
Switch(config)# class-map cmap1
Switch (config-cmap)# match access-group ip-acl
Switch (config-cmap)# quit
```

NOTE

- Оператор match-any используется для выполнения логического ИЛИ в рамках данной карты классов. Должен быть выполнен хотя бы один или несколько критериев соответствия. `match-any` – режим по умолчанию.

- Оператор match-all используется для выполнения логического И в рамках этой карты классов. Все критерии соответствия в карте классов должны быть строго соблюдены.

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

```
Switch# show class-map cmap1
    CLASS-MAP-NAME: cmap1 (match-any)
      match access-group: ip-acl
```

10.1.2.3 Создание policy-map (карты политик)

Ниже показано создание карты политик для классификации, ограничения и маркировки трафика. В этом примере создается карта политик и применяется к входящему интерфейсу. В этом примере IP ACL разрешает трафик из сети 10.1.0.0. При этом, если соответствующий трафик превышает среднюю скорость 48000 Кбит/с, он отбрасывается.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте списки контроля доступа (ACL) и записи ACE.

```
Switch(config)# ip access-list ip-acl
Switch(config-ip-acl)# permit any 10.1.0.0 0.0.255.255 any
Switch(config-ip-acl)# quit
```

Шаг 3. Создайте карту классов и сопоставьте ее с ACL.

```
Switch(config)# class-map type qos cmap1
Switch(config-cmap)# match access-group ip-acl
```

```
Switch(config-cmap)# quit
```

Шаг 4. Создайте карту политик и сопоставьте ее с картой классов; установите действие в режиме настройки policy-class.

```
switch(config)# policy-map type qos pmap1
switch(config-pmap)# class type qos cmap1
Switch(config-pmap-c)# policer color-blind cir 48000 cbs 10000 ebs 16000
violate drop
Switch(config-pmap-qos-c)# set traffic-class 5
Switch(config-pmap-qos-c)# set color yellow
Switch(config-pmap-c)# quit
Switch(config-pmap)# quit
```

NOTE Используйте параметр «no policy-map» в глобальном режиме настройки, чтобы удалить карту политик. Используйте параметр «no policer» в режиме настройки policy-class, чтобы удалить ограничитель. Используйте параметр «no set» в режиме настройки policy-class, чтобы сбросить значение приоритета или цвета маркировки по умолчанию. Значения по умолчанию: приоритет 0, а цвет маркировки — зелёный.

Шаг 5. Войдите в режим настройки интерфейса и примените карту политик.

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type qos input pmap1
Switch(config-if)# exit
```

NOTE Для каждого интерфейса поддерживается только одна карта политик на каждое направление. Команда «no service-policy input|output» используется для отмены применения карты политик.

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

```
Switch# show policy-map pmap1

  POLICY-MAP-NAME: pmap1 ( type qos)
    State: detached

    CLASS-MAP-NAME: cmap1
      match access-group: ip-acl
        set traffic-class       : 5
```

```
        set color                  : yellow
        policer color-blind cir 48000 cbs 10000 ebs 16000 violate drop
```

10.1.2.4 Создание агрегированного ограничителя для трафика

Ниже показано создание агрегированного ограничителя (контролируется совокупность факторов) трафика для классификации, контроля и маркировки. Создается агрегированный ограничитель и применяется к нескольким классам в рамках одной карты политик. В примере списки контроля доступа IP разрешают трафик из сети 10.1.0.0 и от хоста 11.3.1.1. Скорость трафика из сети 10.1.0.0 и от хоста 11.3.1.1 контролируется. Если трафик превышает среднюю скорость 48000 Кбит/с и обычный размер пакета превышает 8000 байт, трафик считается не соответствующим профилю и отбрасывается. Карта политик применена к входящему интерфейсу.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте списки контроля доступа (ACL) и записи ACE.

```
Switch(config)# ip access-list ip-acl1
Switch(config-ip-acl)# permit any 10.1.0.0 0.0.255.255 any
Switch(config-ip-acl)# exit
Switch(config)# ip access-list ip-acl2
Switch(config-ip-acl)# permit any host 11.3.1.1 any
Switch(config-ip-acl)# exit
```

Шаг 3. Создайте агрегированный policer.

```
Switch(config)# qos aggregate-policer transmit1 color-blind cir 48000 cbs
8000 ebs 10000 violate drop
```

NOTE Для удаления aggregate-policer используйте команду “no qos aggregate-policer”.

Шаг 4. Создайте карту классов и сопоставьте ее с ACL.

```
Switch(config)# class-map type qos cmap1
Switch(config-cmap)# match access-group ip-acl1
Switch(config-cmap)# exit
Switch(config)# class-map type qos cmap2
Switch(config-cmap)# match access-group ip-acl2
Switch(config-cmap)# exit
```

Шаг 5. Создайте карту политик и сопоставьте с ней карту классов; примените агрегированный policer в режиме конфигурации policy-class.

```
Switch(config)# policy-map type qos aggflow1
Switch(config-pmap)# class type qos cmap1
Switch(config-pmap-c)# aggregate-policer transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class type qos cmap2
Switch(config-pmap-c)# aggregate-policer transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

NOTE Чтобы удалить агрегированный полисер, используйте команду «no policer-aggregate» в режиме настройки классов политик.

Шаг 6. Войдите в режим настройки интерфейса и примените карту политик.

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type qos input aggflow1
Switch(config-if)# exitSwitch(config)# exit
```

Шаг 7. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 8. Проверка.

```
Switch# show qos aggregate-policer
Aggreate policer: transmit1
  color blind
  CIR 48000 kbps, CBS 8000 bytes, EBS 10000 bytes
  drop violate packets
```

10.1.3 Настройка очередности QoS

10.1.3.1 Настройка распределения трафика

Пакеты распределяются между различными классами алгоритмом SP и между очередями в одном классе алгоритмом WDRR (Weight Disclosure Reader Revision).

В следующем примере показана настройка распределения для исходящих очередей. В этом примере тип трафика 5 и 6 относится к классу 6, который является наивысшим приоритетом. Трафик типа 2 относится к классу 0, пропускная способность составляет 20%.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте карту классов и сопоставьте ее с классом трафика.

```
Switch(config)# class-map type traffic-class tc5
Switch(config-cmap-tc)# match traffic-class 5
Switch(config-cmap-tc)# exit

Switch(config)# class-map type traffic-class tc6
Switch(config-cmap-tc)# match traffic-class 6
Switch(config-cmap-tc)# exit

Switch(config)# class-map type traffic-class tc2
Switch(config-cmap-tc)# match traffic-class 2
Switch(config-cmap-tc)# exit
```

Шаг 3. Создайте карту политик и сопоставьте ее с картой классов; установите приоритет в режиме настройки policy-class.

```
Switch(config)# policy-map type traffic-class tc
Switch(config-pmap-tc)# class type traffic-class tc5
Switch(config-pmap-tc-c)# priority level 6
Switch(config-pmap-tc-c)# exit

Switch(config-pmap-tc)# class type traffic-class tc6
Switch(config-pmap-tc-c)# priority level 6
Switch(config-pmap-tc-c)# exit

Switch(config-pmap-tc)# class type traffic-class tc2
Switch(config-pmap-tc-c)# bandwidth percentage 20
Switch(config-pmap-tc-c)# exit
Switch(config-pmap-tc)# exit
```

Шаг 4. Войдите в режим настройки интерфейса и примените карту политик.

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type traffic-class tc
Switch(config-if)# exit
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

```
Switch# show qos interface eth-0-1 egress
TC  Priority Bandwidth  Shaping(kbps)  Drop-Mode    Max-Queue-Limit(Cell)    ECN
0   0        -          -              dynamic      level 10                  -
1   0        -          -              random-drop  596
Disable
2   0        20         -              dynamic      level 10                  -
3   0        -          -              tail-drop    2000                     2000
4   0        -          -              dynamic      level 10                  -
5   6        -          -              dynamic      level 10                  -
6   6        -          -              dynamic      level 10                  -
7   7        -          -              tail-drop    64                       -
```

10.1.3.2 Настройка сброса пакетов конца очереди (Tail Drop)

Отбрасывание пакетов конца очереди (tail drop) — это стандартный метод предотвращения перегрузки в каждой исходящей очереди. Ниже показана настройка порога отбрасывания пакетов в конце очереди для различных приоритетов и типов трафика. Выполните эти шаги в режиме привилегированного доступа Exec.

В этом примере настраивается пороговое значение для отбрасывания пакетов для 3-го класса трафика. В данном примере пороговое значение для отбрасывания пакетов составляет 2000.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте карту классов и сопоставьте ее с классом трафика.

```
Switch(config)# class-map type traffic-class tc3
Switch(config-cmap-tc)# match traffic-class 3
Switch(config-cmap-tc)# exit
```

Шаг 3. Создайте карту политик и сопоставьте ее с картой классов.

```
Switch(config)# policy-map type traffic-class tc
Switch(config-pmap-tc)# class type traffic-class tc3
```

Шаг 4. Установите пороговое значение для отбрасывания "хвостовых" пакетов в режиме настройки класса политики.

```
Switch(config-pmap-tc-c)# queue-limit 2000
Switch(config-pmap-tc-c)# exit
Switch(config-pmap-tc)# exit
```

Шаг 5. Войдите в режим настройки интерфейса и примените карту политик.

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type traffic-class tc
Switch(config-if)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

```
Switch# show qos interface eth-0-1 egress
TC  Priority Bandwidth  Shaping(kbps) Drop-Mode   Max-Queue-Limit(Cell)   ECN
0   0        -          -             dynamic     level 10                -
1   0        -          -             dynamic     level 10                -
2   0        -          -             dynamic     level 10                -
3   0        -          -             tail-drop   2000                    2000
4   0        -          -             dynamic     level 10                -
5   0        -          -             dynamic     level 10                -
6   0        -          -             dynamic     level 10                -
7   7        -          -             tail-drop   64                      -
```

10.1.3.3 Настройка алгоритма WRED

WRED предотвращает потери пакетов в конце очереди, выборочно отбрасывая пакеты, когда выходной интерфейс обнаруживает перегрузку. Отбрасывая часть пакетов на ранней стадии, не дожидаясь заполнения очереди, WRED предотвращает разрыв синхронизации TCP и, следовательно, повышает общую пропускную способность сети.

В следующем примере показана настройка порогового значения WRED для класса трафика 1. В этом примере максимальное пороговое значение равно 596, минимальное пороговое значение равно 596/8 = 71. Если количество буферизованных пакетов превышает минимальное пороговое значение, следующий пакет будет случайным образом отброшен.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте карту классов и сопоставьте ее с классом трафика.

```
Switch(config)# class-map type traffic-class tc1
Switch(config-cmap-tc)# match traffic-class 1
Switch(config-cmap-tc)# exit
```

Шаг 3. Создайте карту политик и сопоставьте ее с картой классов.

```
Switch(config)# policy-map type traffic-class tc
Switch(config-pmap-tc)# class type traffic-class tc1
```

Шаг 4. Установите пороговое значение для WRED в режиме настройки классов политик.

```
Switch(config-pmap-tc-c)# random-detect maximum-threshold 596
Switch(config-pmap-tc-c)# exit
Switch(config-pmap-tc)# exit
```

Шаг 5. Войдите в режим настройки интерфейса и примените карту политик.

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type traffic-class tc
Switch(config-if)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

```
Switch# show qos interface eth-0-1 egress
TC  Priority Bandwidth  Shaping(kbps)  Drop-Mode    Max-Queue-Limit(Cell)    ECN
0   0        -          -              dynamic      level 10                  -
1   0        -          -              random-drop  596
Disable
2   0        -          -              dynamic      level 10                  -
3   0        -          -              tail-drop    2000                     2000
4   0        -          -              dynamic      level 10                  -
5   0        -          -              dynamic      level 10                  -
6   0        -          -              dynamic      level 10                  -
7   7        -          -              tail-drop    64                       -
```

10.1.3.4 Оформление (ограничение) очереди

Весь трафик в исходящей очереди может быть отформатирован (ограничен), при этом весь избыточный трафик будет буферизован. Если буфер отсутствует, трафик отбрасывается.

В следующем примере показано создание механизма оформления потока для очереди 3. В этом примере, если трафик в очереди 3 превышает 1000 Мбит/с, он буферизуется.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте карту классов и сопоставьте ее с классом трафика.

```
Switch(config)# class-map type traffic-class tc3
Switch(config-cmap-tc)# match traffic-class 3
Switch(config-cmap-tc)# exit
```

Шаг 3. Создайте карту политик и сопоставьте ее с картой классов.

```
Switch(config)# policy-map type traffic-class tc
Switch(config-pmap-tc)# class type traffic-class tc3
```

Шаг 4. Установите пиковую скорость передачи информации (PIR) в режиме конфигурации класса политики.

```
Switch(config-pmap-tc-c)# shape rate pir 1000000
Switch(config-pmap-tc-c)# exit
Switch(config-pmap-tc)# exit
```

NOTE Используйте команду «no shape rate», чтобы отменить настройку пиковой скорости.

Шаг 5. Войдите в режим настройки интерфейса и примените карту политик.

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type traffic-class tc
Switch(config-if)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

```
Switch# show qos interface eth-0-1 egress
TC  Priority  Bandwidth  Shaping(kbps)  Drop-Mode    Max-Queue-Limit(Cell)    ECN
0   0         -          -              dynamic      level 10                  -
1   0         -          -              random-drop  596
Disable
2   0         20         -              dynamic      level 10                  -
3   0         -          1000000        tail-drop    2000                     2000
4   0         -          -              dynamic      level 10                  -
```

```
5   6        -          -              dynamic     level 10                  -
6   6        -          -              dynamic     level 10                  -
7   7        -          -              tail-drop   64                      -
```

10.1.4 Настройка конфигурации ограничения траффика

10.1.4.1 Контроль полосы пропускания порта

Скорость передачи трафика, принимаемого или передаваемого через физический интерфейс, может быть ограничена. Весь трафик, превышающий заданную скорость, будет отброшен.

В следующем примере показано создание ограничителя входящего трафика. Если входящий трафик превышает среднюю скорость 48000 Кбит/с, он отбрасывается.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и установите скорость ограничения скорости.

```
Switch(config)# interface eth-0-1
Switch(config-if)# qos policer input color-blind cir 48000 cbs 10000 ebs
20000 violate drop
Switch(config-if)# exit
```

NOTE Для удаления ограничителя для порта используйте команду «no port-policier input|output». Используемые выше операторы: CIR (Committed Information Rate), CBS (Committed Burst Size) и EBS (Excess Burst Size)

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show qos interface eth-0-1 statistics policer port input
Interface: eth-0-1
  input port policer:
   color blind
    CIR 48000 kbps, CBS 10000 bytes, EBS 20000 bytes
    drop violate packets
```

10.1.4.2 Настройка шейпинга (ограничения) полосы пропускания порта

Весь трафик, передаваемый через физический интерфейс, может быть ограничен, и весь избыточный трафик будет буферизован. Если буфер отсутствует, трафик отбрасывается.

В следующем примере показано создание ограничения скорости порта. В этом примере, если входящий трафик превышает 1000 Мбит/с, он буферизуется.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и установите ограничение максимальной пропускной способности трафика.

```
Switch(config)# interface eth-0-1
Switch(config-if)# qos shape rate pir 1000000
Switch(config-if)# exit
```

NOTE Чтобы удалить ограничение, используйте команду «no shape».

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch# show running-config interface eth-0-1
Building configuration...
!
interface eth-0-1
 service-policy type traffic-class tc
 qos policer input color-blind cir 48000 cbs 10000 ebs 20000 violate drop
 qos shape rate pir 1000000
!
```

10.1.4.3 Настройка маркировки трафика при достижении ECN

Пороговое значение ECN (Explicit Congestion Notification) — это заданное ограничение длины очереди на сетевых устройствах, превышение которого приводит к пометке пакетов вместо их отбрасывания.

Весь трафик, передаваемый через физический интерфейс, может быть ограничен и весь трафик, превышающий пороговое значение ECN, помечается.

В следующем примере показано, как настроить маркировку при достижении ECN. В этом примере, если занимаемая память буфера очереди превышает 500 ячеек, будет произведена маркировка.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте карту классов и сопоставьте ее с классом трафика.

```
Switch(config)# class-map type traffic-class tc5
Switch(config-cmap-tc)# match traffic-class 5
Switch(config-cmap-tc)# exit
```

Шаг 3. Создайте карту политик и сопоставьте ее с картой классов; установите приоритет.

```
Switch(config)# policy-map type traffic-class tc
Switch(config-pmap-tc)# class type traffic-class tc5
Switch(config-pmap-tc-c)# queue-limit 6000 ecn-threshold 500
Switch(config-pmap-tc-c)# exit
```

Шаг 4. Войдите в режим настройки интерфейса и примените карту политик.

```
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type traffic-class tc
Switch(config-if)# exit
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

```
Switch# show running-config interface eth-0-1
Building configuration...
!
class-map type traffic-class tc5
 match traffic-class 5
!
policy-map type traffic-class tc
 class type traffic-class tc5
  queue-limit 6000 ecn-threshold 500
!
interface eth-0-1
 service-policy type traffic-class tc
!
```

11 Руководство по настройке VPN

11.1 Настройка туннеля IPv4 GRE

11.1.1 Общие положения

11.1.1.1 Описание функции

Туннелирование — это технология инкапсуляции, которая использует один сетевой протокол для инкапсуляции пакетов другого и их передачи по виртуальному соединению типа «точка-точка». Виртуальное соединение называется туннелем. Туннелирование охватывает весь процесс от инкапсуляции данных до их передачи и деинкапсуляции.

11.1.1.2 Механизм работы

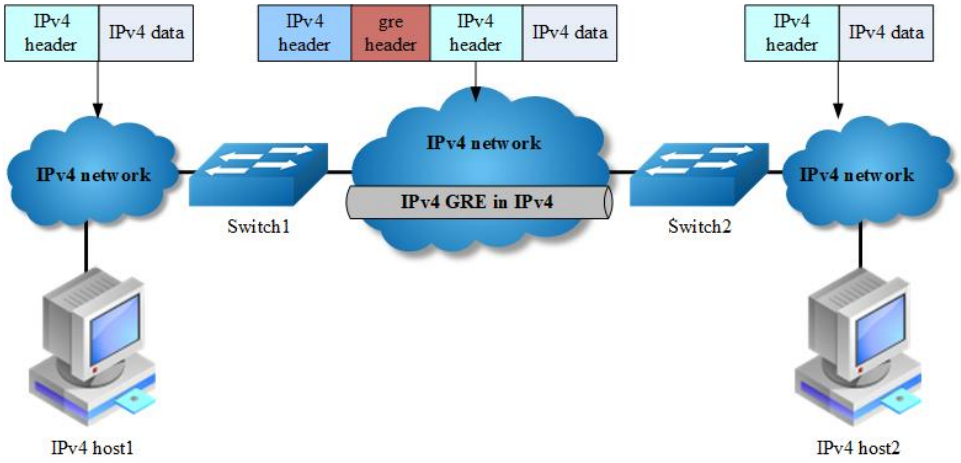


Рисунок 48 – Схема наложения IPv4 GRE поверх сети IPv4

Когда требуется связь между изолированными сетями IPv4, следует создать между ними туннель. Туннель по протоколу GRE, соединяющий два изолированных IPv4-сегмента, называется туннелем IPv4 GRE. В этом случае пакеты IPv4 инкапсулируются протоколом GRE поверх пакетов IPv4. В инкапсулированные пакеты GRE-туннель добавляет заголовок GRE, включающий ключ, последовательность, контрольную сумму и т. д. Для реализации туннеля GRE оба конечных узла туннеля должны поддерживать стеки протоколов IPv4.

Туннель IPv4 GRE обрабатывает пакеты следующим образом:

- Хост в сети IPv4 отправляет пакет IPv4 коммутатору Switch1, находящемуся в туннеле;
- После определения, на основе таблицы маршрутизации, необходимости пересылки пакета через туннель, коммутатор Switch1 инкапсулирует пакет, добавляет заголовок IPv4 и пересылает его через физический интерфейс туннеля;
- После получения пакета коммутатор Switch2 деинкапсулирует его;

- Коммутатор Switch2 пересылает пакет в соответствии с адресом назначения в деинкапсулированном IPv4-пакете. Если адрес назначения совпадает с адресом самого устройства, Switch2 передает IPv4-пакет для обработки. В процессе деинкапсуляции проверяется ключ GRE; обрабатываться может только тот ключ, который совпал с ключом пакета, в противном случае пакет отбрасывается.

IP-адрес источника и назначения туннеля назначается вручную, обеспечивая соединение точка-точка. Использование оверлейных туннелей позволяет взаимодействовать с изолированными сетями IPv4 без обновления инфраструктуры IPv4 между ними. Туннели могут быть настроены между пограничными маршрутизаторами или между пограничными маршрутизаторами и хостом.

Основное применение — обеспечение стабильных соединений, требующих регулярной защищенной связи между двумя пограничными маршрутизаторами или между удаленной конечной системой и пограничным маршрутизатором, а также для подключения к удаленным сетям.

11.1.2 Настройка

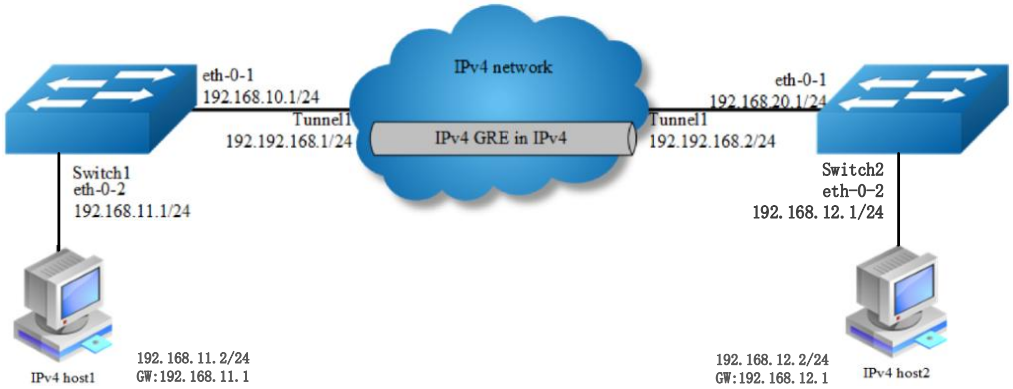


Рисунок 49 – IPv4 GRE туннель

Как видно из топологии, две сети IPv4 подключены через коммутаторы Switch1 и Switch2. Для соединения этих двух сетей необходим туннель IPv4 GRE между коммутаторами Switch1 и Switch2.

NOTE Для пересылки пакетов в туннеле необходим IPv4-маршрут. IPv4-адрес должен быть настроен на туннельном интерфейсе; в противном случае маршрут через этот туннельный интерфейс будет недействителен.

Если точный идентификатор коммутатора не указан, действия по настройке выполняются на всех коммутаторах топологии.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.10.1/24
Switch(config-if)# tunnel enable
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.11.1/24
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.20.1/24
Switch(config-if)# tunnel enable
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.12.1/24
Switch(config-if)# exit
```

Шаг 3. Настройка туннельного интерфейса.

Switch1:

```
Switch(config)# interface tunnel1
Switch(config-if)# tunnel mode gre
Switch(config-if)# tunnel source eth-0-1
Switch(config-if)# tunnel destination 192.168.20.1
Switch(config-if)# tunnel gre key 100
Switch(config-if)# ip address 192.192.168.1/24
Switch(config-if)# keepalive 5 3
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface tunnel1
Switch(config-if)# tunnel mode gre
Switch(config-if)# tunnel source eth-0-1
Switch(config-if)# tunnel destination 192.168.10.1
```

```
Switch(config-if)# tunnel gre key 100
Switch(config-if)# ip address 192.192.168.2/24
Switch(config-if)# keepalive 5 3
Switch(config-if)# exit
```

Шаг 4. Настройте статический маршрут.

Switch1:

```
Switch(config)# ip route 192.168.20.0/24 192.168.10.2
Switch(config)# ip route 192.168.12.0/24 tunnel1
```

Switch2:

```
Switch(config)# ip route 192.168.10.0/24 192.168.20.2
Switch(config)# ip route 192.168.11.0/24 tunnel1
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Switch1:

```
Switch# show interface tunnel1
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Internet primary address:
    192.192.168.1/24 pointopoint 192.192.168.255
  Tunnel protocol/transport GRE/IP, Status Valid
  Tunnel source 192.168.10.1(eth-0-1), destination 192.168.20.1
  Tunnel DSCP inherit,  Tunnel TTL 255
  Tunnel GRE key enable: 100
  Tunnel GRE keepalive enable, Send period: 5, Retry times: 3
  0 packets input, 0 bytes
  0 packets output, 0 bytes
```

Switch2:

```
Switch# show interface tunnel1
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Internet primary address:
```

```
  192.192.168.2/24 pointopoint 192.192.168.255
Tunnel protocol/transport GRE/IP, Status Valid
Tunnel source 192.168.20.1(eth-0-1), destination 192.168.10.1
Tunnel DSCP inherit,  Tunnel TTL 255
Tunnel GRE key enable: 100
Tunnel GRE keepalive enable, Send period: 5, Retry times: 3
0 packets input, 0 bytes
0 packets output, 0 bytes
```

11.2 Настройка туннеля IPv4 ERSPAN

11.2.1 Общие положения

11.2.1.1 Описание функции

ERSPAN (Encapsulated Remote Switch Port Analyzer) — это технология зеркалирования удаленных портов уровня 3, которая работает путем копирования пакетов и отправки их через туннель на удаленное устройство мониторинга, что позволяет пользователю анализировать такие данные (отзеркалированные пакеты) для отладки и устранения неполадок.

11.2.2 Примеры конфигурации

11.2.2.1 Настройка ERSPAN с одним адресом назначения

Топология

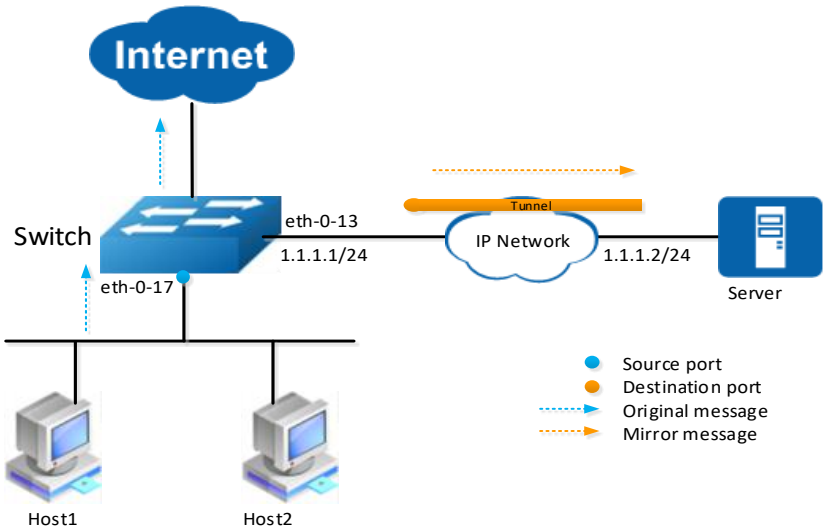


Рисунок 50 – Топология IPv4 ERSPAN туннель (один адрес назначения)

Этапы настройки

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

```
Switch(config)# interface loopback0
Switch(config-if)# ip address 192.168.1.1/32
Switch(config-if)# exit
Switch(config)# interface eth-0-13
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# exit
```

Шаг 3. Настройка туннельного интерфейса.

```
Switch(config)# interface tunnel0
Switch(config-if)# tunnel mode erspan
Switch(config-if)# tunnel source 192.168.1.1
Switch(config-if)# tunnel destination 1.1.1.2
Switch(config-if)# exit
```

Шаг 4. Настройте порты для анализа и целевой порт для отправки пакетов зеркалирования.

```
Switch(config)# monitor session 1 source interface eth-0-17 both
Switch(config)# monitor session 1 destination interface tunnel0
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

```
Switch# show interface tunnel0
Interface tunnel0
  Interface current state: UP
  Hardware is Tunnel
  Index 9216 , Metric 0 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport gre/erspan, Status Valid
  Tunnel source 192.168.1.1(loopback0)
  Tunnel destination 1.1.1.2
```

```
Tunnel DSCP inherit,  Tunnel TTL 254
Tunnel GRE key disable
Tunnel extend header disable
```

11.2.2.2 Настройка ERSPAN с несколькими адресами назначения

Топология

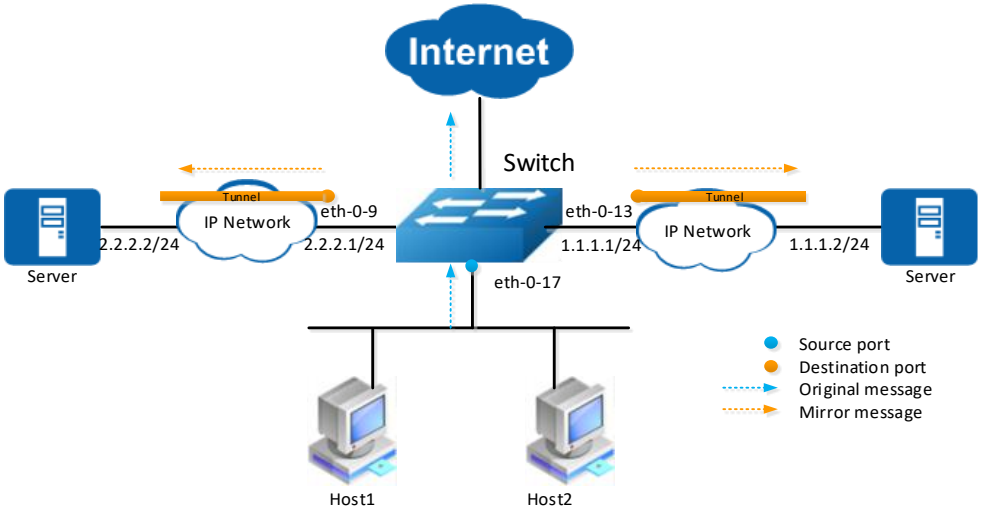


Рисунок 51 – IPv4 ERSPAN туннель (несколько адресов назначения)

Этапы настройки

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

```
Switch(config)# interface loopback0
Switch(config-if)# ip address 192.168.1.1/32
Switch(config-if)# exit
Switch(config)# interface eth-0-13
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# exit
Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 2.2.2.1/24
Switch(config-if)# exit
```

Шаг 3. Настройка туннельного интерфейса.

```
Switch(config)# interface tunnel0
Switch(config-if)# tunnel mode erspan ecmp-dst-gre
Switch(config-if)# tunnel source 192.168.1.1
Switch(config-if)# tunnel ecmp-destination 2.2.2.2
Switch(config-if)# tunnel ecmp-destination 1.1.1.2
Switch(config-if)# exit
```

Шаг 4. Настройте порты для анализа и целевой порт для отправки пакетов зеркалирования.

```
Switch(config)# monitor session 1 source interface eth-0-17 both
Switch(config)# monitor session 1 destination interface tunnel0
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

```
Switch# show interface tunnel0
Interface tunnel0
  Interface current state: UP
  Hardware is Tunnel
  Index 9216 , Metric 0 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport gre/ecmp-dst, Status Valid
  Tunnel source 192.168.1.1(loopback0)
  Tunnel ecmp-destination 2.2.2.2
                          1.1.1.2
  Tunnel DSCP inherit,  Tunnel TTL 254
  Tunnel GRE key disable
  Tunnel extend header disable
```

11.3 Настройка UDLD

11.3.1 Общие положения

11.3.1.1 Описание функции

Протокол обнаружения однонаправленного соединения (Unidirectional Link Detection) — это протокол, который можно использовать для обнаружения и отключения односторонних

соединений до того, как они создадут опасные ситуации, такие как сетевые петли или другие сбои в работе сети.

11.3.2 Настройка

Следующие параметры конфигурации одинаковы на коммутаторах Switch1 и Switch2.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и включите UDLD.

```
Switch(config)# interface eth-0-9
Switch(config-if)# no shutdown
Switch(config-if)# udld port
Switch(config-if)# exit
```

Шаг 3. Включите UDLD глобально.

```
Switch(config)# udld enable
```

Шаг 4. Установите интервал отправки сообщений (необязательно).

Если значение не указано, используется значение по умолчанию: 15 секунд.

```
Switch(config)# udld message interval 10
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Switch1:

```
Switch# show udld eth-0-9
Interface eth-0-9
---
UDLD mode          : normal
Operation state    : Bidirectional
Message interval   : 10
Message timeout    : 3
  Neighbor 1
  ---
  Device ID        : 4c7b.8510.ab00
  Port ID          : eth-0-9
```

```
  Device Name      : Switch
  Message interval: 10
  Message timeout : 3
  Link Status      : bidirectional
  Expiration time : 29
```

Switch2:

```
Switch# show udld eth-0-9
Interface eth-0-9
---
UDLD mode        : normal
Operation state : Bidirectional
Message interval: 10
Message timeout : 3
  Neighbor 1
  ---
  Device ID        : 28bc.83db.8400
  Port ID          : eth-0-9
  Device Name      : Switch
  Message interval: 10
  Message timeout : 3
  Link Status      : bidirectional
  Expiration time : 23
```

11.4 Настройка ERPS

11.4.1 Общие положения

11.4.1.1 Описание функции

Протокол ERPS повышает доступность и надежность кольцевых сетей Ethernet. В случае обрыва оптоволокна система ERPS восстанавливается менее чем за одну секунду, часто менее чем за 50 миллисекунд.

Основная идея описывается следующим образом. ERPS работает путем объявления домена ERPS на одном кольце. В этом кольцевом домене один коммутатор, или узел, назначается главным узлом, а все остальные узлы — транзитными узлами. Один порт главного узла назначается в качестве основного порта главного узла для связи с кольцом; другой порт назначается в качестве вторичного порта главного узла для связи с кольцом. В нормальном режиме работы главный узел блокирует вторичный порт для всего трафика, не относящегося к ERPS, тем самым предотвращая образование петли в кольце. Сообщения Keep-alive отправляются главным узлом через заданный интервал времени. Транзитные узлы в кольцевом домене будут пересылать сообщения ERPS. При отказе канала главный узел обнаружит это либо путем получения сообщения о разрыве связи, отправленного смежным узлом, либо по истечении

времени ожидания сообщения Keep-alive. После обнаружения отказа канала главный узел откроет вторичный порт для передачи данных, чтобы перенаправить трафик.

11.4.1.2 Предыстория

В сетях второго уровня обычно используются резервные каналы связи для повышения надежности сети; резервные каналы могут приводить к образованию кольцевых цепей, и для решения этой проблемы можно использовать протокол STP. Протокол STP, разработанный IEEE, является стандартным протоколом защиты кольцевых цепей и широко используется; однако STP ограничен размером сети, а скорость сходимости зависит от топологии. Время сходимости STP обычно составляет секунды, и чем больше диаметр сети, тем дольше время сходимости. Использование RSTP/MSTP может сократить время сходимости, но оно не может удовлетворить требованиям аудио/видеосвязи и других услуг более высокого качества. Для сокращения времени сходимости и устранения влияния размера сети был создан протокол ERPS. ERPS — это протокол канального уровня, он предотвращает широковещательную передачу, вызванную петлями данных; при обрыве одного канала связи в сети Ethernet используется резервный канал для быстрого восстановления связи между узлами. По сравнению с протоколом STP, протокол ERPS обладает более быстрой скоростью сходимости топологии (менее 50 мс), при этом время сходимости не зависит от количества узлов.

11.4.1.3 Основные понятия

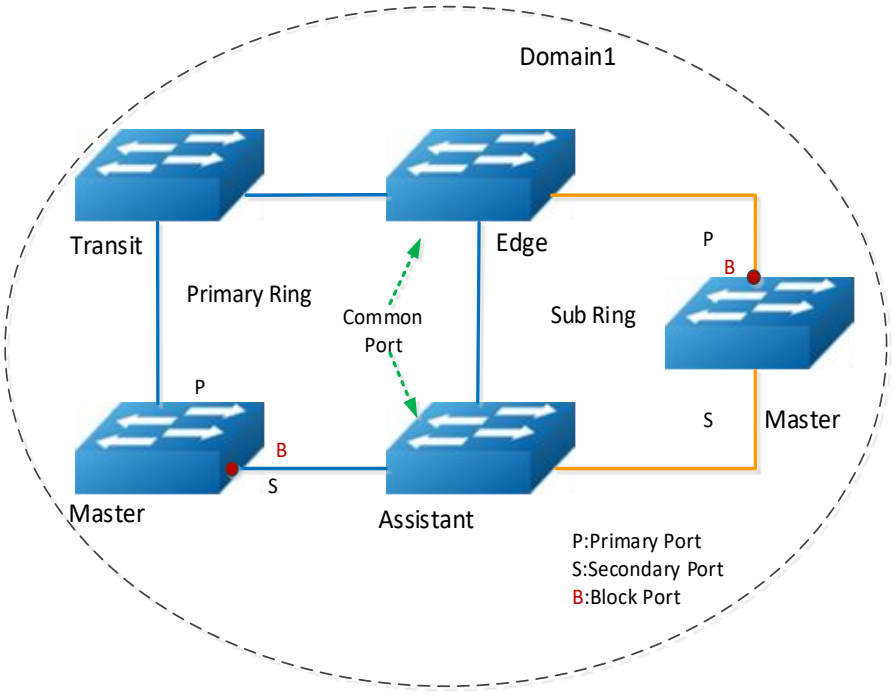


Рисунок 52 – ERPS топология

ERPS Домен

Домен ERPS — это топология, управляемая протоколом ERPS. Идентификатор домена — это уникальный идентификатор домена ERPS. ERPS включает в себя взаимосвязанные устройства с одинаковым идентификатором домена и управляющей VLAN. Одно устройство может присоединиться к нескольким доменам ERPS.

ERPS кольца

Каждое кольцо ERPS имеет соответствующую топологию Ethernet кольцевого типа, которая обозначается идентификатором кольца ERPS (ERPS Ring ID). Один домен ERPS содержит одно или несколько колец ERPS, одно из которых является основным, а остальные — второстепенными. В условиях однокольцевой архитектуры кольцо может быть настроено как основное, так и как второстепенное.

Тип кольца ERPS

- Single ring: Все устройства в однокольцевой сети находятся в одном домене ERPS.
- Intersecting ring: Все устройства в пересекающемся кольце находятся в одном домене ERPS.
- Tangetial ring: содержит два одиночных кольца, требует двух доменов, каждое кольцо находится в своем собственном домене ERPS domain.

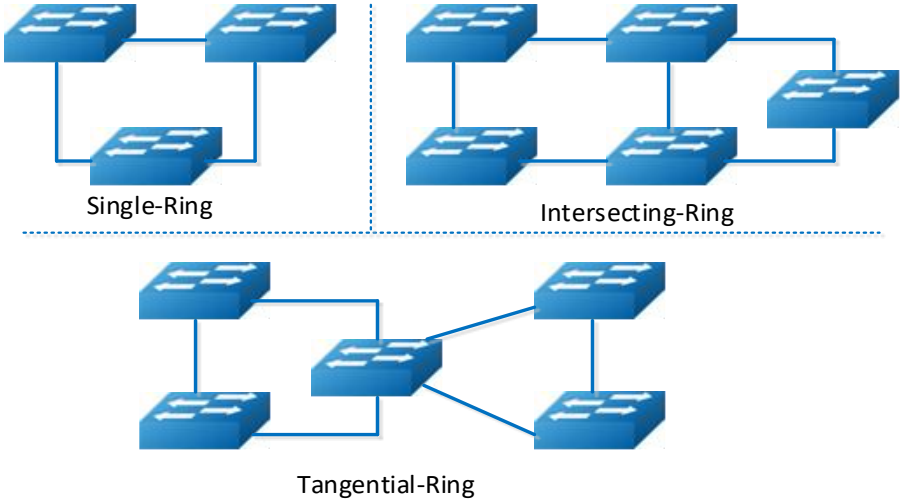


Рисунок 53 – Типы кольца ERPS

Управляющая VLAN ERPS:

Каждый домен ERPS может иметь две управляющие VLAN — основную управляющую VLAN и второстепенную. Сообщения протокола ERPS основного кольца будут пересылаться в основную управляющую VLAN, а сообщения протокола ERPS второстепенных колец — в второстепенную VLAN. В управляющих VLAN передаются только сообщения протокола ERPS.

Главный узел (master):

Каждый коммутатор в кольцевой цепи называется узлом. Главный узел — это основной узел принятия решений и управления в кольцевой системе ERPS, который выполняет

обнаружение отказа и принимает меры. Каждая кольцевая система ERPS должна иметь только один главный узел.

Транзитный узел (transit):

Другие узлы в кольцевой сети, за исключением главного узла, могут называться транзитными узлами. Транзитный узел передает пакет «Hello», отслеживает непосредственно подключенные каналы ERPS и уведомляет главный узел о событии типа DOWN.

Edge узел и вспомогательный узел (Assistant)

В домене, содержащим основное и вторичные кольца, при пересечении подкольца с основным кольцом образуются два узла пересечения; одно из них называется edge узлом, а другое — вспомогательным узлом.

Узел Edge и узел Assistant формируют вторичные подкольца, при этом являясь главным и транзитным узлами в основном кольце.

Основной порт и резервный порт

Основной и резервный порты являются портами Ethernet. Роли интерфейса определяются пользовательской конфигурацией. Главный узел отправляет пакеты «Hello» с основного порта; если резервный порт принимает этот пакет, это означает, что сеть исправна, и резервный порт следует заблокировать, чтобы предотвратить зацикливание. Если резервный порт не может принять пакет «Hello» в течение указанного времени, это означает, что сеть неисправна, и резервный порт следует разблокировать, чтобы обеспечить нормальную работу сети. Основной и резервный порты транзитного узла - один и тот же порт. Роли интерфейса определяются пользовательской конфигурацией.

Common/Edge порт

Edge узел (вспомогательный узел) подключается к двум портам вторичного кольца: один из них — common порт, а другой — edge порт.

Типы сообщений протокола ERPS:

- Сообщение Hello: отправляется основным портом главного узла и проверяет целостность сетевого соединения;

- Сообщение Link down: когда состояние соединения меняется с активного на неактивное, сообщение отправляется транзитным узлом, граничным узлом или вспомогательным граничным узлом этого соединения напрямую, уведомляя главный узел о том, что соединение в кольце оборвано;

- Сообщение Ring-up flush fdb: сообщение о восстановлении и обновлении кольца; отправляется главным узлом, уведомляет транзитный узел, граничный узел или вспомогательный узел о необходимости обновления каждой FDB и открывает резервный порт для обработки трафика перегрузки;

- Сообщение Ring-down flush fdb: сообщение о сбое кольцевой цепи; отправляется главным узлом, уведомляет транзитный узел, граничный узел или вспомогательный граничный узел о необходимости обновления каждой FDB;

- Сообщение Edge Hello: отправляется граничным узлом и доставляется вспомогательному граничному узлу того же вторичного под-кольца. Под-кольцо проверяет целостность соединения основного кольца, в котором передается сообщение;

- Сообщение о серьезной неисправности: неисправность основного кольцевого канала. Если вспомогательный граничный узел не получает сообщение Edge Hello от граничного узла в течении определенного времени, он отправляет граничному узлу сообщение о такой неисправности, уведомляя о сбое основного кольцевого канала в домене.

11.4.1.4 Принцип работы

Автомат опроса:

Главный узел будет периодически отправлять hello сообщение через свой основной порт, которое будет проходить через каждый транзитный узел в кольце. Если ГУ сможет получить отправленное им приветственное сообщение, это означает, что кольцо рабочее, и главный узел блокирует вторичный порт; в противном случае, если ГУ не может получить приветственное сообщение в течение определенного времени (таймер сбоя), это будет считаться сбоем связи, главный узел переходит в состояние отказа и открывает вторичный.

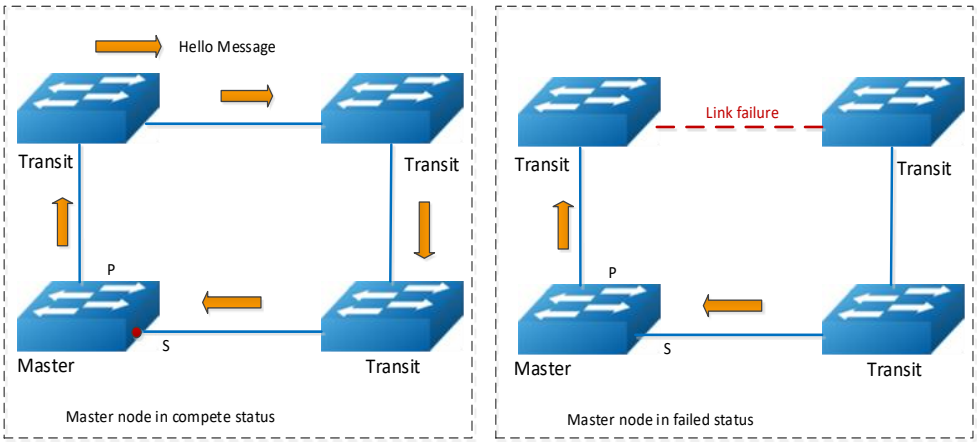


Рисунок 1-6 Статус главного узла

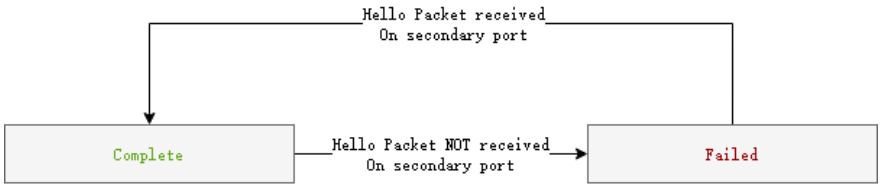


Рисунок 1-7 Диаграмма изменений статуса главного узла

Когда статус главного узла меняется с complete на failed, он отправляет сообщение ring-down flush fdb, чтобы уведомить другой узел о необходимости обновления FDB; когда статус меняется с failed на complete, он отправляет сообщение ring-up flush fdb, уведомляя другой узел о необходимости обновления FDB и открывает заблокированный порт.

Механизм оповещения о сбоях в работе транзитного узла

Транзитный узел будет отслеживать состояние подключенного напрямую канала ERPS и сообщать о сбоях канала главному узлу. Транзитный узел может находиться в одном из трех состояний:

- Когда основной и резервный порты транзитного узла находятся в состоянии «включено», транзитный узел переходит в состояние «подключен». При обнаружении обрыва связи на основном или резервном порту он переходит из состояния «подключен» в состояние «отключен» и отправляет сообщение об отключении связи главному узлу, чтобы уведомить его о сбое соединения;
- Когда порт транзитного узла, находившийся в состоянии "канал связи неактивен", восстанавливается, транзитный узел переходит в состояние "предварительная пересылка" и блокирует восстановленный порт. В тот момент, когда основной и резервный порты транзитного узла не сразу получают это уведомление, главный узел не может сразу узнать об этом, поэтому его резервный порт остается открытым. Если транзитный узел сразу же возвращается в состояние "канал связи активен", это может вызвать широковещательную петлю в кольцевой сети, поэтому транзитный узел первым перейдет в состояние "предварительная пересылка";
- Когда транзитный узел в состоянии предварительной пересылки получает сообщение FDB о завершении соединения от главного узла, он переходит в состояние установления связи. Если сообщение FDB о завершении соединения теряется во время перехода, и транзитный узел не может получить его в течение определенного времени, он переходит в состояние установления связи и открывает временно заблокированный порт.

NOTE При выходе из строя канала связи между основным и дополнительным кольцами, сообщение о разрыве связи будет отправлено только главному узлу основного кольца.

Edge и Assistant Edge узлы – механизм обнаружения каналов вторичных колец

Edge узел периодически отправляет сообщение Edge Hello вспомогательному граничному узлу, сообщение с основным управляющим VLAN передается в основное кольцо.

При отказе основного канала связи, если выходит из строя только один канал, sub-кольцо остается цельным:

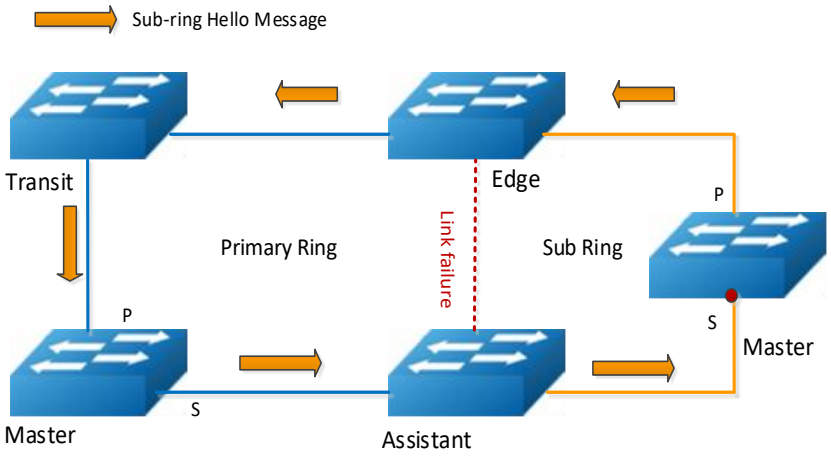


Рисунок 54 – Сетевая топология соединений sub-кольца

Если канал связи между основным и дополнительным кольцами выйдет из строя, и при этом произойдет прерывание связи на другом канале в основном кольце, в таком случае вспомогательный граничный узел не сможет получить сообщение Edge Hello и отправит сообщение о серьезной неисправности с указанием VLAN управления sub-кольцом. В свою очередь граничный узел получит сообщение о серьезной неисправности и заблокирует свой граничный порт:

NOTE Edge узел блокирует Edge интерфейс, чтобы предотвратить образование петли из нескольких sub-колец.

Если имеется только одно sub-кольцо, граничному узлу не нужно блокировать граничный интерфейс. Пользователь может отключить механизм проверки граничного и вспомогательного узлов с помощью команды «erps ring srpt disable».

Если на вторичный порт главного узла sub-кольца не поступает сообщение "Hello" в течение определенного времени, главный узел sub-кольца переходит в состояние "сбой" и открывает вторичный порт.

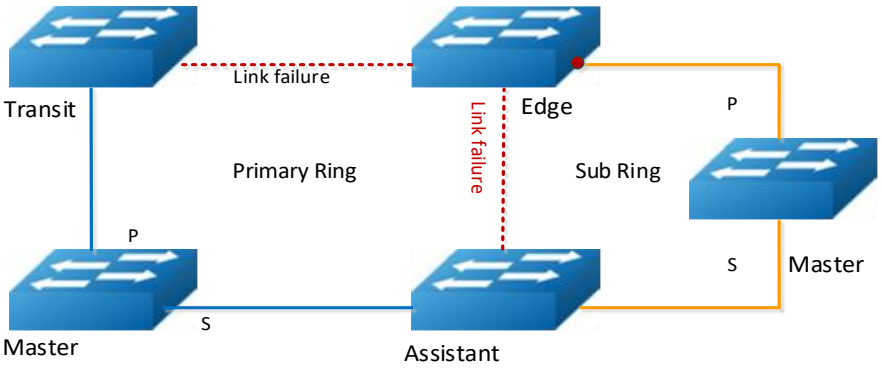


Рисунок 55 – Master узел sub-кольца перешёл в состояние сбоя

Если в sub-кольце восстанавливается связь, то вторичный порт главного узла sub-кольца получает сообщение «hello», переходит в состояние «complete», блокирует вторичный порт и

отправляет сообщение «ring-up flush fd»; после получения граничным узлом сообщения «ring-up flush fdb», он открывает граничный порт:

В обычной сети ERPS вторичный порт главного узла заблокирован, трафик данных будет передаваться только по оранжевым стрелкам, а пропускная способность коммутаторов Switch2, Switch3 и Switch4 не будет использоваться. Для повышения эффективности использования каналов связи в одном физическом контуре могут быть два логических кольца ERPS, каждый из которых соответствует определенной физической топологии. Каждый контур будет независимо проверять целостность канала связи, блокируя или открывая соответствующий порт; они не будут влиять друг на друга. Поэтому в одном физическом контуре может быть два заблокированных порта. Каждый логический сегмент использует свой диапазон VLAN данных, и каждый заблокированный порт действителен только в пределах своего сегмента ERPS. Трафик, принадлежащий разным логическим кольцам, может проходить по разным путям, обеспечивая распределение нагрузки и повышая эффективность использования каналов связи.

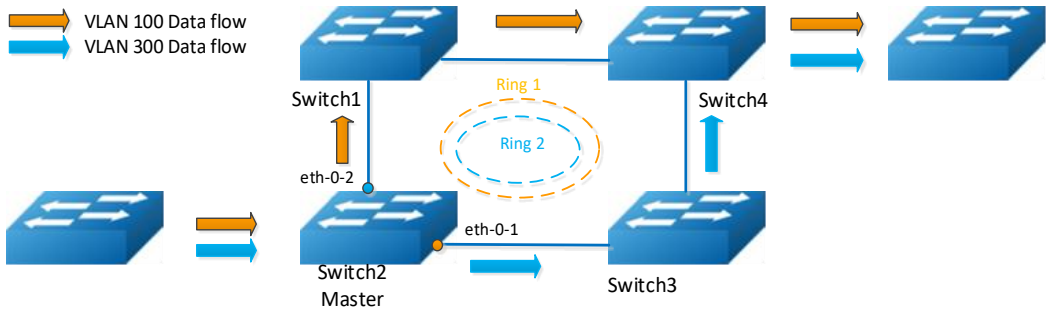


Рисунок 56 – Распределение нагрузки в схеме с двумя sub-кольцами

VLAN100-200 подключается к кольцу 1, VLAN300-400 — к кольцу 2. Кольца 1 и 2 блокируют eth-0-1 и eth-0-2 по отдельности, затем eth-0-1 блокирует только данные VLAN100-200, а eth-0-2 — только данные VLAN300-400. Затем поток данных VLAN100-200 передается через оранжевые стрелки, а поток данных VLAN300-400 — через синие стрелки, обеспечивая распределение нагрузки.

11.4.2 Настройка

ERPS — это протокол с программным и динамическим управлением состояния. Основное требование — включить ERPS на необходимых устройствах и правильно настроить ERPS под определенную сетевую топологию.

В этом разделе приведены примеры конфигурации ERPS для типичных сетевых топологий.

11.4.2.1 Настройка ERPS для однокольцевой топологии

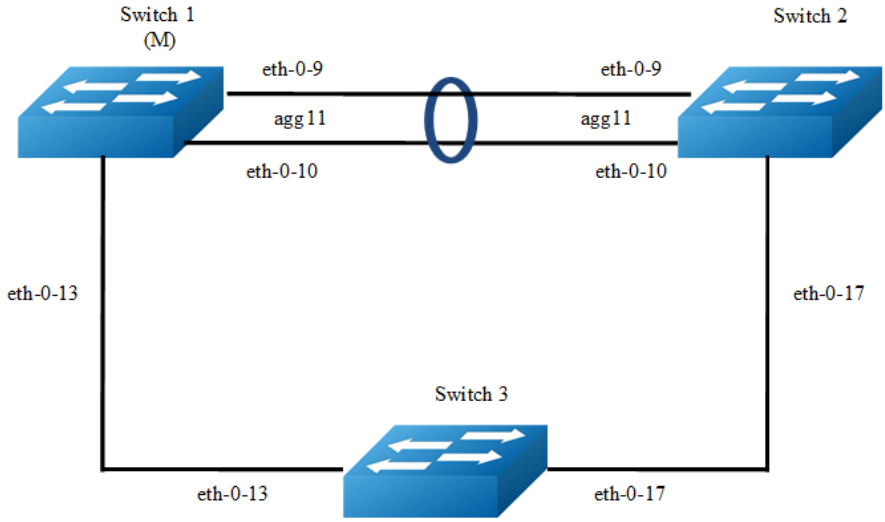


Рисунок 57 – Топология ERPS - одно кольцо

Настройте одинаковый домен и кольцо ERPS на коммутаторах Switch1, Switch2 и Switch3. Коммутатор Switch1 настроен как главный узел ERPS, а два других коммутатора — как транзитные. Интерфейс agg11, имеющий два участника, eth-0-9 и eth-0-10, настроен как основной интерфейс на коммутаторе Switch1, а eth-0-13 — как дополнительный интерфейс.

NOTE Порты кольца ERPS должны быть настроены как транковые порты, разрешая прохождение трафика данных VLAN. Если коммутатор поддерживает стекирование, порт кольца ERPS не должен находиться на устройстве стекирования.

Порты, подключенные к кольцевой сети ERPS, должны быть настроены как члены управляющей VLAN, что позволит отправлять и получать пакеты ERPS.

Протокол STP на портах кольца ERPS необходимо отключить.

В качестве главного узла можно настроить только один узел.

Управляющая VLAN не должна быть настроена как интерфейс уровня 3.

На портах ERPS не следует включать mapping VLAN.

Native VLAN порта, подключенного к кольцу ERPS, не должна быть установлена как первичная управляющая VLAN или вторичная управляющая VLAN.

Если точный идентификатор коммутатора не указан, действия по настройке выполняются на всех коммутаторах топологии.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 15
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Как показано на схеме, интерфейсы eth-0-9 и eth-0-10 коммутаторов Switch1 и Switch2 соединяются с agg 11. Интерфейс eth-0-13 коммутаторов Switch1 и Switch3 напрямую связаны друг с другом. Интерфейс eth-0-17 коммутаторов Switch2 и Switch3 напрямую связаны друг с другом.

Конфигурация интерфейса agg 11 для коммутаторов Switch1 и Switch2:

```
Switch(config)# interface eth-0-9
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# static-channel-group 11
Switch(config-if)# exit

Switch(config)# interface eth-0-10
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# static-channel-group 11
Switch(config-if)# exit

Switch(config)# interface agg11
Switch(config-if)# spanning-tree port disable
```

Конфигурация интерфейса eth-0-13 для коммутаторов Switch1 и Switch3:

```
Switch(config)# interface eth-0-13
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
```

Конфигурация интерфейса eth-0-17 для коммутаторов Switch2 и Switch3:

```
Switch(config)# interface eth-0-17
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# spanning-tree port disable
Switch(config-vlan)# exit
```

Шаг 4. Создайте и включите домен ERPS.

Switch1:

```
Switch(config)# erps 11
Switch(config)# erps 11 primary control vlan 15
Switch(config)# erps 11 mstp instance 0
Switch(config)# erps 11 ring 1 level primary
Switch(config)# erps 11 ring 1 mode master
Switch(config)# erps 11 ring 1 primary interface agg11
Switch(config)# erps 11 ring 1 secondary interface eth-0-13
Switch(config)# erps 11 ring 1 enable
Switch(config)# erps 11 enable
```

Switch2:

```
Switch(config)# erps 11
Switch(config)# erps 11 primary control vlan 15
Switch(config)# erps 11 mstp instance 0
Switch(config)# erps 11 ring 1 level primary
Switch(config)# erps 11 ring 1 mode transit
Switch(config)# erps 11 ring 1 primary interface agg11
Switch(config)# erps 11 ring 1 secondary interface eth-0-17
Switch(config)# erps 11 ring 1 enable
Switch(config)# erps 11 enable
```

Switch3:

```
Switch(config)# erps 11
Switch(config)# erps 11 primary control vlan 15
Switch(config)# erps 11 mstp instance 0
Switch(config)# erps 11 ring 1 level primary
Switch(config)# erps 11 ring 1 mode transit
Switch(config)# erps 11 ring 1 primary interface eth-0-17
Switch(config)# erps 11 ring 1 secondary interface eth-0-13
Switch(config)# erps 11 ring 1 enable
Switch(config)# erps 11 enable
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Switch1.

```
Switch# show erps 11
ERPS domain ID: 11
ERPS domain name: ERPS0011
ERPS domain mode: normal
```

```
ERPS domain primary control VLAN ID: 15
ERPS domain sub control VLAN ID: 0
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS domain protected mstp instance: 0
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: master
ERPS ring 1 node state: complete
ERPS ring 1 primary interface name: agg11          state:unblock
ERPS ring 1 secondary interface name: eth-0-13     state:block
ERPS ring 1 stats:
Sent:
  total packets:51
  hello packets:47                    ring-up-flush-fdb packets:2
  ring-down-flush-fdb packets:2       link-down packets:0
  edge-hello packets:0                major-fault packets:0
Received:
  total packets:21
  hello packets:21                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0       link-down packets:0
  edge-hello packets:0                major-fault packets:0
```

Switch2.

```
Switch# show erps 11
ERPS domain ID: 11
ERPS domain name: ERPS0011
ERPS domain mode: normal
ERPS domain primary control VLAN ID: 15
ERPS domain sub control VLAN ID: 0
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS domain protected mstp instance: 0
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: transit
ERPS ring 1 node state: link up
ERPS ring 1 primary interface name: agg11          state:unblock
ERPS ring 1 secondary interface name: eth-0-17     state:unblock
ERPS ring 1 stats:
Sent:
  total packets:0
  hello packets:0                     ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0       link-down packets:0
  edge-hello packets:0                major-fault packets:0
Received:
  total packets:114
  hello packets:113                   ring-up-flush-fdb packets:1
```

```
  ring-down-flush-fdb packets:0       link-down packets:0
  edge-hello packets:0                major-fault packets:0
```

Switch3.

```
Switch# show erps 11
ERPS domain ID: 11
ERPS domain name: ERPS0011
ERPS domain mode: normal
ERPS domain primary control VLAN ID: 15
ERPS domain sub control VLAN ID: 0
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS domain protected mstp instance: 0
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: transit
ERPS ring 1 node state: link up
ERPS ring 1 primary interface name: eth-0-17       state:unblock
ERPS ring 1 secondary interface name: eth-0-13     state:unblock
ERPS ring 1 stats:
Sent:
  total packets:0
  hello packets:0                   ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0     link-down packets:0
  edge-hello packets:0              major-fault packets:0
Received:
  total packets:130
  hello packets:129                 ring-up-flush-fdb packets:1
  ring-down-flush-fdb packets:0     link-down packets:0
  edge-hello packets:0              major-fault packets:0
```

11.4.2.2 Настройка топологии пересекающихся колец

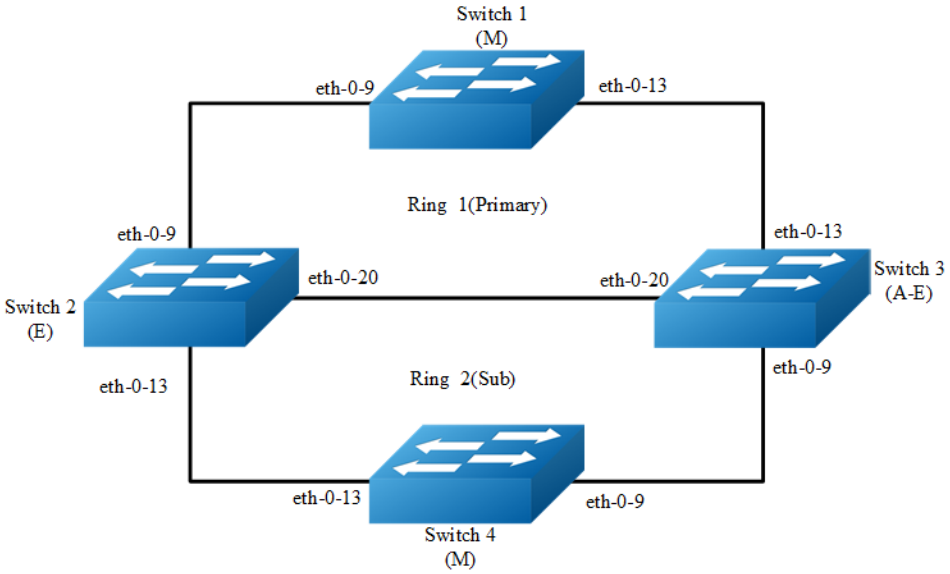


Рисунок 58 – ERPS пересекающиеся кольца

Настройте одинаковый домен ERPS на коммутаторах Switch1, Switch2, Switch3 и Switch4. Коммутаторы Switch1, Switch2 и Switch3 входят в основное кольцо ERPS 1, а коммутаторы Switch2, Switch3 и Switch4 — в sub-кольцо ERPS 2. Коммутатор Switch1 настроен как главный узел кольца ERPS 1, два других коммутатора — как транзитные узлы ERPS, а коммутатор Switch4 — как главный узел кольца ERPS 2. Кроме того, коммутатор Switch2 настроен как граничный узел, а коммутатор Switch3 — как вспомогательный граничный узел.

Порты, подключенные к кольцевой сети ERPS, должны быть настроены как транковые порты, позволяющие пропускать трафик данных VLAN.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 11,12
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

```
Switch(config)# interface eth-0-9
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 11,12
```

```
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit

Switch(config)# interface eth-0-13
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 11,12
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
```

Конфигурация интерфейса eth-0-20 для коммутаторов Switch2 и Switch3:

```
Switch(config)# interface eth-0-20
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 11,12
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
```

Шаг 4. Создайте и включите домен ERPS.

Switch1:

```
Switch(config)# erps 1
Switch(config)# erps 1 primary control vlan 11
Switch(config)# erps 1 sub control vlan 12
Switch(config)# erps 1 mstp instance 0
Switch(config)# erps 1 ring 1 level primary
Switch(config)# erps 1 ring 1 mode master
Switch(config)# erps 1 ring 1 primary interface eth-0-9
Switch(config)# erps 1 ring 1 secondary interface eth-0-13
Switch(config)# erps 1 ring 1 enable
Switch(config)# erps 1 enable
```

Switch2:

```
Switch(config)# erps 1
Switch(config)# erps 1 primary control vlan 11
Switch(config)# erps 1 sub control vlan 12
Switch(config)# erps 1 mstp instance 0
Switch(config)# erps 1 ring 1 level primary
Switch(config)# erps 1 ring 1 mode transit
Switch(config)# erps 1 ring 1 primary interface eth-0-9
Switch(config)# erps 1 ring 1 secondary interface eth-0-20
Switch(config)# erps 1 ring 1 enable

Switch(config)# erps 1 ring 2 level sub
Switch(config)# erps 1 ring 2 edge-mode edge
Switch(config)# erps 1 ring 2 edge interface eth-0-13
Switch(config)# erps 1 ring 2 common interface eth-0-20
```

```
Switch(config)# erps 1 ring 2 srpt disable
Switch(config)# erps 1 ring 2 enable
Switch(config)# erps 1 enable
```

Switch3:

```
Switch(config)# erps 1
Switch(config)# erps 1 primary control vlan 11
Switch(config)# erps 1 sub control vlan 12
Switch(config)# erps 1 mstp instance 0
Switch(config)# erps 1 ring 1 level primary
Switch(config)# erps 1 ring 1 mode transit
Switch(config)# erps 1 ring 1 primary interface eth-0-13
Switch(config)# erps 1 ring 1 secondary interface eth-0-20
Switch(config)# erps 1 ring 1 enable

Switch(config)# erps 1 ring 2 level sub
Switch(config)# erps 1 ring 2 edge-mode assistant-edge
Switch(config)# erps 1 ring 2 edge interface eth-0-9
Switch(config)# erps 1 ring 2 common interface eth-0-20
Switch(config)# erps 1 ring 2 enable
Switch(config)# erps 1 enable
```

Switch4:

```
Switch(config)# erps 1
Switch(config)# erps 1 sub control vlan 12
Switch(config)# erps 1 mstp instance 0
Switch(config)# erps 1 ring 2 level sub
Switch(config)# erps 1 ring 2 mode master
Switch(config)# erps 1 ring 2 primary interface eth-0-9
Switch(config)# erps 1 ring 2 secondary interface eth-0-13
Switch(config)# erps 1 ring 2 enable
Switch(config)# erps 1 enable
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Switch1.

```
Switch# show erps 1
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain mode: normal
ERPS domain primary control VLAN ID: 11
ERPS domain sub control VLAN ID: 12
ERPS domain hello timer interval: 1 second(s)
```

```
ERPS domain fail timer interval: 3 second(s)
ERPS domain protected mstp instance: 0
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: master
ERPS ring 1 node state: complete
ERPS ring 1 primary interface name: eth-0-9        state:unblock
ERPS ring 1 secondary interface name: eth-0-13     state:block
ERPS ring 1 stats:
Sent:
  total packets:1310
  hello packets:1303                  ring-up-flush-fdb packets:3
  ring-down-flush-fdb packets:4       link-down packets:0
  edge-hello packets:0                major-fault packets:0
Received:
  total packets:921
  hello packets:921                   ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0       link-down packets:0
  edge-hello packets:0                major-fault packets:0
```

Switch2.

```
Switch# show erps 1
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain mode: normal
ERPS domain primary control VLAN ID: 11
ERPS domain sub control VLAN ID: 12
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS domain protected mstp instance: 0
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: transit
ERPS ring 1 node state: link up
ERPS ring 1 primary interface name: eth-0-9        state:unblock
ERPS ring 1 secondary interface name: eth-0-20     state:unblock
ERPS ring 1 stats:
Sent:
  total packets:0
  hello packets:0                     ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0       link-down packets:0
  edge-hello packets:0                major-fault packets:0
Received:
  total packets:988
  hello packets:985                   ring-up-flush-fdb packets:2
  ring-down-flush-fdb packets:1       link-down packets:0
  edge-hello packets:0                major-fault packets:0
ERPS ring ID: 2
```

```
ERPS ring level: sub
ERPS ring 2 node mode: transit
ERPS ring 2 edge node mode: edge
ERPS ring 2 node state: link up
ERPS ring 2 edge interface name: eth-0-13       state: unblock
ERPS ring 2 common interface name: eth-0-20     state: unblock
EPRS ring 2 SRPT is disabled
ERPS ring 2 stats:
Sent:
  total packets:0
  hello packets:0                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
Received:
  total packets:858
  hello packets:856                  ring-up-flush-fdb packets:1
  ring-down-flush-fdb packets:1      link-down packets:0
  edge-hello packets:0               major-fault packets:0
```

Switch3.

```
Switch# show erps 1
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain mode: normal
ERPS domain primary control VLAN ID: 11
ERPS domain sub control VLAN ID: 12
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS domain protected mstp instance: 0
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: transit
ERPS ring 1 node state: link up
ERPS ring 1 primary interface name: eth-0-13       state:unblock
ERPS ring 1 secondary interface name: eth-0-20     state:unblock
ERPS ring 1 stats:
Sent:
  total packets:0
  hello packets:0                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
Received:
  total packets:645
  hello packets:644                  ring-up-flush-fdb packets:1
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
ERPS ring ID: 2
ERPS ring level: sub
```

```
ERPS ring 2 node mode: transit
ERPS ring 2 edge node mode: assistant edge
ERPS ring 2 node state: link up
ERPS ring 2 edge interface name: eth-0-9        state: unblock
ERPS ring 2 common interface name: eth-0-20     state: unblock
ERPS ring 2 stats:
Sent:
  total packets:0
  hello packets:0                       ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0         link-down packets:0
  edge-hello packets:0                  major-fault packets:0
Received:
  total packets:645
  hello packets:644                     ring-up-flush-fdb packets:1
  ring-down-flush-fdb packets:0         link-down packets:0
  edge-hello packets:0                  major-fault packets:0
```

Switch4.

```
Switch# show erps 1
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain mode: normal
ERPS domain primary control VLAN ID: 0
ERPS domain sub control VLAN ID: 12
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS domain protected mstp instance: 0
ERPS ring ID: 2
ERPS ring level: sub
ERPS ring 2 node mode: master
ERPS ring 2 node state: complete
ERPS ring 2 primary interface name: eth-0-9         state:unblock
ERPS ring 2 secondary interface name: eth-0-13      state:block
ERPS ring 2 stats:
Sent:
  total packets:814
  hello packets:810                     ring-up-flush-fdb packets:2
  ring-down-flush-fdb packets:2         link-down packets:0
  edge-hello packets:0                  major-fault packets:0
Received:
  total packets:774
  hello packets:774                     ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0         link-down packets:0
  edge-hello packets:0                  major-fault packets:0
Switch#
```

11.4.2.3 Настройка в топологии смежных колец

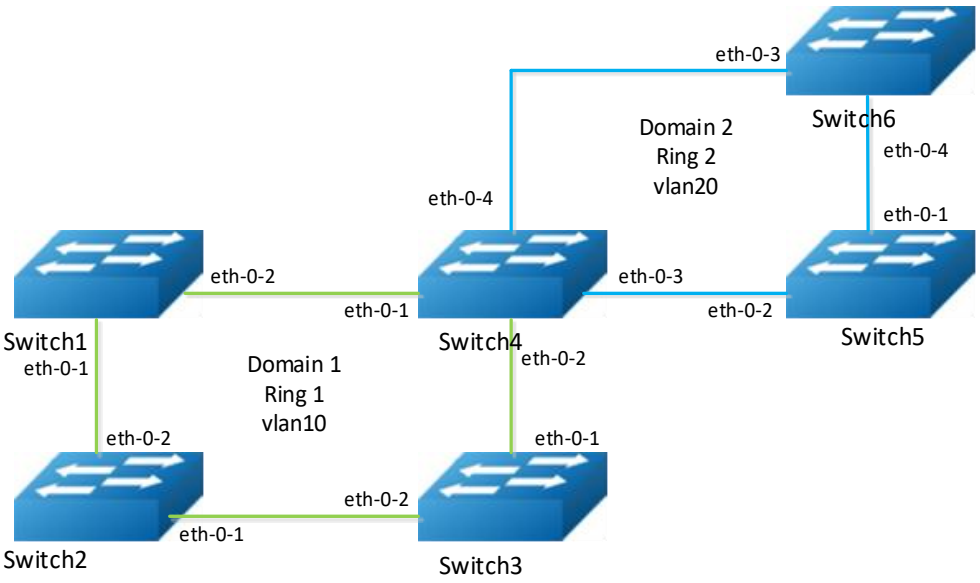


Рисунок 59 – Топология схемы сети смежных колец

Коммутаторы 1-6 образуют два кольца, протокол ERPS обеспечивает защиту этих двух колец за счет резервирования на уровне 2.

- В топологии два кольца без общих физических связей не подходят для конфигурации в режиме «основное кольцо – sub-кольцо». Их можно рассматривать как два независимых кольца внутри двух доменов ERPS.

- Настройте порты 1/2/3/4 как ring1 в домене erps domain1; 2 — главный узел, eth-0-1 — основной порт, eth-0-2 — дополнительный порт.

- Настройте порты 4/5/6 как ring2 в домене erps domain2; порт 6 — главный узел, eth-0-3 — основной порт, а eth-0-4 — дополнительный порт.

11.4.2.4 Этапы настройки

NOTE «SwitchX» указывает, что конфигурация одинакова для всех коммутаторов (Switch 1-6).

Шаг 1. Войдите в режим настройки.

```
SwitchX# configure terminal
```

Шаг 2. Настройка VLAN 10 для устройств кольца 1 (коммутаторы 1-4).

```
SwitchX(config)# vlan database
SwitchX(config-vlan)# vlan 10
```

```
SwitchX(config-vlan)# exit
SwitchX(config)# no ip igmp snooping vlan 10
```

NOTE Пакеты ERPS являются многоадресными, поэтому для управляющей VLAN необходимо отключить IGMP-snooping.

Шаг 3. Настройка VLAN 20 для устройств кольца 2 (коммутаторы 4-6).

```
SwitchX(config)# vlan database
SwitchX(config-vlan)# vlan 20
SwitchX(config-vlan)# exit
SwitchX(config)# no ip igmp snooping vlan 20
```

Шаг 4. Настройка атрибутов интерфейса.

```
SwitchX(config)# interface eth-0-X
SwitchX(config-if)# switchport
SwitchX(config-if)# no shutdown
SwitchX(config-if)# switchport mode trunk
SwitchX(config-if)# switchport trunk allowed vlan all
SwitchX(config-if)# spanning-tree port disable
SwitchX(config-if)# exit
```

NOTE Обозначение eth-0-X означает eth-0-1/eth-0-2/eth-0-3/eth-0-4, конфигурация одинакова.

Шаг 5. Настройка атрибутов интерфейса для коммутатора 4.

```
Switch4(config)# interface eth-0-1
Switch4(config-if)# switchport trunk allowed vlan remove 20
Switch4(config-if)# exit
Switch4(config)# interface eth-0-2
Switch4(config-if)# switchport trunk allowed vlan remove 20
Switch4(config-if)# exit
Switch4(config)# interface eth-0-3
Switch4(config-if)# switchport trunk allowed vlan remove 10
Switch4(config-if)# exit
Switch4(config)# interface eth-0-4
Switch4(config-if)# switchport trunk allowed vlan remove 10
Switch4(config-if)# exit
```

NOTE Удалите VLAN 20 на интерфейсе eth-0-1/eth-0-2 и VLAN 10 на интерфейсе eth-0-3/eth-0-4.

Шаг 6. Настройка Master узла Switch2 в домене 1.

```
Switch2(config)# erps 1
Switch2(config)# erps 1 primary control vlan 10
Switch2(config)# erps 1 ring 1 level primary
Switch2(config)# erps 1 ring 1 mode master
Switch2(config)# erps 1 ring 1 primary interface eth-0-1
Switch2(config)# erps 1 ring 1 secondary interface eth-0-2
Switch2(config)# erps 1 mstp instance 0
Switch2(config)# erps 1 ring 1 enable
Switch2(config)# end
```

Шаг 7. Настройка транзитного узла Switch1 в Domain1.

```
Switch1(config)# erps 1
Switch1(config)# erps 1 primary control vlan 10
Switch1(config)# erps 1 ring 1 level primary
Switch1(config)# erps 1 ring 1 mode transit
Switch1(config)# erps 1 ring 1 primary interface eth-0-1
Switch1(config)# erps 1 ring 1 secondary interface eth-0-2
Switch1(config)# erps 1 mstp instance 0
Switch1(config)# erps 1 ring 1 enable
```

Шаг 8. Настройка транзитного узла Switch3 в домене Domain1.

```
Switch3(config)# erps 1
Switch3(config)# erps 1 primary control vlan 10
Switch3(config)# erps 1 ring 1 level primary
Switch3(config)# erps 1 ring 1 mode transit
Switch3(config)# erps 1 ring 1 primary interface eth-0-1
Switch3(config)# erps 1 ring 1 secondary interface eth-0-2
Switch3(config)# erps 1 mstp instance 0
Switch3(config)# erps 1 ring 1 enable
```

Шаг 9. Настройка Master узел Switch6 в Domain2.

```
Switch6(config)# erps 2
Switch6(config)# erps 2 primary control vlan 20
Switch6(config)# erps 2 ring 2 level primary
Switch6(config)# erps 2 ring 2 mode master
Switch6(config)# erps 2 ring 2 primary interface eth-0-3
Switch6(config)# erps 2 ring 2 secondary interface eth-0-4
Switch6(config)# erps 2 mstp instance 0
Switch6(config)# erps 2 ring 2 enable
```

Шаг 10. Настройка транзитного узла Switch5 в Domain2.

```
Switch5(config)# erps 2
Switch5(config)# erps 2 primary control vlan 10
Switch5(config)# erps 2 ring 1 level primary
Switch5(config)# erps 2 ring 1 mode transit
Switch5(config)# erps 2 ring 1 primary interface eth-0-1
Switch5(config)# erps 2 ring 1 secondary interface eth-0-2
Switch5(config)# erps 2 mstp instance 0
Switch5(config)# erps 2 ring 1 enable
```

Шаг 11. Настройка атрибутов Ring1.

```
Switch4(config)# erps 1
Switch4(config)# erps 1 primary control vlan 10
Switch4(config)# erps 1 ring 1 level primary
Switch4(config)# erps 1 ring 1 mode transit
Switch4(config)# erps 1 ring 1 primary interface eth-0-1
Switch4(config)# erps 1 ring 1 secondary interface eth-0-2
Switch4(config)# erps 1 mstp instance 0
Switch4(config)# erps 1 ring 1 enable
```

Шаг 12. Настройка атрибутов Ring2.

```
Switch4(config)# erps 2
Switch4(config)# erps 2 primary control vlan 20
Switch4(config)# erps 2 ring 2 level primary
Switch4(config)# erps 2 ring 2 mode transit
Switch4(config)# erps 2 ring 2 primary interface eth-0-3
Switch4(config)# erps 2 ring 2 secondary interface eth-0-4
Switch4(config)# erps 2 mstp instance 0
Switch4(config)# erps 2 ring 2 enable
```

Шаг 13. Выход из режима настройки.

```
SwitchX(config)# end
```

11.4.2.5 Настройка ERPS с несколькими под-кольцами

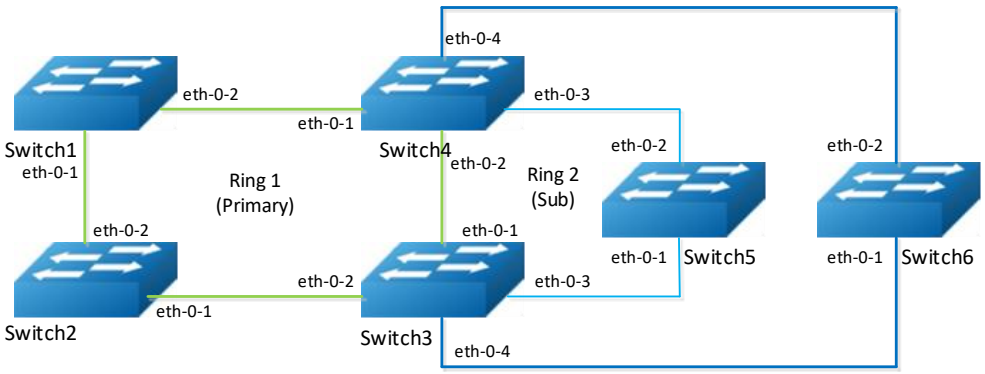


Рисунок 60 – Топология схемы сети с несколькими sub-кольцами

Коммутаторы 1-6 образуют кольцевую сеть, работающую по протоколу ERPS и обеспечивая защиту резервированием на уровне 2.

- существуют три пересекающихся кольца; следовательно, рассматривается вариант конфигурации с одним основным кольцом и двумя sub-кольцами.

- существует несколько sub-колец с граничными и вспомогательными узлами, поэтому STP следует включить на одном sub-кольце и отключить на другом, чтобы предотвратить изоляцию sub-кольца при блокировке всех вспомогательных узлов.

11.4.2.6 Этапы настройки

NOTE «SwitchX» указывает, что конфигурация одинакова для всех коммутаторов (Switch 1-6).

Шаг 1. Войдите в режим настройки.

```
SwitchX# configure terminal
```

Шаг 2. Настройка VLAN 10 для устройств основного кольца (коммутаторы 1-4).

```
SwitchX(config)# vlan database
SwitchX(config-vlan)# vlan 10,20
SwitchX(config-vlan)# exit
SwitchX(config)# no ip igmp snooping vlan 10
SwitchX(config)# no ip igmp snooping vlan 20
```

Шаг 3. Настройка VLAN 20 для устройств кольца 2 (коммутатор 5, 6).

```
SwitchX(config)# vlan database
SwitchX(config-vlan)# vlan 20
SwitchX(config-vlan)# exit
SwitchX(config)# no ip igmp snooping vlan 20
```

Шаг 4. Настройка атрибутов интерфейса.

```
SwitchX(config)# interface eth-0-X
SwitchX(config-if)# switchport
SwitchX(config-if)# no shutdown
SwitchX(config-if)# switchport mode trunk
SwitchX(config-if)# switchport trunk allowed vlan all
SwitchX(config-if)# spanning-tree port disable
SwitchX(config-if)# exit
```

NOTE eth-0-X обозначает, что для eth-0-1/eth-0-2/eth-0-3/eth-0-4 конфигурация одинакова.

Шаг 5. Настройка атрибутов интерфейса для assistant-edge (коммутаторы 3, 4).

```
SwitchX(config)# interface eth-0-3
SwitchX(config-if)# switchport trunk allowed vlan remove 10
SwitchX(config)# interface eth-0-4
SwitchX(config-if)# switchport trunk allowed vlan remove 10
```

NOTE Удалите VLAN 10 на интерфейсе eth-0-3/eth-0-4 на устройстве assistant-edge.

Шаг 6. Настройка главного узла коммутатора 2 в основном кольце.

```
Switch2(config)# erps 1
Switch2(config)# erps 1 primary control vlan 10
Switch2(config)# erps 1 ring 1 level primary
Switch2(config)# erps 1 ring 1 mode master
Switch2(config)# erps 1 ring 1 primary interface eth-0-1
Switch2(config)# erps 1 ring 1 secondary interface eth-0-2
Switch2(config)# erps 1 sub control vlan 20
Switch2(config)# erps 1 mstp instance 0
Switch2(config)# erps 1 ring 1 enable
```

Шаг 7. Настройка коммутатора 1 как транзитного узла.

```
Switch1(config)# erps 1
Switch1(config)# erps 1 primary control vlan 10
Switch1(config)# erps 1 ring 1 level primary
Switch1(config)# erps 1 ring 1 mode transit
Switch1(config)# erps 1 ring 1 primary interface eth-0-1
Switch1(config)# erps 1 ring 1 secondary interface eth-0-2
Switch1(config)# erps 1 sub control vlan 20
Switch1(config)# erps 1 mstp instance 0
Switch1(config)# erps 1 ring 1 enable
```

Шаг 8. Настройка атрибутов основного кольца Ring1. Assistant-edge switch4.

```
Switch4(config)# erps 1
Switch4(config)# erps 1 primary control vlan 10
Switch4(config)# erps 1 sub control vlan 20
Switch4(config)# erps 1 ring 1 level primary
Switch4(config)# erps 1 ring 1 mode master
Switch4(config)# erps 1 ring 1 primary interface eth-0-1
Switch4(config)# erps 1 ring 1 secondary interface eth-0-2
Switch4(config)# erps 1 mstp instance 0
Switch4(config)# erps 1 ring 1 enable
```

Шаг 9. Настройка атрибутов sub-кольца 2: assistant-edge switch4.

```
Switch4(config)# erps 1 ring 2 level sub
Switch4(config)# erps 1 ring 2 edge-mode edge
Switch4(config)# erps 1 ring 2 edge interface eth-0-3
Switch4(config)# erps 1 ring 2 common interface eth-0-2
Switch4(config)# erps 1 ring 2 srpt disable
Switch4(config)# erps 1 ring 2 enable
```

Шаг 10. Настройка атрибутов sub-кольца 3: assistant-edge switch4.

```
Switch4(config)# erps 1 ring 3 level sub
Switch4(config)# erps 1 ring 3 edge-mode assistant-edge
Switch4(config)# erps 1 ring 3 edge interface eth-0-4
Switch4(config)# erps 1 ring 3 common interface eth-0-2
Switch4(config)# erps 1 ring 3 enable
```

Шаг 11. Настройка атрибутов основного кольца ring1 (Коммутатор 3).

```
Switch3(config)# erps 1
Switch3(config)# erps 1 primary control vlan 10
Switch3(config)# erps 1 sub control vlan 20
Switch3(config)# erps 1 ring 1 level primary
Switch3(config)# erps 1 ring 1 mode master
Switch3(config)# erps 1 ring 1 primary interface eth-0-1
Switch3(config)# erps 1 ring 1 secondary interface eth-0-2
Switch3(config)# erps 1 mstp instance 0
Switch3(config)# erps 1 ring 1 enable
```

Шаг 12. Настройка атрибутов sub-кольца 2 (assistant-edge switch3).

```
Switch3(config)# erps 1 ring 2 level sub
Switch3(config)# erps 1 ring 2 edge-mode assistant-edge
Switch3(config)# erps 1 ring 2 edge interface eth-0-3
Switch3(config)# erps 1 ring 2 common interface eth-0-1
```

```
Switch3(config)# erps 1 ring 2 srpt disable
Switch3(config)# erps 1 ring 2 enable
```

Шаг 13. Настройка атрибутов sub-кольца 3 (assistant-edge switch3).

```
Switch3(config)# erps 1 ring 3 level sub
Switch3(config)# erps 1 ring 3 edge-mode edge
Switch3(config)# erps 1 ring 3 edge interface eth-0-4
Switch3(config)# erps 1 ring 3 common interface eth-0-1
Switch3(config)# erps 1 ring 3 enable
```

Шаг 14. Настройка коммутатора 5 как главного узла в sub-кольце.

```
Switch5(config)# erps 1
Switch5(config)# erps 1 sub control vlan 20
Switch5(config)# erps 1 ring 2 level sub
Switch5(config)# erps 1 ring 2 mode master
Switch5(config)# erps 1 ring 2 primary interface eth-0-1
Switch5(config)# erps 1 ring 2 secondary interface eth-0-2
Switch5(config)# erps 1 mstp instance 0
Switch5(config)# erps 1 ring 2 enable
```

Шаг 15. Настройка главного узла коммутатора 6 в sub-кольце.

```
Switch6(config)# erps 1
Switch6(config)# erps 1 sub control vlan 20
Switch6(config)# erps 1 ring 3 level sub
Switch6(config)# erps 1 ring 3 mode master
Switch6(config)# erps 1 ring 3 primary interface eth-0-2
Switch6(config)# erps 1 ring 3 secondary interface eth-0-1
Switch6(config)# erps 1 mstp instance 0
Switch6(config)# erps 1 ring 3 enable
```

Шаг 16. Выход из режима настройки.

```
SwitchX(config)# end
```

11.4.2.7 Настройка ERPS в режиме Multi-instance

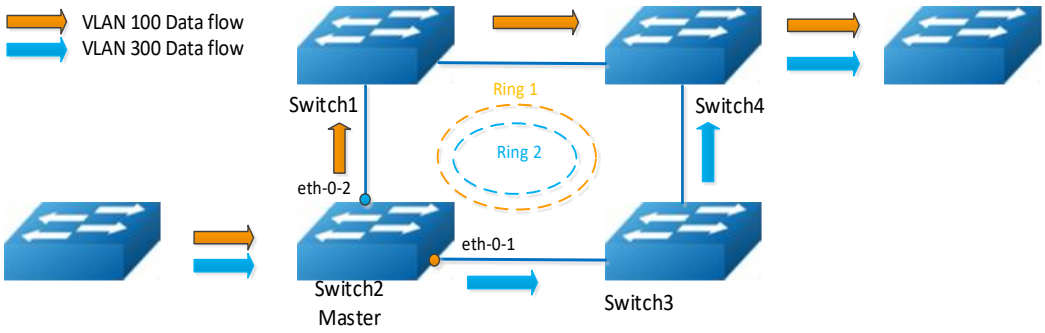


Рисунок 61 – Multiple-instances сетевая топология

Коммутаторы 1-4 образуют кольцевую сеть и используют протокол ERPS, обеспечивая резервирование и защиту от петель на уровне 2. При настройке нескольких виртуальных контуров, трафик с коммутатора 2 перенаправляется на коммутатор 4, поток данных VLAN 100-200 следует по маршруту пересылки коммутаторов 2-1-4, а поток данных VLAN 300-400 — по маршруту пересылки коммутаторов 2-3-4. Это позволяет реализовать распределение нагрузки и повысить эффективность использования каналов связи.

- Настройте главный узел для кольца 1 домена 1 и кольца 2 домена 2, вторичный порт кольца 1 - eth-0-1, а вторичный порт кольца 2 - eth-0-2;
- Настройка instance: instance 1 подключается к VLAN 100-200, instance 2 — к VLAN 300-400;
- Присвоить домену domain1 значение instance1, домену domain2 значение instance2.

11.4.2.8 Этапы настройки

NOTE «SwitchX» указывает, что конфигурация одинакова для всех коммутаторов (Switch 1-4).

Шаг 1. Войдите в режим настройки.

```
SwitchX# configure terminal
```

Шаг 2. Настройка VLAN 10/20 для управляющего VLAN.

```
SwitchX(config)# vlan database
SwitchX(config-vlan)# vlan 10,20,100-200,300-400
SwitchX(config-vlan)# exit
SwitchX(config)# no ip igmp snooping vlan 10
SwitchX(config)# no ip igmp snooping vlan 20
```

Шаг 3. Настройка VLAN 100-200/300-400 для передачи данных.

```
SwitchX(config)# vlan database
SwitchX(config-vlan)# vlan 100-200,300-400
SwitchX(config-vlan)# exit
```

Шаг 4. Настройка атрибутов интерфейса.

```
SwitchX(config)# interface eth-0-1
SwitchX(config-if)# switchport
SwitchX(config-if)# no shutdown
SwitchX(config-if)# switchport mode trunk
SwitchX(config-if)# switchport trunk allowed vlan all
SwitchX(config-if)# spanning-tree port disable
SwitchX(config-if)# exit
SwitchX(config)# interface eth-0-2
SwitchX(config-if)# switchport
SwitchX(config-if)# no shutdown
SwitchX(config-if)# switchport mode trunk
SwitchX(config-if)# switchport trunk allowed vlan all
SwitchX(config-if)# spanning-tree port disable
SwitchX(config-if)# exit
```

Шаг 5. Настройка MSTP.

```
SwitchX(config)# spanning-tree mode mstp
SwitchX(config)# spanning-tree mst configuration
SwitchX(config-mst)# instance 1 vlan 10,100-200
SwitchX(config-mst)# instance 2 vlan 20,300-400
```

NOTE Предлагается добавить управляющую VLAN кольцевой сети ERPS в инстанции защиты кольцевой сети по MSTP.

Шаг 6. Настройка кольца 1 на главном узле - коммутатор 2.

```
Switch2(config)# erps 1
Switch2(config)# erps 1 primary control vlan 10
Switch2(config)# erps 1 ring 1 level primary
Switch2(config)# erps 1 ring 1 mode master
Switch2(config)# erps 1 ring 1 primary interface eth-0-2
Switch2(config)# erps 1 ring 1 secondary interface eth-0-1
Switch2(config)# erps 1 mstp instance 1
Switch2(config)# erps 1 ring 1 enable
```

Шаг 7. Настройка кольца 2 на главном узле – коммутатор 2.

```
Switch2(config)# erps 2
Switch2(config)# erps 2 primary control vlan 20
Switch2(config)# erps 2 ring 2 level primary
Switch2(config)# erps 2 ring 2 mode master
Switch2(config)# erps 2 ring 2 primary interface eth-0-1
Switch2(config)# erps 2 ring 2 secondary interface eth-0-2
Switch2(config)# erps 2 mstp instance 2
Switch2(config)# erps 2 ring 2 enable
```

Шаг 8. Настройка кольца 1 на транзитном узле - коммутатор 1.

```
Switch1(config)# erps 1
Switch1(config)# erps 1 primary control vlan 10
Switch1(config)# erps 1 ring 1 level primary
Switch1(config)# erps 1 ring 1 mode transit
Switch1(config)# erps 1 ring 1 primary interface eth-0-1
Switch1(config)# erps 1 ring 1 secondary interface eth-0-2
Switch1(config)# erps 1 mstp instance 1
Switch1(config)# erps 1 ring 1 enable
```

Шаг 9. Настройка кольца 2 на транзитном узле - коммутатор 1.

```
Switch1(config)# erps 2
Switch1(config)# erps 2 primary control vlan 20
Switch1(config)# erps 2 ring 2 level primary
Switch1(config)# erps 2 ring 2 mode transit
Switch1(config)# erps 2 ring 2 primary interface eth-0-1
Switch1(config)# erps 2 ring 2 secondary interface eth-0-2
Switch1(config)# erps 2 mstp instance 2
Switch1(config)# erps 2 ring 2 enable
```

Шаг 10. Настройка кольца 1 на транзитном узле - коммутатор 3.

```
Switch3(config)# erps 1
Switch3(config)# erps 1 primary control vlan 10
Switch3(config)# erps 1 ring 1 level primary
Switch3(config)# erps 1 ring 1 mode transit
Switch3(config)# erps 1 ring 1 primary interface eth-0-1
Switch3(config)# erps 1 ring 1 secondary interface eth-0-2
Switch3(config)# erps 1 mstp instance 1
Switch3(config)# erps 1 ring 1 enable
```

Шаг 11. Настройка кольца 2 на транзитном узле - коммутатор 3.

```
Switch3(config)# erps 2
Switch3(config)# erps 2 primary control vlan 20
Switch3(config)# erps 2 ring 2 level primary
Switch3(config)# erps 2 ring 2 mode transit
Switch3(config)# erps 2 ring 2 primary interface eth-0-1
Switch3(config)# erps 2 ring 2 secondary interface eth-0-2
Switch3(config)# erps 2 mstp instance 2
Switch3(config)# erps 2 ring 2 enable
```

Шаг 12. Настройка кольца 1 на транзитном узле - коммутатор 4.

```
Switch4(config)# erps 1
Switch4(config)# erps 1 primary control vlan 10
Switch4(config)# erps 1 ring 1 level primary
Switch4(config)# erps 1 ring 1 mode transit
Switch4(config)# erps 1 ring 1 primary interface eth-0-1
Switch4(config)# erps 1 ring 1 secondary interface eth-0-2
Switch4(config)# erps 1 mstp instance 1
Switch4(config)# erps 1 ring 1 enable
```

Шаг 13. Настройка кольца 2 на транзитном узле - коммутатор 4.

```
Switch4(config)# erps 2
Switch4(config)# erps 2 primary control vlan 20
Switch4(config)# erps 2 ring 2 level primary
Switch4(config)# erps 2 ring 2 mode transit
Switch4(config)# erps 2 ring 2 primary interface eth-0-1
Switch4(config)# erps 2 ring 2 secondary interface eth-0-2
Switch4(config)# erps 2 mstp instance 2
Switch4(config)# erps 2 ring 2 enable
```

Шаг 14. Выход из режима настройки.

```
SwitchX(config)# end
```

11.5 Настройка Smart Link

11.5.1 Общие положения

11.5.1.1 Описание функции

Smart Link – это простая, но практичная технология быстрой защиты каналов связи. Это решение специально разработано для сетей с двумя восходящими каналами, обеспечивает резервирование и быстрое переключение активных и резервных каналов.

Каждая группа smart-link каналов связи включает пару интерфейсов уровня 2, где один интерфейс настроен на резервирование другого. Эта функция предоставляет альтернативное решение протоколу STP. Пользователи могут отключить STP и при этом сохранить избыточность каналов связи. Также поддерживается балансировка нагрузки, благодаря чему оба интерфейса одновременно пересылают трафик.

11.5.2 Настройка

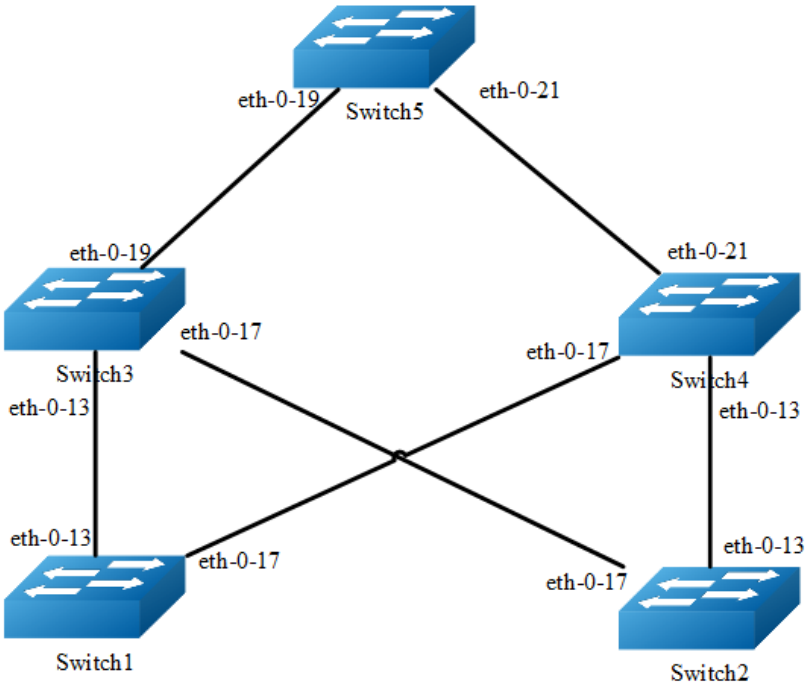


Рисунок 62 – Smart-Link типовая топология

На рисунке выше показано типовое применение технологии SmartLink. Коммутаторы Switch1 и Switch2 настроены как группа SmartLink. Коммутаторы Switch3, Switch4 и Switch5 настроены как smart-link flush receiver.

Для настройки smart-link группы необходимо предварительно выполнить некоторые действия:

- Необходимо настроить VLAN.
- Необходимо настроить экземпляр MSTP.
- Протокол Spanning-tree следует отключить на интерфейсе.

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 2-20
Switch(config-vlan)# exit
```

Шаг 3. Установите режим STP (Spanning Tree Protocol) и создайте экземпляр MSTP.

Создайте экземпляр MSTP на коммутаторах Switch1 и Switch2:

```
Switch(config)# spanning-tree mode mstp
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 1
Switch(config-mst)# instance 2 vlan 2
Switch(config-mst)# instance 3 vlan 3
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# exit
```

Шаг 4. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1 и Switch2:

```
Switch(config)# interface eth-0-13
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# spanning-tree port disable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-17
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# spanning-tree port disable
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Switch3 и Switch4:

```
Switch(config)# interface eth-0-13
Switch(config-if)# switchport mode trunk
Switch(config-if)# no shutdown
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# smart-link flush receive control-vlan 10 password simple
test
Switch(config-if)# exit

Switch(config)# interface eth-0-17
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
```

```
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# smart-link flush receive control-vlan 10 password simple
test
Switch (config-if)# exit
```

Interface eth-0-19 на Switch3:

```
Switch(config)# interface eth-0-19
Switch(config-if)# switchport mode trunk
Switch(config-if)# no shutdown
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# exit
```

Interface eth-0-21 на Switch4:

```
Switch(config)# interface eth-0-21
Switch(config-if)# switchport mode trunk
Switch(config-if)# no shutdown
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# exit
```

Switch5:

```
Switch(config)# interface eth-0-19
Switch(config-if)# switchport mode trunk
Switch(config-if)# no shutdown
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# smart-link flush receive control-vlan 10 password simple
test
Switch(config-if)# exit

Switch(config)# interface eth-0-21
Switch(config-if)# switchport mode trunk
Switch(config-if)# no shutdown
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# smart-ink flush receive control-vlan 10 password simple
test
Switch(config-if)# exit
```

Шаг 5. Создайте группу smart-link и задайте атрибуты группы.

Switch1 и Switch2:

```
Switch(config)# smart-link group 1
Switch(config-smlk-group)# interface eth-0-13 master
Switch(config-smlk-group)# interface eth-0-17 slave
Switch(config-smlk-group)# protected mstp instance 1
Switch(config-smlk-group)# protected mstp instance 2
Switch(config-smlk-group)# protected mstp instance 3
Switch(config-smlk-group)# protected mstp instance 10
```

```
Switch(config-smlk-group)# load-balance instance 3
Switch(config-smlk-group)# restore time 40
Switch(config-smlk-group)# restore enable
Switch(config-smlk-group)# flush send control-vlan 10 password simple test
Switch(config-smlk-group)# group enable
Switch(config-smlk-group)# exit
```

Шаг 6 Отключите функцию smart link relay.

Switch5:

```
Switch(config)# no smart-link relay enable
```

Шаг 7. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 8. Проверка.

Switch1.

```
Switch1# show smart-link group 1
Smart-link group 1 information:
 The smart-link group was enabled.
 ============================================================
 Auto-restore:
   state        time             count     Last-time
   enabled       40                0       N/A
 ============================================================
 Protected instance: 1  2  3
 Load balance instance: 3
 Flush sender , Control-vlan ID: 10    Password:test
 ============================================================
 INTERFACE:
 Role    Member     DownCount Last-Down-Time  FlushCount Last-Flush-Time
 MASTER eth-0-13     0        N/A                    0     N/A
 SLAVE  eth-0-17     0        N/A                    0     N/A
 ============================================================
 Instance states in the member interfaces:
   A - ACTIVE ,   B -BLOCK  , D-The interface is link-down
 Map-instance-ID   MASTER(eth-0-13)     SLAVE(eth-0-17)
       1               A                   B
       2               A                   B
       3               B                   A
```

Switch2.

```
Switch# show smart-link group 1
Smart-link group 1 information:
```

```
The smart-link group was enabled.
============================================================
Auto-restore:
  state        time             count     Last-time
  enabled       40                0       N/A
============================================================
Protected instance: 1  2  3
Load balance instance: 3
Flush sender , Control-vlan ID: 10    Password:test
============================================================
INTERFACE:
Role    Member     DownCount Last-Down-Time   FlushCount Last-Flush-Time
MASTER eth-0-13     0        N/A                    0      N/A
SLAVE  eth-0-17     0        N/A                    0      N/A
============================================================
Instance states in the member interfaces:
  A - ACTIVE ,   B -BLOCK  , D-The interface is link-down
Map-instance-ID   MASTER(eth-0-13)     SLAVE(eth-0-17)
      1              A                    B
      2              A                    B
      3              B                    A
```

Switch3.

```
Switch# show smart-link
 Relay smart-link flush packet is enabled
 Smart-link flush receiver interface:
    eth-0-13   control-vlan:10   password:test
    eth-0-17   control-vlan:10   password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 0.
```

Switch4.

```
Switch# show smart-link
 Relay smart-link flush packet is enabled
 Smart-link flush receiver interface:
    eth-0-13   control-vlan:10   password:test
    eth-0-17   control-vlan:10   password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 0.
```

Switch5.

```
Switch# show smart-link
 Relay smart-link flush packet is disabled
 Smart-link flush receiver interface:
    eth-0-21   control-vlan:10   password: test
    eth-0-19   control-vlan:10   password:test
```

```
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
 Smart link Group Number is 0.
```

11.6 Настройка Multi-Link

11.6.1 Общие положения

11.6.1.1 Описание функции

Технология Multi-Link — это простая, но практичная технология быстрой защиты каналов связи. Это решение, специально разработанное для многоканальных сетей, обеспечивающее резервирование и быстрое переключение между каналами.

Эта функция похожа на «smart link», но количество линков увеличено с 2 до 4.

11.6.2 Настройка

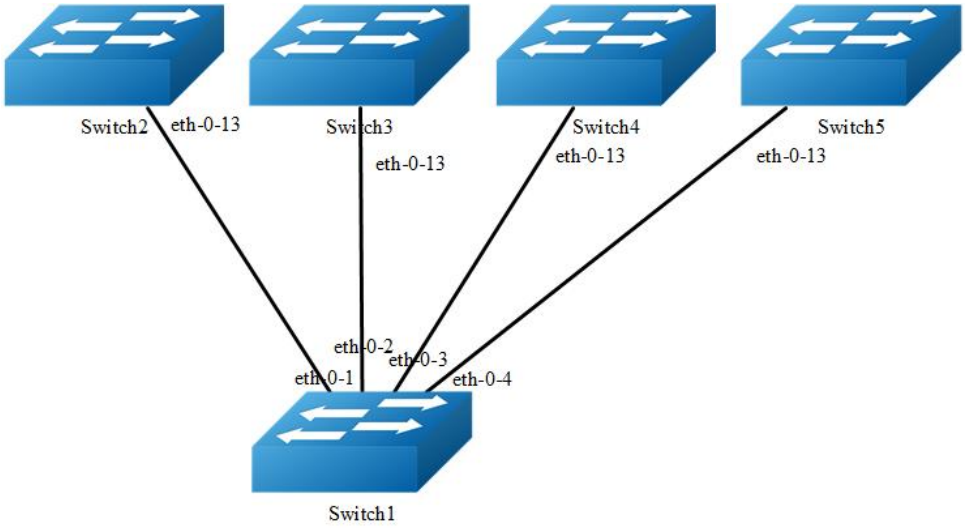


Рисунок 1-8 Multi-Link типовая топология

На рисунке выше показано типовое применение Multi-link. Коммутатор Switch1 настроен как Multi-link группа. Коммутаторы Switch2, Switch3, Switch4 и Switch5 настроены как multi-link flush receiver.

Для настройки Multi-link группы необходимо предварительно выполнить некоторые действия.

- Необходимо настроить VLAN;
- Необходимо настроить экземпляр MSTP;
- Протокол Spanning-tree следует отключить на интерфейсе.

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config- vlan)# vlan 2-10
Switch(config- vlan)# exit
```

Шаг 3. Установите режим STP (Spanning Tree Protocol) и создайте экземпляр MSTP.

```
Switch(config)# spanning-tree mode mstp
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 1
Switch(config-mst)# instance 2 vlan 2
Switch(config-mst)# instance 3 vlan 3
Switch(config-mst)# instance 4 vlan 4-10
Switch(config-mst)# exit
```

Шаг 4. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface range eth-0-1 - 4
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# spanning-tree port disable
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Switch2 ~ 5:

```
Switch(config)# interface eth-0-13
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# multi-link flush receive control-vlan 10 password simple
test
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 5. Создайте multi-link группу и задайте атрибуты группы.

Switch1:

```
Switch(config)# multi-link group 1
Switch(config-multilk-group)# interface eth-0-1 priority 1
Switch(config-multilk-group)# interface eth-0-2 priority 2
Switch(config-multilk-group)# interface eth-0-3 priority 3
```

```
Switch(config-multilk-group)# interface eth-0-4 priority 4
Switch(config-multilk-group)# protected mstp instance 1
Switch(config-multilk-group)# protected mstp instance 2
Switch(config-multilk-group)# protected mstp instance 3
Switch(config-multilk-group)# protected mstp instance 4
Switch(config-multilk-group)# load-balance instance 2 priority 2
Switch(config-multilk-group)# load-balance instance 3 priority 3
Switch(config-multilk-group)# load-balance instance 4 priority 4
Switch(config-multilk-group)# restore time 40
Switch(config-multilk-group)# restore enable
Switch(config-multilk-group)# flush send control-vlan 10 password simple test
Switch(config-multilk-group)# group enable
Switch(config-multilk-group)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Switch1.

```
Switch# show multi-link group 1
Multi-link group 1 information:
 The multi-link group was enabled.
 ============================================================
 Auto-restore:
   state        time             count     Last-time
   enabled       40                0       N/A
 ============================================================
 Protected instance: 1  2  3  4
 Load balance instance: 2(to P2)  3(to P3)  4(to P4)
 Flush sender , Control-vlan ID: 10    Password:test
 ============================================================
 INTERFACE:
 Role    Member     DownCount Last-Down-Time       FlushCount Last-Flush-Time
 PRI1    eth-0-1    0         N/A                  1
2016/09/05,07:13:24
 PRI2    eth-0-2    0         N/A                  1
2016/09/05,07:13:24
 PRI3    eth-0-3    0         N/A                  1
2016/09/05,07:13:24
 PRI4    eth-0-4    0         N/A                  1
2016/09/05,07:13:24
 ============================================================
 Instance states in the member interfaces:
   A - ACTIVE ,   B -BLOCK  , D-The interface is link-down
 Map-instance-ID  P1(eth-0-1 )  P2(eth-0-2 )  P3(eth-0-3 )  P4(eth-0-4 )
```

```
 1                A              B              B              B
 2                B              A              B              B
 3                B              B              A              B
 4                B              B              B              A
```

Switch2~5.

```
Switch# show multi-link
Relay multi-link flush packet is enabled
 Multi-link flush receiver interface:
    eth-0-13   control-vlan:10   password:test
 Multi-link received flush packet number:0
 Multi-link processed flush packet number:0
 Multi-link tcn is disabled
 Multi-link tcn query count    :2
 Multi-link tcn query interval :10
 Multi-link Group Number is 0.
```

11.7 Настройка Monitor Link

11.7.1 Общие положения

11.7.1.1 Описание функции

Функция Monitor Link — это отслеживание состояния каналов. Monitor Link работает совместно с протоколами уровня 2. Идея заключается в отслеживании состояний восходящих uplink-портов и переключении состояния (включено/выключено) нисходящих downlink-портов, обеспечивая перенаправление трафика на другой коммутатор.

11.7.2 Настройка

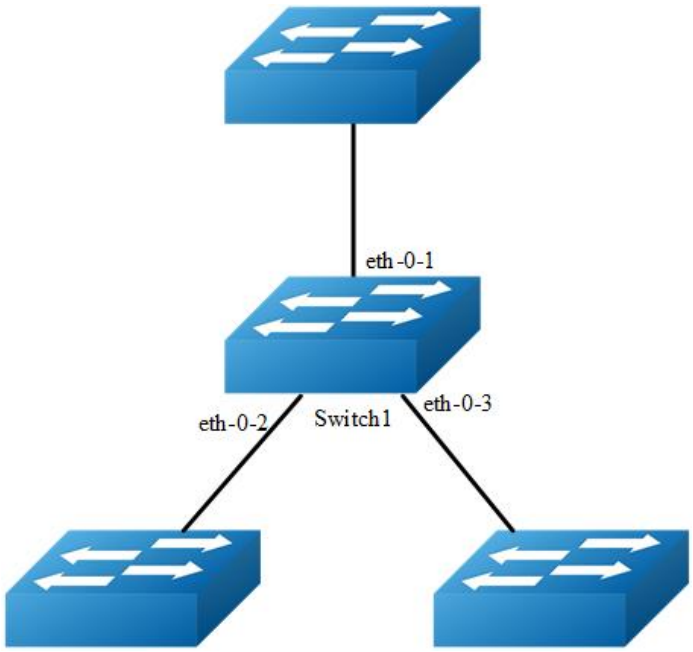


Рисунок 63 – Топология Monitor link

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и включите интерфейс.

```
Switch(config)# interface range eth-0-1 - 3
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

Шаг 3. Создайте multi-link группу и задайте атрибуты группы.

```
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link uplink interface eth-0-1
Switch(config-mtlk-group)# monitor-link downlink interface eth-0-2
Switch(config-mtlk-group)# monitor-link downlink interface eth-0-3
Switch(config-mtlk-group)# exit
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

```
Switch# show monitor-link group
Group Id: 1
Monitor link status: UP
Role     Member    Last-up-time      Last-down-time          upcount
downcount
UpLk 1   eth-0-1   2011/07/15,02:07:31   2011/07/15,02:07:31     2          1
DwLk 1   eth-0-2   2011/07/15,02:07:34   2011/07/15,02:07:31     1          1
DwLk 2   eth-0-3   N/A                       N/A                          0
0
```

11.8 Настройка VRRP

11.8.1 Общие положения

11.8.1.1 Описание функции

В этой главе представлен обзор протокола VRRP (Virtual Router Redundancy Protocol) и его реализация. VRRP устраняет риск возникновения единой точки отказа, присущей статической среде маршрутизации. VRRP динамически назначает ответственность за маршрутизацию одному из VRRP-маршрутизаторов в локальной сети. Одним из главных преимуществ VRRP является то, что он делает доступным основной шлюз по умолчанию без необходимости настройки динамической маршрутизации на каждом конечном устройстве.

NOTE Аутентификация MD5 не поддерживается для VRRP.

11.8.1.2 Основные термины и описание

Протокол VRRP описан стандартом RFC 3768 (VRRP): Knight, S., “Virtual Router Redundancy Protocol (VRRP)”.

Терминология:

- Backup Router: VRRP-маршрутизатор, который выполняет резервирование основного. Он берет на себя ответственность за пересылку трафика в случае отказа основного маршрутизатора;
- Critical IP: IP-адрес, по которому маршрутизатор VRRP отправляет/получает пакеты в течение конкретной сессии;
- IP Address Owner: VRRP-маршрутизатор, который использует IP-адрес виртуального маршрутизатора в качестве реального адреса интерфейса. Это маршрутизатор, который в активном состоянии будет отвечать на пакеты, адресованные этому IP-адресу (ICMP-пинги, TCP-соединения и т. д.);
- Master Router: VRRP-маршрутизатор, которому принадлежит IP-адрес (т.е. который резервируется) и который является маршрутизатором по умолчанию;

- Virtual IP: резервный IP-адрес сессии VRRP;
- Virtual Router: маршрутизатор, управляемый протоколом VRRP, который выступает в качестве маршрутизатора по умолчанию для хостов в общей локальной сети. Он состоит из идентификатора виртуального маршрутизатора и набора связанных с ним IP-адресов в общей локальной сети. Маршрутизатор VRRP может быть резервным для одного или нескольких виртуальных маршрутизаторов;
- VRRP Router: маршрутизатор с включенным VRRP. Может выполнять роль одного или нескольких виртуальных маршрутизаторов routers.

Как правило, конечные устройства подключаются к корпоративной сети через один маршрутизатор (маршрутизатор первого перехода), находящийся в том же сегменте локальной сети (LAN). Наиболее распространенный метод настройки конечных устройств — статическая настройка адреса этого маршрутизатора в качестве шлюза по умолчанию. Это минимизирует затраты на настройку и обработку. Главная проблема этого метода настройки заключается в том, что в случае отказа маршрутизатора первого перехода создается единая точка отказа.

Протокол VRRP решает эту проблему, вводя концепцию виртуального маршрутизатора, состоящего из двух или более маршрутизаторов VRRP в одной подсети. Также вводится концепция виртуального IP-адреса, который представляет собой адрес, который конечные хосты настраивают в качестве своего шлюза по умолчанию. Только один маршрутизатор (называемый главным) пересылает пакеты от этого IP-адреса. В случае отказа главного маршрутизатора один из других маршрутизаторов (резервный) берет на себя ответственность за пересылку пакетов.

На первый взгляд, описанная конфигурация может показаться не очень эффективной, поскольку она удваивает стоимость и оставляет один маршрутизатор в режиме ожидания. Этого можно избежать, создав два виртуальных маршрутизатора и разделив трафик между ними.

11.8.2 Настройка

11.8.2.1 Настройка VRRP (один роутер Virtual-Router)

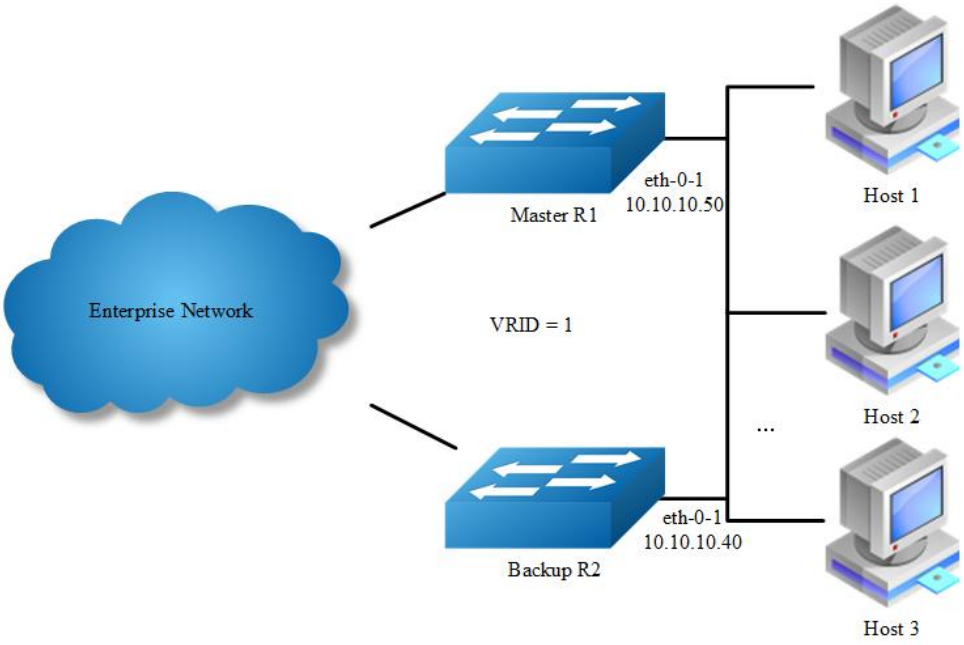


Рисунок 64 – Топология VRRP с одним виртуальным роутерером (virtual-router)

В этой конфигурации конечные хосты устанавливают маршрут по умолчанию к IP-адресу виртуального маршрутизатора 1 (VRID = 1), оба маршрутизатора R1 и R2 работают по протоколу VRRP. R1 настроен как главный маршрутизатор для виртуального маршрутизатора 1 (VRID = 1), а R2 — как резервный. В случае отказа R1, R2 возьмет на себя управление виртуальным маршрутизатором 1 и его IP-адресами, обеспечивая бесперебойное обслуживание хостов. Настройка только одного виртуального маршрутизатора удваивает стоимость и оставляет R2 постоянно в режиме ожидания.

Если точный идентификатор устройства не указан, следующие настройки следует выполнить на всех устройствах топологии.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

R1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.50/24
```

```
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

R2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.40/24
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 3. Создайте экземпляр VRRP.

```
Switch(config)# router vrrp 1
Switch(config-router)# virtual-ip 10.10.10.60
Switch(config-router)# interface eth-0-1
Switch(config-router)# preempt-mode true
Switch(config-router)# advertisement-interval 5
```

Шаг 4. Установите приоритет (необязательно).

Установите приоритет на R1. Если приоритет не задан, R1 будет использовать значение по умолчанию.

```
Switch(config-router)# priority 200
```

Шаг 5. Включите VRRP и выйдите из режима настройки VRRP.

```
Switch(config-router)# enable
Switch(config-router)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

R1.

```
Switch# show vrrp
vrrp session count: 1
vrrp version      : 2
VRID <1>
 State               : Master
 Virtual IP          : 10.10.10.60(Not IP owner)
 Interface           : eth-0-1
 VMAC                : 0000.5e00.0101
 VRF                 : Default
```

```
 Uniform-mac          : -
 Advt timer           : 5 second(s)
 Preempt mode         : TRUE
 Conf pri             : 200             Run pri    : 200
 Master router ip     : 10.10.10.50
 Master priority      : 200
 Master advt timer    : 5 second(s)
 Master down timer    : 15 second(s)
 Preempt delay        : 0 second(s)
 Learn master mode    : FALSE
```

R2.

```
Switch# show vrrp
vrrp session count: 1
vrrp version       : 2
VRID <1>
 State                : Backup
 Virtual IP           : 10.10.10.60(Not IP owner)
 Interface            : eth-0-1
 VMAC                 : 0000.5e00.0101
 VRF                  : Default
 Uniform-mac          : -
 Advt timer           : 5 second(s)
 Preempt mode         : TRUE
 Conf pri             : 100             Run pri    : 100
 Master router ip     : 10.10.10.50
 Master priority      : 200
 Master advt timer    : 5 second(s)
 Master down timer    : 16 second(s)
 Preempt delay        : 0 second(s)
 Learn master mode    : FALSE
```

11.8.2.2 Настройка VRRP (два роутера Virtual-Router)

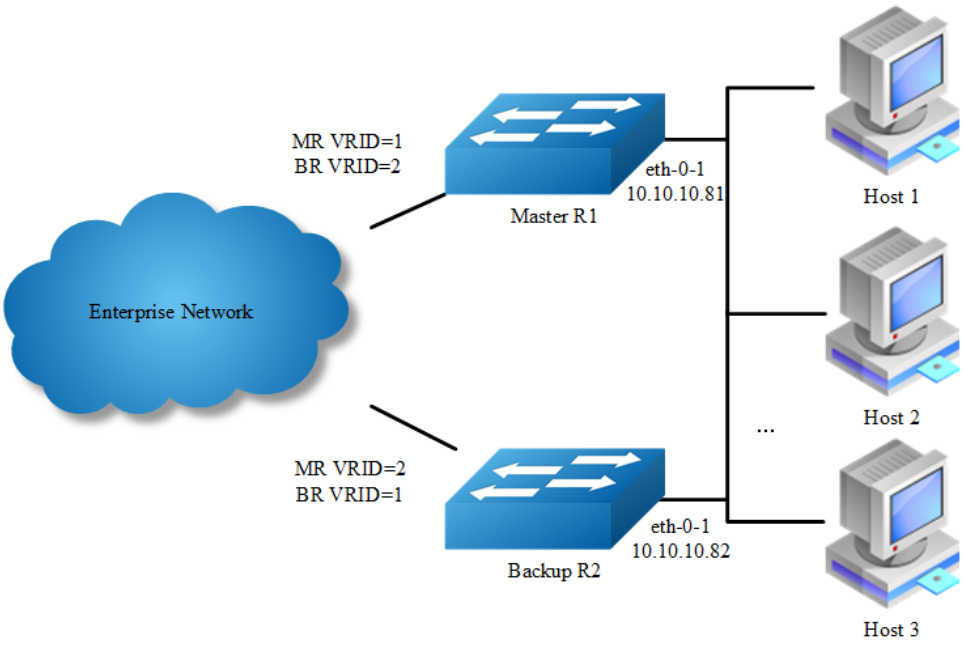


Рисунок 65 – Топология VRRP с двумя виртуальными роутерами (virtual-router)

В приведенном ранее примере с одним виртуальным маршрутизатором маршрутизатор R2 не резервируется маршрутизатором R1. В этом же примере показано, как создать резерв для R2, настроив второй виртуальный маршрутизатор.

В данной конфигурации R1 и R2 представляют собой два виртуальных маршрутизатора, и хосты распределяют свой трафик между ними. R1 и R2 выполняют функцию резервных маршрутизаторов друг для друга.

Если точный идентификатор устройства не указан, следующие настройки следует выполнить на всех устройствах топологии.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

R1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.81/24
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

R2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.82/24
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 3. Создайте экземпляр VRRP.

R1:

```
Switch(config)# router vrrp 1
Switch(config-router)# virtual-ip 10.10.10.81
Switch(config-router)# interface eth-0-1
Switch(config-router)# preempt-mode true
Switch(config-router)# advertisement-interval 5
Switch(config-router)# enable
Switch(config-router)# exit

Switch(config)# router vrrp 2
Switch(config-router)# virtual-ip 10.10.10.82
Switch(config-router)# interface eth-0-1
Switch(config-router)# priority 200
Switch(config-router)# preempt-mode true
Switch(config-router)# advertisement-interval 5
Switch(config-router)# enable
Switch(config-router)# exit
```

R2:

```
Switch(config)# router vrrp 1
Switch(config-router)# virtual-ip 10.10.10.81
Switch(config-router)# interface eth-0-1
Switch(config-router)# priority 200
Switch(config-router)# preempt-mode true
Switch(config-router)# advertisement-interval 5
Switch(config-router)# enable
Switch(config-router)# exit

Switch(config)# router vrrp 2
Switch(config-router)# virtual-ip 10.10.10.82
Switch(config-router)# interface eth-0-1
Switch(config-router)# preempt-mode true
Switch(config-router)# advertisement-interval 5
Switch(config-router)# enable
Switch(config-router)# exit
```

Шаг 4. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 5. Проверка.

R1.

```
Switch# show vrrp
vrrp session count: 2
vrrp version      : 2
VRID <1>
 State               : Master
 Virtual IP          : 10.10.10.81(IP owner)
 Interface           : eth-0-9
 VMAC                : 0000.5e00.0101
 VRF                 : Default
 Uniform-mac         : -
 Advt timer          : 5 second(s)
 Preempt mode        : TRUE
 Conf pri            : 100            Run pri    : 255
 Master router ip    : 10.10.10.81
 Master priority     : 255
 Master advt timer   : 5 second(s)
 Master down timer   : 15 second(s)
 Preempt delay       : 0 second(s)
 Learn master mode   : FALSE
VRID <2>
 State               : Backup
 Virtual IP          : 10.10.10.82(Not IP owner)
 Interface           : eth-0-9
 VMAC                : 0000.5e00.0102
 VRF                 : Default
 Uniform-mac         : -
 Advt timer          : 5 second(s)
 Preempt mode        : TRUE
 Conf pri            : 200            Run pri    : 200
 Master router ip    : 10.10.10.82
 Master priority     : 255
 Master advt timer   : 5 second(s)
 Master down timer   : 15 second(s)
 Preempt delay       : 0 second(s)
 Learn master mode   : FALSE
```

R2.

```
Switch# show vrrp
vrrp session count: 2
vrrp version      : 2
```

```
VRID <1>
 State                : Backup
 Virtual IP           : 10.10.10.81(Not IP owner)
 Interface            : eth-0-9
 VMAC                 : 0000.5e00.0101
 VRF                  : Default
 Uniform-mac          : -
 Advt timer           : 5 second(s)
 Preempt mode         : TRUE
 Conf pri             : 200            Run pri    : 200
 Master router ip     : 10.10.10.81
 Master priority      : 255
 Master advt timer    : 5 second(s)
 Master down timer    : 15 second(s)
 Preempt delay        : 0 second(s)
 Learn master mode    : FALSE
VRID <2>
 State                : Master
 Virtual IP           : 10.10.10.82(IP owner)
 Interface            : eth-0-9
 VMAC                 : 0000.5e00.0102
 VRF                  : Default
 Uniform-mac          : -
 Advt timer           : 5 second(s)
 Preempt mode         : TRUE
 Conf pri             : 100            Run pri    : 255
 Master router ip     : 10.10.10.82
 Master priority      : 255
 Master advt timer    : 5 second(s)
 Master down timer    : 15 second(s)
 Preempt delay        : 0 second(s)
 Learn master mode    : FALSE
```

11.8.2.3 Настройка VRRP Circuit Failover

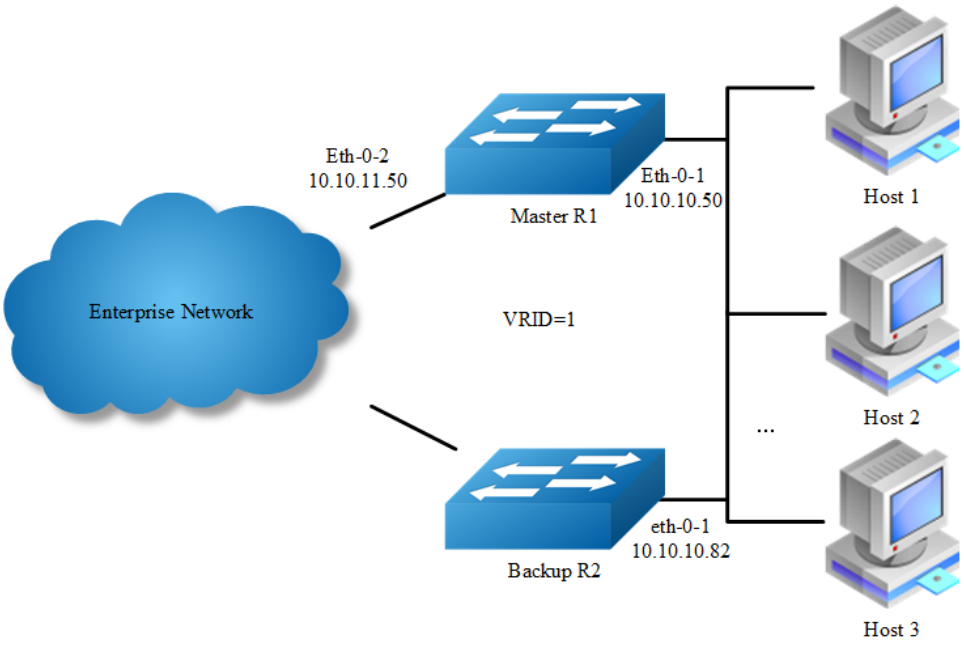


Рисунок 66 – Топология VRRP Circuit Failover

Необходимость в VRRP Circuit Failover возникла из-за того, что VRRPv2 не мог отслеживать состояние интерфейса. Функция VRRP Circuit Failover обеспечивает динамический отказ всего пути в случае выхода из строя одного из участников группы. Вводится понятие пути, в котором участвуют два или более маршрутизатора. В случае сбоя и перехода одного из виртуальных роутеров с ведущего на резервный, другие VR в группе получают уведомление и переходят с ведущего на резервный. Входящие и исходящие пакеты будут проходить через один и тот же роутер-шлюз. Это необходимо в сетях, использующих NAT или межсетевые экраны. Следующий сценарий объясняет работу этой функции.

Повышение отказоустойчивости каналов происходит следующим образом. Для перехода на резервный VR на каждом пути настраивается значение изменения приоритета, которое применяется при сбое. Приоритет каждого маршрутизатора пути уменьшается на значение изменения приоритета, что приводит к переходу резервных VR в состояние главных VR.

В этом примере два маршрутизатора R1 и R2 настроены как резервные маршрутизаторы с разными приоритетами. Приоритет R1 равен 100, а R2 — 90. Разница их приоритетов – 10. Маршрутизатор R1 с более высоким приоритетом является главным виртуальным маршрутизатором (Virtual Router Master). Значение изменения приоритета (decrement) при выходе из строя отслеживаемого канала настроено в 20 - чтобы быть больше разницы приоритетов R1 и R2. При отказе внешнего интерфейса eth1 на маршрутизаторе R1 его приоритет становится равным 80 (100 минус 20). Поскольку приоритет R2 выше (90), чем у R1, R2 становится главным виртуальным маршрутизатором, и маршрутизация пакетов продолжается без пауз.

Когда VR (R1) снова заработает, он восстановит свой первоначальный приоритет (100) и снова станет VR Master.

Если идентификатор устройства не указан, следующие настройки следует выполнить на всех устройствах.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

R1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.50/24
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.11.50/24
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

R2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.40/24
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 3. Создайте track отслеживания для мониторинга состояния канала.

R1:

```
Switch(config)# track 10 interface eth-0-2 linkstate
```

Для получения более подробной информации о системе Track, пожалуйста, обратитесь к главе «Настройка Track».

Шаг 4. Создайте экземпляр VRRP.

R1:

```
Switch(config)# router vrrp 1
Switch(config-router)# virtual-ip 10.10.10.1
Switch(config-router)# interface eth-0-1
Switch(config-router)# preempt-mode true
```

```
Switch(config-router)# advertisement-interval 5
Switch(config-router)# priority 100
Switch(config-router)# track 10 decrement 20
Switch(config-router)# enable
```

R2:

```
Switch(config)# router vrrp 1
Switch(config-router)# virtual-ip 10.10.10.1
Switch(config-router)# interface eth-0-1
Switch(config-router)# preempt-mode true
Switch(config-router)# advertisement-interval 5
Switch(config-router)# priority 90
Switch(config-router)# enable
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

R1.

```
Switch# show vrrp
vrrp session count: 1
vrrp version      : 2
VRID <1>
 State               : Master
 Virtual IP          : 10.10.10.1(Not IP owner)
 Interface           : eth-0-9
 VMAC                : 0000.5e00.0101
 VRF                 : Default
 Uniform-mac         : -
 Advt timer          : 5 second(s)
 Preempt mode        : TRUE
 Conf pri            : 100            Run pri    : 100
 Track Object        : 10             Decre pri  : 20
 Decre pri           : 20
 Master router ip    : 10.10.10.50
 Master priority     : 100
 Master advt timer   : 5 second(s)
 Master down timer   : 16 second(s)
 Preempt delay       : 0 second(s)
 Learn master mode   : FALSE
```

R2.

```
Switch# show vrrp
vrrp session count: 1
vrrp version      : 2
```

```
VRID <1>
 State                : Backup
 Virtual IP           : 10.10.10.1(Not IP owner)
 Interface            : eth-0-9
 VMAC                 : 0000.5e00.0101
 VRF                  : Default
 Uniform-mac          : -
 Advt timer           : 5 second(s)
 Preempt mode         : TRUE
 Conf pri             : 90              Run pri    : 90
 Master router ip     : 10.10.10.50
 Master priority      : 100
 Master advt timer    : 5 second(s)
 Master down timer    : 16 second(s)
 Preempt delay        : 0 second(s)
 Learn master mode    : FALSE
```

11.9 Настройка трэкинга (Track)

11.9.1 Общие положения

11.9.1.1 Описание функции

Track используется для связи функциональных модулей и модулей мониторинга. Track формирует структуру системы с 3 уровнями: «функциональные модули – Track – модули мониторинга».

Track может экранировать различия между модулями мониторинга и предоставлять унифицированный API для функциональных модулей.

Поддерживаются следующие модули мониторинга:

- IP SLA;
- состояния интерфейса;
- состояния bfd.

Поддерживаются следующие функциональные модули:

- Static Route;
- VRRP.

Система Track обеспечивает связь между функциональными модулями и модулями мониторинга. При изменении состояния каналов связи или производительности сети модули мониторинга могут обнаружить событие и уведомить модуль Track; в свою очередь, Track отразит событие изменения и уведомит соответствующие функциональные модули.

11.9.2 Настройка

11.9.2.1 Настройка IP SLA для интерфейсов VRF

IP SLA (Service Level Agreement) — это инструмент измерения и диагностики производительности сети, использующий активный мониторинг. Активный мониторинг — это генерация трафика надежным и предсказуемым образом для измерения производительности сети. Каждая операция IP SLA имеет возвращаемое значение кода. Этот код интерпретируется процессом отслеживания. Код возврата имеет значения OK, Over Threshold и несколько других кодов. Различные операции могут иметь разные значения кодов возврата, поэтому используются только значения, общие для всех типов операций. В IP SLA используется ICMP Echo для проверки состояния или доступности маршрута.

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах топологии.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте экземпляр VRF.

```
Switch(config)# ip vrf vpn1
Switch(config-vrf)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip vrf forwarding vpn1
Switch(config-if)# ip address 192.168.0.2/24
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip vrf forwarding vpn1
Switch(config-if)# ip address 192.168.0.1/24
Switch(config-if)# exit
```

Шаг 4. Создайте IP SLA и задайте атрибуты.

Switch1:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# type icmp-echo 192.168.0.1
Switch(config-ipsla)# frequency 35
Switch(config-ipsla)# timeout 6
Switch(config-ipsla)# threshold 3000
Switch(config-ipsla)# ttl 65
Switch(config-ipsla)# tos 1
Switch(config-ipsla)# data-size 29
Switch(config-ipsla)# data-pattern abababab
Switch(config-ipsla)# fail-percent 90
Switch(config-ipsla)# packets-per-test 4
Switch(config-ipsla)# interval 9
Switch(config-ipsla)# statistics packet 10
Switch(config-ipsla)# statistics test 3
Switch(config-ipsla)# vrf vpn1
Switch(config-ipsla)# exit
```

NOTE Параметры для IP SLA:

- Частота: Время между двумя измерениями. Допустимый диапазон: 1–4800 секунд, значение по умолчанию — 60 секунд;
- timeout: таймаут для ответа ICMP. Допустимый диапазон: 1–4800 секунд, значение по умолчанию: 5 секунд;
- threshold: тайм-аут для ICMP-запроса. Допустимый диапазон: 1–4800000 миллисекунд, значение по умолчанию: 5000 миллисекунд;
- packets-per-test: Количество пакетов для каждой попытки. Допустимый диапазон: 1-10, значение по умолчанию: 3;
- Интервал: Время между двумя пакетами. Допустимый диапазон: 1–4800 секунд, значение по умолчанию — 6 секунд;
- Пакет статистики: Номер пакета для сбора статистики. Допустимый диапазон: 0-1000, значение по умолчанию: 50;
- Номер пробы. Допустимый диапазон: 0-10, значение по умолчанию: 5.

Шаг 5. Включить IP SLA.

Настройка коммутатора Switch1:

```
Switch(config)# ip sla monitor schedule 1
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Switch1.

```
Switch# sho ip sla monitor 1
Entry 1
Type                  : Echo
Admin state           : Disable
Destination address   : 192.168.0.1
Frequency             : 35s
Timeout               : 6s
Threshold             : 3000ms
Interval              : 9s
Packet per test       : 4
TTL                   : 65
TOS                   : 1
Data Size             : 29 bytes
Fail Percent          : 90%
Packet Item Cnt       : 10
Test Item Cnt         : 3
Vrf                   : vpn1
Return code           : Unknown
```

11.9.2.2 Настройка IP SLA для интерфейсов уровня 3

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах топологии:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.0.2/24
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.0.1/24
Switch(config-if)# exit
```

Шаг 3. Создайте IP SLA и задайте атрибуты.

Switch1:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# type icmp-echo  192.168.0.1
Switch(config-ipsla)# frequency 10
Switch(config-ipsla)# timeout 5
Switch(config-ipsla)# exit
```

Шаг 4. Включить IP SLA.

Switch1:

```
Switch(config)# ip sla monitor schedule 1
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Switch1.

```
Switch# show ip sla monitor
Entry 1
    Type                          : Echo
    Admin state                   : Enable
    Destination address           : 192.168.0.1
    Frequency                     : 10 seconds
    Timeout                       : 5 seconds
    Threshold                     : 5 seconds
    Running Frequency             : 8 seconds
Return code                       : OK

Switch# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.846 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.643 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.978 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.640 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.704 ms
```

Выключите интерфейс eth-0-1 на коммутаторе Switch2.

```
Switch(config)# interface eth-0-1
Switch(config-if)# shutdown
```

Повторно отобразите результат на Switch1.

```
Switch# show ip sla monitor
Entry 1
    Type                              : Echo
    Admin state                       : Enable
    Destination address               : 192.168.0.1
    Frequency                         : 10 seconds
    Timeout                           : 5 seconds
    Threshold                         : 5 seconds
    Running Frequency                 : 9 seconds
    Running Timeout                   : 4 seconds
    Running Threshold                 : 4 seconds
Return code                           : Timeout
```

11.9.2.3 Настройка IP SLA для исходящего интерфейса статического маршрута

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах топологии:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.0.2/24n
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.0.1/24
Switch(config-if)# exit

Switch(config)# interface loopback 1
```

```
Switch(config-if)# ip address 1.1.1.1/32
Switch(config-if)# exit
```

Шаг 3. Создайте IP SLA и задайте атрибуты.

Switch1:

```
Switch(config)# ip sla monitor 2
Switch(config-ipsla)# type icmp-echo 1.1.1.1
Switch(config-ipsla)# frequency 10
Switch(config-ipsla)# timeout 5
Switch(config-ipsla)# exit
```

Шаг 4. Включить IP SLA.

Switch1:

```
Switch(config)# ip sla monitor schedule 2
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

Switch1.

```
Switch# show ip sla monitor 2
Entry 2
    Type                          : Echo
    Admin state                       : Enable
    Destination address               : 1.1.1.1
    Frequency                     : 10 seconds
    Timeout                       : 5 seconds
    Threshold                         : 5 seconds
    Running Frequency                 : 1 seconds
    Return code                       : Unreachable
Switch# ping 1.1.1.1
connect: Network is unreachable
```

Создайте статический маршрут на Switch1

```
Switch#configure terminal
Switch(config)# ip route 1.1.1.1/32 192.168.0.1
Switch(config)# end
```

Повторно отобразите результат на Switch1.

```
Switch# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=1.03 ms
```

```
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=64 time=0.661 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=64 time=0.762 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=64 time=0.942 ms


Entry 2
    Type                              : Echo
    Admin state                       : Enable
    Destination address               : 1.1.1.1
    Frequency                         : 10 seconds
    Timeout                           : 5 seconds
    Threshold                         : 5 seconds
    Running Frequency                 : 8 seconds
    Return code                       : OK
```

11.9.2.4 Настройка трэкинга состояния интерфейса

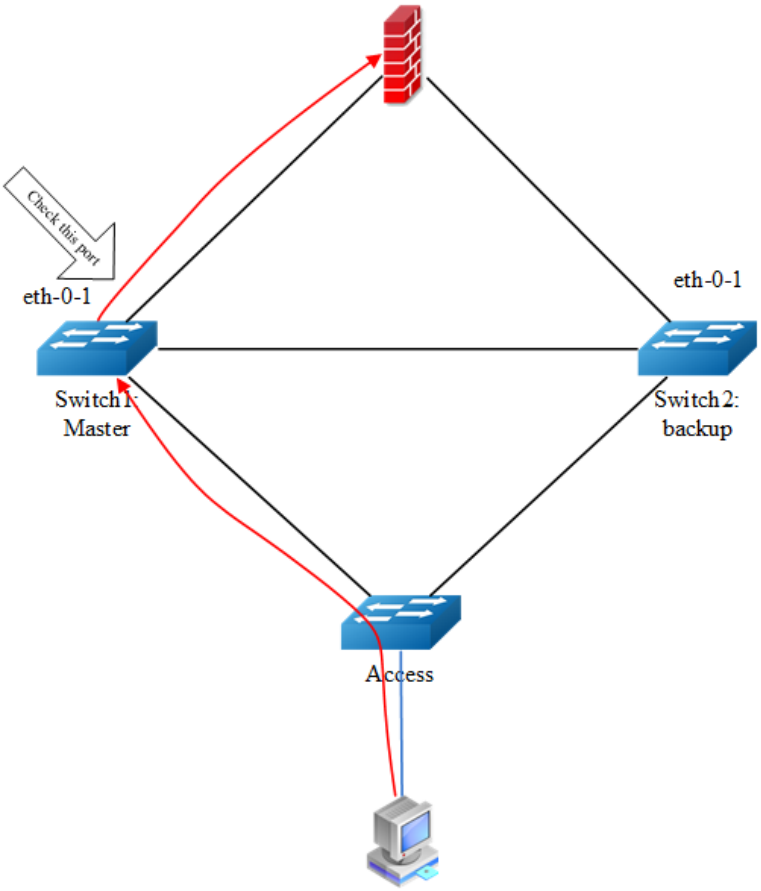


Рисунок 67 – Tracking интерфейса

До появления функции трекинга, VRRP имел простой механизм отслеживания, который позволял отслеживать только состояние соединения интерфейса. Если канал переставал работать, приоритет VRRP-маршрутизатора снижался, позволяя другому VRRP-маршрутизатору с

более высоким приоритетом стать активным. Функция трекинга же отделяет механизм отслеживания от VRRP и создает отдельный автономный процесс отслеживания, который может быть использован другими процессами. Эта функция позволяет отслеживать другие объекты в дополнение к состоянию соединения интерфейса. Теперь VRRP может зарегистрировать свою заинтересованность в отслеживании объектов и затем получать уведомления, когда отслеживаемый объект меняет состояние. Таким образом, TRACK — это отдельный автономный процесс, который может использоваться как другими процессами, так и VRRP. Функция позволяет отслеживать другие объекты в дополнение к состоянию канала интерфейса.

Настройка Switch1:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Создайте трек и задайте его атрибуты.

```
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# delay up 30
Switch(config-track)# delay down 30
Switch(config-track)# exit
```

NOTE Параметры трека:

- delay up: После того, как состояние интерфейса восстановится, трек будет ждать перед восстановлением состояний. Допустимый диапазон: 1-180 секунд. По умолчанию восстановление происходит без задержки$

- delay down: После того, как состояние интерфейса изменится на «отключено», трекер будет ждать перед изменением состояния. Допустимый диапазон: 1-180 секунд. Конфигурация по умолчанию — без задержки delay.

Шаг 3. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 4. Проверка.

```
Switch#show track
Track 2
    Type                    : Interface Link state
    Interface               : eth-0-1
    State                   : down
    Delay up                : 30 seconds
Delay down                  : 30 seconds
```

11.9.2.5 Настройка трэка доступности IP SLA

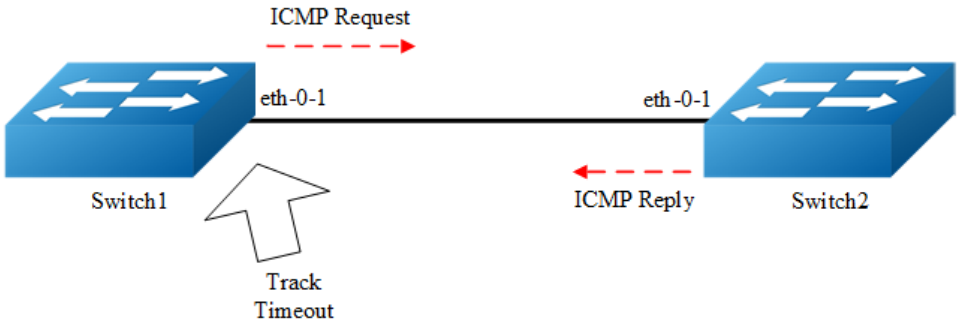


Рисунок 68 – Track IP SLA

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах топологии:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.0.2/24
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.0.1/24
```

Шаг 3. Создайте IP SLA и включите его.

Switch1:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# type icmp-echo  192.168.0.1
Switch(config-ipsla)# frequency 10
Switch(config-ipsla)# timeout 5
Switch(config-ipsla)# threshold 1
Switch(config-ipsla)# exit
Switch(config)# ip sla monitor schedule 1
```

Шаг 4. Создайте трек и задайте атрибуты.

Switch1:

```
Switch(config)# track 1 rtr 1 reachability
Switch(config-track)# delay up 30
Switch(config-track)# delay down 30
Switch(config-track)#exit
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

```
Switch#show track
Track 1
    Type                    : Response Time Reporter(RTR) Reachability
    RTR entry number      : 1
    State                   : up
    Delay up                : 30 seconds
Delay down                  : 30 seconds
```

11.9.2.6 Настройка трека состояния IP SLA

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах топологии:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.0.2/24
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.0.1/24
```

Шаг 3. Создайте IP SLA и включите его.

Switch1:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# type icmp-echo  192.168.0.1
Switch(config-ipsla)# frequency 10
Switch(config-ipsla)# timeout 5
Switch(config-ipsla)# threshold 1
Switch(config-ipsla)# exit
Switch(config)# ip sla monitor schedule 1
```

Шаг 4. Создайте трек и задайте атрибуты.

Switch1:

```
Switch(config)# track 1 rtr 1 state
Switch(config-track)# delay up 30
Switch(config-track)# delay down 30
Switch(config-track)#exit
```

Шаг 5. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 6. Проверка.

```
Switch# show track
Track 1
    Type                    : Response Time Reporter(RTR) State
    RTR entry number      : 1
    State                   : up
    Delay up                : 30 seconds
Delay down                  : 30 seconds
```

11.9.2.7 Настройка трека для VRRP

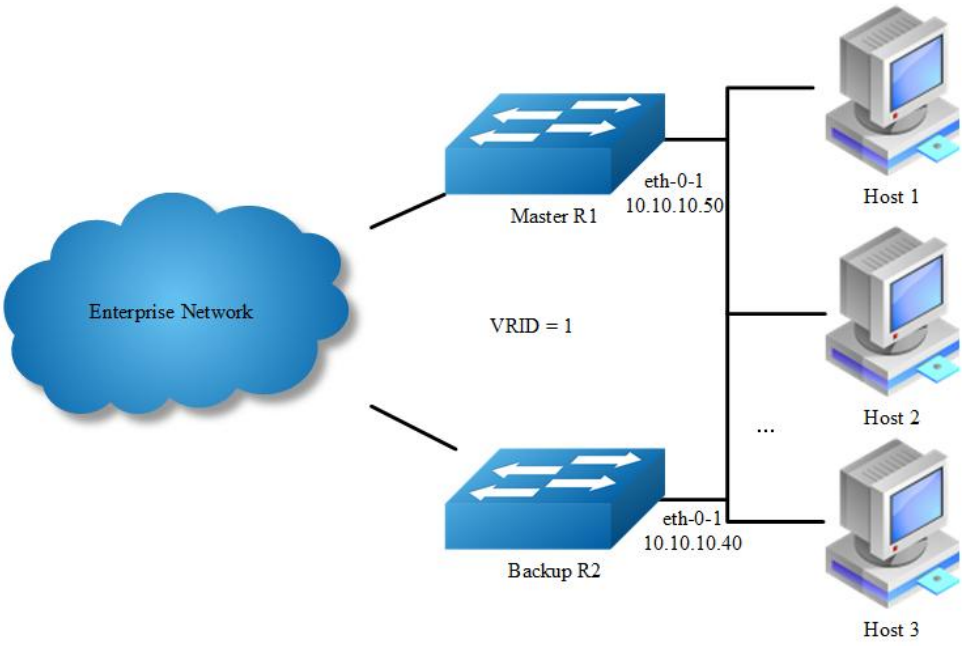


Рисунок 69 – VRRP Track

Шаг 1. Проверьте текущую конфигурацию.

Для справки - изучите главу «Настройка VRRP»

Отобразите конфигурацию на R1.

```
interface eth-0-1
 no switchport
 ip address 10.10.10.50/24
!
router vrrp 1
 interface eth-0-1
 virtual-ip 10.10.10.60
 advertisement-interval 5
 enable
```

Отобразите конфигурацию на R2.

```
interface eth-0-1
 no switchport
 ip address 10.10.10.40/24
!
router vrrp 1
 interface eth-0-1
 priority 200
 virtual-ip 10.10.10.60
 advertisement-interval 5
 enable
```

Шаг 2. Создайте трек и задайте его атрибуты.

Создать трек на Switch1

Привязка к состоянию интерфейса

```
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# exit
```

Привязка к CFM (см. раздел «CFM» данного руководства)

```
Switch(config)# track 1 cfm domain cust service cst
Switch(config-track)# exit
```

Примечание: мониторинг состояния RDI в пакетах CCM настраивается согласно следующему примеру:

```
Switch(config)# track 1 cfm domain cust service cst rdi-trigger
```

Шаг 3. Применить трек для VRRP.

Применить трек на Switch1

```
Switch(config)# router vrrp 1
Switch(config-router)# disable
Switch(config-router)# track 1 decrement 30
Switch(config-router)# enable
```

Шаг 4. Проверка.

Switch1:

```
Switch# show vrrp
vrrp session count: 1
VRID <1>
 State                : Backup
 Virtual IP           : 10.10.10.60(Not IP owner)
 Interface            : eth-0-9
 VMAC                 : 0000.5e00.0101
 VRF                  : Default
 Advt timer           : 5 second(s)
 Preempt mode         : TRUE
 Conf pri             : Unset          Run pri    : 100
 Increased pri        : 0
 Track Object         : 1
 Decre pri            : 30
 Master router ip     : 10.10.10.40
 Master priority      : 200
 Master advt timer    : 5 second(s)
 Master down timer    : 16 second(s)
 Preempt delay        : 0 second(s)
```

```
Learn master mode    : FALSE
BFD session state    : UNSET
```

11.9.2.8 Настройка трека для статического маршрута

Рисунок 70 – Track статического маршрута

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах топологии:

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)#interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.1.10/24
Switch(config-if)# exit
```

Switch2:

```
Switch(config)#interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 192.168.1.11/24
Switch(config-if)# exit
```

Шаг 3. Создайте IP SLA и включите его.

Switch1:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# type icmp-echo 192.168.1.11
Switch(config-ipsla)# exit
Switch(config)# ip sla monitor schedule 1
```

Шаг 4. Создайте трек и задайте атрибуты.

Настройка коммутатора Switch1:

```
Switch(config)# track 1 rtr 1 reachability
Switch(config-track)# exit
```

Шаг 5. Примените трек к статическому маршруту.

```
Switch(config)#ip route 10.10.10.0/24 192.168.1.11 track 1
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Switch1:

```
Switch# show ip sla monitor 1
Entry 1
    Type                  : Echo
    Admin state           : Enable
    Destination address   : 192.168.1.11
    Frequency             : 60 seconds
    Timeout               : 5 seconds
    Threshold             : 5 seconds
    Running Frequency     : 49 seconds
Return code           : OK

Switch# show track 1
Track 1
    Type                : Response Time Reporter(RTR) Reachability
    RTR entry number    : 1
    State               : up
Switch# show ip route static
S        10.10.10.0/24 [1/0] via 192.168.1.11, eth-0-1
```

Выключите интерфейс eth-0-1 на коммутаторе Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# shutdown
```

Повторно отобразите результат на Switch1:

```
Switch# show ip sla monitor 1
Entry 1
    Type                  : Echo
    Admin state           : Enable
    Destination address   : 192.168.1.11
    Frequency             : 60 seconds
    Timeout               : 5 seconds
    Threshold             : 5 seconds
```

```
    Running Frequency     : 8 seconds
Return code           : Timeout
Switch# show track 1
Track 1
    Type                  : Response Time Reporter(RTR) Reachability
    RTR entry number      : 1
    State                 : down
Switch# show ip route static
Switch#
```

11.10 Настройка VARP

11.10.1 Общие положения

11.10.1.1 Описание функции

Виртуальный ARP (VARP) позволяет нескольким коммутаторам одновременно маршрутизировать пакеты с одним и тем же MAC-адресом назначения. Каждый коммутатор настраивается с одним и тем же виртуальным MAC-адресом для интерфейсов L3, настроенных с виртуальным IP-адресом. В конфигурациях MLAG VARP предпочтительнее VRRP, поскольку VARP работает в активном режиме без передачи трафика через одноранговый канал.

Для запросов ARP и GARP к виртуальному IP-адресу VARP будет использовать виртуальный MAC-адрес для ответа. Виртуальный MAC-адрес используется только в поле назначения входящих пакетов и никогда не используется в поле адреса источника исходящих пакетов.

11.10.2 Настройка

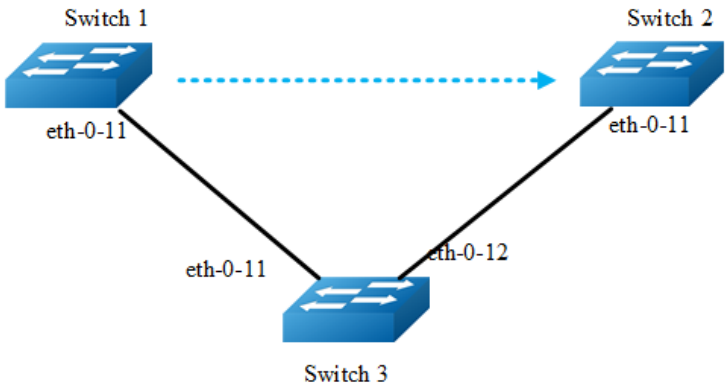


Рисунок 71 – Топология VARP совместно с MLAG

Если идентификатор устройства не указан, следующие настройки следует выполнить на всех устройствах топологии.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Установите MAC-адрес виртуального маршрутизатора.

```
Switch(config)# ip virtual-router mac aaa
```

Шаг 3. Войдите в режим настройки VLAN и создайте VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# exit
```

Шаг 4. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

```
Switch(config)# interface eth-0-11
Switch(config-if)# switchport access vlan 2
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Шаг 5. Создайте интерфейс VLAN, задайте IP-адрес и IP-адрес виртуального маршрутизатора.

Switch1:

```
Switch1(config)# interface vlan 2
Switch1(config-if)# ip address 10.10.10.1/24
Switch1(config-if)# ip virtual-router address 10.10.10.254
Switch1(config-if)# exit
```

Switch2:

```
Switch2(config-if)# interface vlan 2
Switch2(config-if)# ip address 10.10.10.2/24
Switch2(config-if)# ip virtual-router address 10.10.10.254
Switch2(config-if)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Switch1.

```
Switch1# show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
```

```
 Internet    10.10.10.1              -   cef0.12da.8100  vlan2
 Internet    10.10.10.254            -   000a.000a.000a  vlan2
```

Switch2.

```
Switch2#  show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    10.10.10.2              -   66d1.4c26.e100  vlan2
 Internet    10.10.10.254            -   000a.000a.000a  vlan2
```

12 Руководство по настройке функций виртуализации

12.1 Настройка VXLAN

12.1.1 Общие положения

12.1.1.1 Описание функции

Virtual Extensible LAN (виртуальная расширяемая локальная сеть (VXLAN) — это сетевая технология, которая инкапсулирует кадры Ethernet уровня 2 на основе MAC-адресов в пакеты UDP уровня 3 для объединения и туннелирования нескольких сетей уровня 2 в рамках инфраструктуры уровня 3. VXLAN масштабируется до 16 миллионов логических сетей и поддерживает смежность уровня 2 в IP-сетях. Для широковещательных/многоадресных/неизвестных пакетов используется подход многоадресной передачи.

Предыстория

В настоящее время виртуализация серверов получает все большее распространение, поскольку снижает затраты на оборудование, повышает гибкость бизнес-процессов, уменьшает затраты на техническое обслуживание и обладает другими преимуществами. Один физический сервер может быть виртуализирован в несколько виртуальных машин.

Иногда виртуальную машину необходимо перенести на новый сервер из-за ограниченности ресурсов сервера и других проблем (например, слишком высокая загрузка ЦП, недостаток места на диске и т. д.). Чтобы гарантировать бесперебойную работу бизнеса во время миграции, необходимо обеспечить неизменность IP-адреса, MAC-адреса и других параметров виртуальной машины. Это требует от бизнес-сети наличия резервных и надежных каналов связи.

Вышеуказанные требования приводят к постоянному расширению традиционного домена второго уровня. Традиционные сети становятся неспособными справиться с растущими требованиями второго уровня, что в основном отражается в следующих аспектах:

- в условиях крупных сетей уровня 2 пересылка пакетов осуществляется путем поиска в таблице MAC-адресов; объем таблицы MAC-адресов коммутатора ограничивает количество виртуальных машин.
- возможности сетевой изоляции ограничены, наиболее популярными методами изоляции являются VLAN или VPN (виртуальные частные сети). Однако у больших виртуальных сетей есть следующее ограничение: поскольку стандарт IEEE 802.1Q определяет размер тега VLAN как 12-битный, доступно только 4096 VLAN, что не может удовлетворить потребностям в больших сетях уровня 2.

- в традиционных сетях второго уровня VLAN/VPN не могут удовлетворить требования динамической перестройки сети. Структура сети ограничивает диапазон миграции виртуальных машин.

Для решения вышеуказанных проблем в крупных сетях второго уровня эффективно используется технология VXLAN (Virtual eXtensible Local Area Network).

- VXLAN решает проблему ограничений размера сети для виртуальных машин. VXLAN инкапсулирует пакеты данных, отправляемые виртуальными машинами, в протокол UDP, используя IP- и MAC-адреса из физической сети в качестве внешнего заголовка для инкапсуляции, а затем передавая пакеты после инкапсуляции в сеть.

- VXLAN, используя идентификаторы пользователей, аналогичные идентификаторам VLAN, импортирует 24-битные идентификаторы, что позволяет изолировать до 16 миллионов пользователей.

- Использование VXLAN для построения крупной сети уровня 2 гарантирует сохранение IP и MAC-адресов в процессе миграции виртуальных машин.

12.1.1.2 Терминология и механизм действия

VTEP (VXLAN Tunnel Endpoint) – это конечная точка туннеля VXLAN, устройство, используемое для инкапсуляции и декапсуляции пакетов VXLAN.

Основной принцип работы

На рисунке 2-1 показан формат пакета VXLAN. Пакет VXLAN содержит заголовок VXLAN и заголовок UDP/IP, которые добавляются к исходному пакету, отправленному виртуальной машиной или физическим сервером. Затем, используя добавленный MAC/IP-код, пакет пересылается на сетевые устройства. После этого декапсулированные пакеты восстанавливаются на конечной точке туннеля, и исходный пакет отправляется виртуальной машине или физическому серверу.

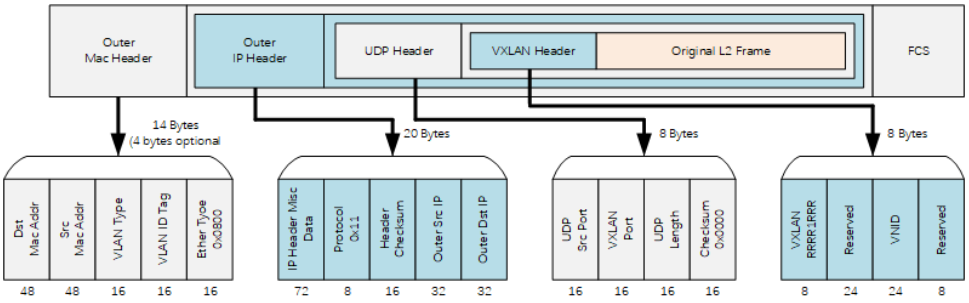


Рисунок 72 – Структура пакета VXLAN

Заголовок VXLAN включает в себя:

- Flag: 8 бит, значение протокола 00001000, пятый бит указывает, является ли пакет VXLAN действительным или нет;

- VNID: Идентификатор сети VXLAN, 24-битный, используется для различения секций VXLAN;

- Reserved: 24-битные и 8-битные значения, должны быть равны 0 для всех;

Заголовок UDP:

- Номер порта назначения — 4789, номер порта источника зависит от вычисления хэш-значения в соответствии с контекстом заголовка исходных пакетов.

Заголовок IP:

- IP-адрес источника — это IP-адрес VTEP, к которому принадлежит передающий сервер или виртуальная машина; IP-адрес назначения — это IP-адрес VTEP-сервера или виртуальной машины.

Ethernet заголовок:

- MAC-адрес источника: MAC-адрес физического сетевого интерфейса VTEP, отправляющего пакеты;

- Dst MAC: MAC-адрес следующего узла до целевого IP-адреса VTEP;

- VLAN: если нижележащая физическая сеть использует интерфейс VLAN, то в этом поле передается соответствующий тег VLAN.

Широковещательная рассылка на уровне 2

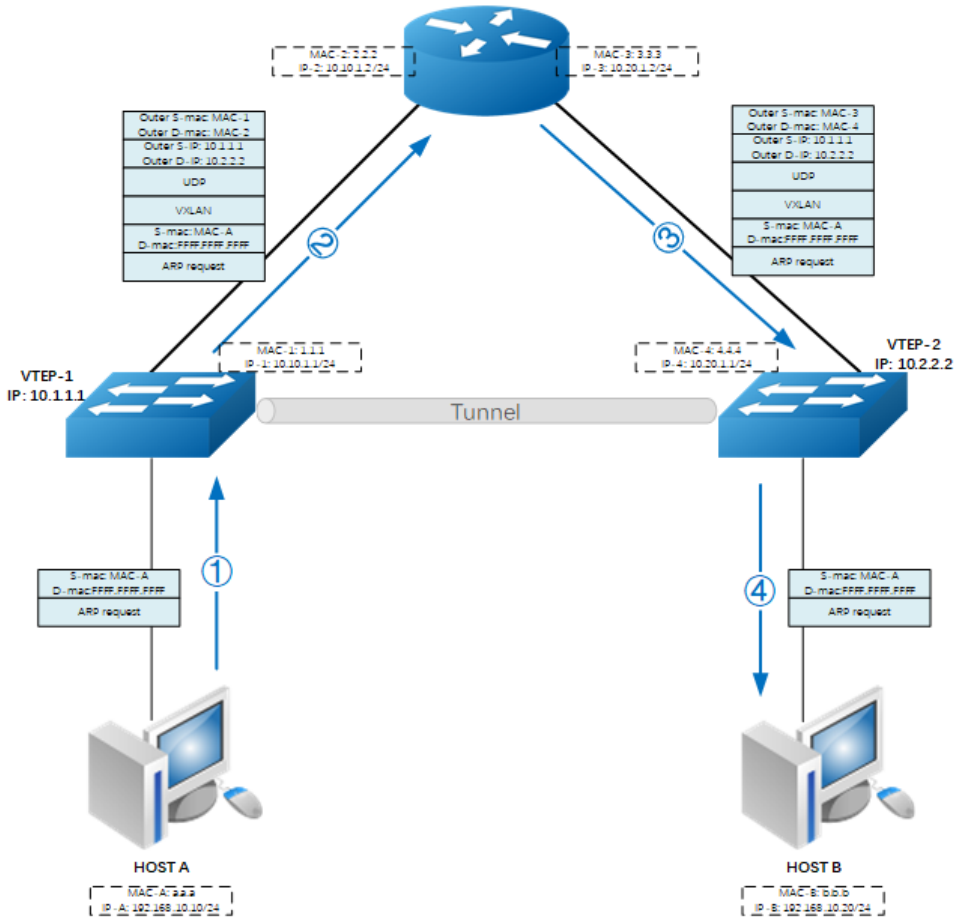


Рисунок 73 – Процесс пересылки широковещательных пакетов

Как показано на рисунке выше, хост A и хост B находятся в одном сетевом сегменте, но распределены по разным VTEP. Подробный процесс работы сети для хостов A и B выглядит следующим образом:

- Хост A и хост B находятся в одном сетевом сегменте. Хост A отправляет ARP-запрос для получения MAC-адреса хоста B.

- Когда запрошенный ARP-пакет достигает VTEP-1, коммутатор обнаруживает, что это широковещательный пакет, и его необходимо распространить по VLAN. Одна копия этого пакета отправляется в туннель VXLAN (если туннелей несколько, то в каждый туннель будет отправлен один пакет). VLAN сопоставляется с VNI с использованием инкапсуляции VXLAN, добавляется внешняя инкапсуляция UDP IP, и в соответствии с таблицей маршрутизации внешнего IP-адреса определяется следующий узел для этого пакета. Одновременно коммутатор запоминает MAC-адрес интерфейса eth-0-1 в соответствующем VLAN.

- Пересылка пакета до VTEP-2.

- После получения этого пакета VTEP-2 обнаружит, что MAC назначения является локальным адресом, и одновременно проверит, настроен ли соответствующий туннель в

локальной сети, используя S-IP, D-IP и VNI пакета. Если туннель есть, то будет выполнена операция декапсуляции: удаляется внешний заголовок, и VNI будет сопоставлен с соответствующим VLAN; после обнаружения широковещательного пакета будет произведена трансляция в VLAN.

Передача Unicast на уровне 2

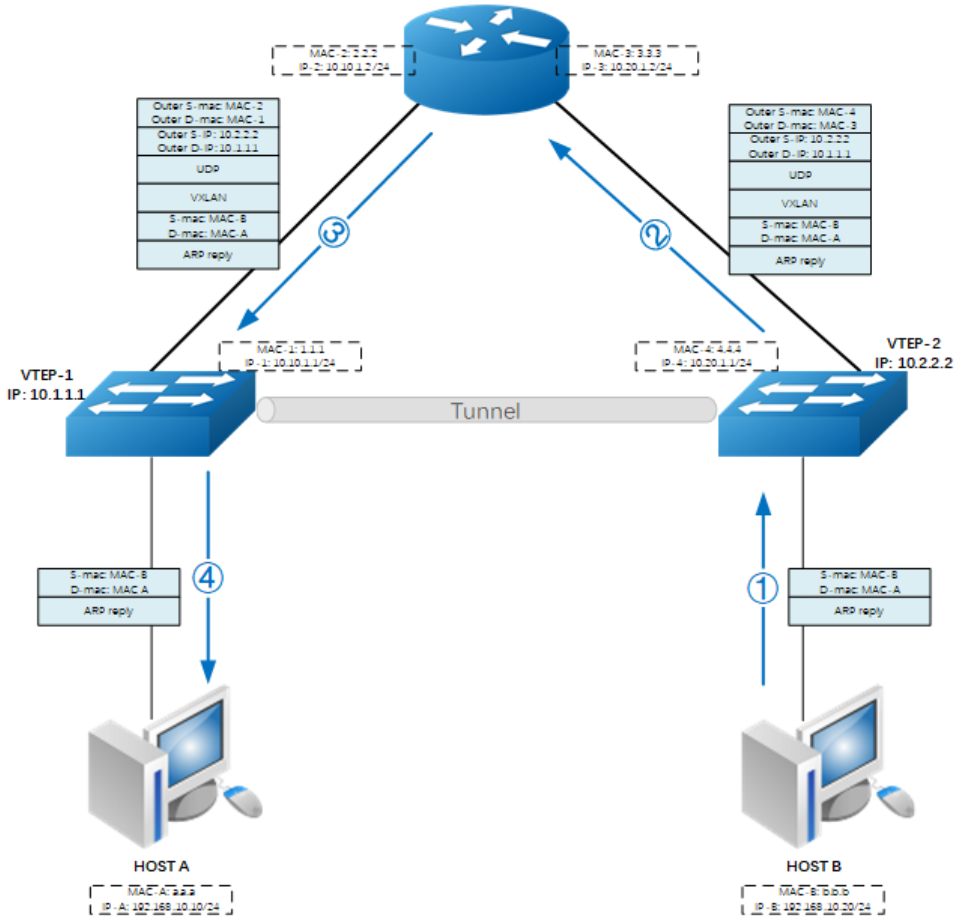


Рисунок 74 – Процесс пересылки одноадресных пакетов

Как показано на рисунке выше, хост B отвечает на ARP-запрос, отправленный хостом A; этот пакет является одноадресным. Данный пример демонстрирует процесс пересылки одноадресных пакетов:

- Хост B отправляет ARP-ответ; он достигнет коммутатора VTEP-2 через интерфейс eth-0-1;
- На VTEP-2 будет установлено, что исходящий интерфейс MAC-B представляет собой туннель VXLAN в этой VLAN, а удаленный терминал VTEP имеет IP-адрес 10.1.1.1, что будет определено путем поиска в таблице MAC-адресов с помощью Dst-mac; затем VLAN, в котором находится исходный пакет, будет сопоставлен с VNI, и будет добавлен заголовок VXLAN, а также заголовок внешнего MAC/IP, где Outer S-IP будет указан как локальный IP-адрес VTEP, Outer D-IP

— как IP-адрес удаленного терминала VTEP, Outer S-mac — как локальный MAC-адрес исходящего интерфейса, Outer D-mac — как MAC-адрес интерфейса следующего перехода для Outer D-IP;

- Пакет пересылается и достигает VTEP-1;

- После получения пакета и обнаружения, что внешний D-mac является локальным адресом, VTEP-1 проверяет, настроен ли соответствующий туннель на основе внешнего S-IP, внешнего D-IP и VNI пакета. VTEP-1 выполняет декапсуляцию, удаляя внешний заголовок и сопоставляя VNI с соответствующим VLAN, а также выполняет поиск в таблице MAC-адресов по целевому MAC-адресу исходного пакета (MAC-A); затем обнаруживает, что исходящий интерфейс MAC-A — это eth-0-1, после чего отправляет пакет через eth-0-1.

NOTE По умолчанию VTEP использует туннели, соединенные друг с другом; если после декапсуляции обнаруживается, что выходной Dst-mac представляет собой туннель, то пакет будет отброшен.

Работа VXLAN в топологии с сетевым шлюзом

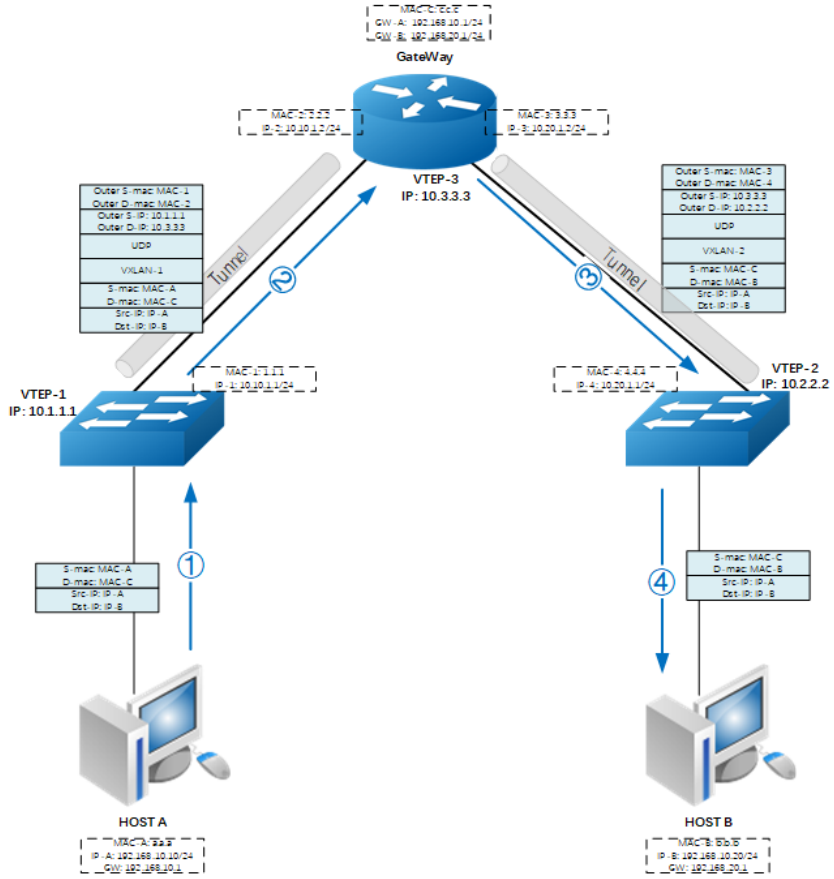


Рисунок 75 – Процесс работы сетевого шлюза и VXLAN

Как показано на рисунке выше, хосты A и B находятся в разных сетевых секциях, и для организации сети между ними необходим сетевой шлюз. В этой ситуации можно выполнить настройку сетевого шлюза на VTEP-3, после чего VTEP-1 и VTEP-2 создадут отдельные VXLAN-туннели к VTEP-3.

Хост A отправляет ARP-запрос для получения MAC-адреса шлюза, VTEP-1 выполняет инкапсуляцию VXLAN для этого ARP-запроса, а затем перенаправляет его на VTEP-3 как неизвестный одноадресный трафик.

VTEP-3 определит, имеет ли он адрес шлюза после получения ARP-запроса. Если имеет, то он отправляет ARP-ответ с инкапсуляцией VXLAN хосту A и изучает ARP-запись хоста A; его исходящий интерфейс представляет собой туннель VXLAN.

VTEP-1 удалит заголовок VXLAN после получения этого ARP-ответа; он перешлет исходный ARP-ответ хосту A и узнает MAC-адрес шлюза, а его исходящий интерфейс будет туннелем VXLAN.

Когда хост A получает ARP-ответ, он запоминает MAC-адрес шлюза и начинает отправлять пакет данных.

После получения этого пакета шлюз определит, нужно ли ему перенаправлять трафик (в таблице ARP хоста B отсутствуют какие-либо записи). Поэтому он отправит запрос ARP для создания ARP-записи для хоста B, который добавит в заголовок VXLAN к VTEP-2.

После получения ARP-запроса VTEP-2 декапсулирует его и пересылает хосту B (исходящий интерфейс представляет собой туннель VXLAN).

Хост B отправляет ARP-ответ, MAC-адрес назначения которого совпадает с MAC-адресом шлюза; он выполнит поиск и переадресацию на VTEP-2 и обнаружит, что исходящий интерфейс представляет собой туннель VXLAN, поэтому VTEP-2 выполнит инкапсуляцию этого пакета в VXLAN и отправит его на шлюз.

После получения этого пакета шлюз изучает ARP-запись для хоста B, и затем пересылает пакет данных хосту B через туннель VXLAN.

Сетевой шлюз распределенной сети VXLAN

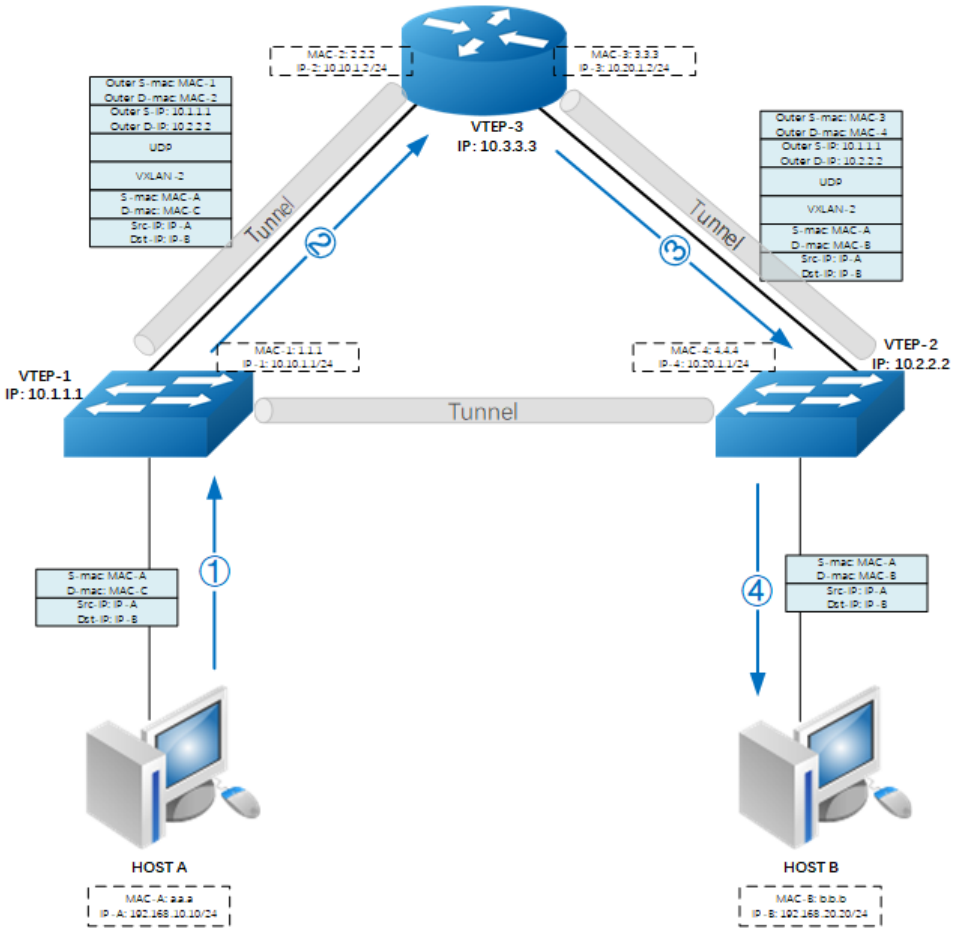


Рисунок 76 – Процесс работы сетевого шлюза распределенной сети VXLAN

Вместо того чтобы функция маршрутизации выполнялась одним шлюзом, у нас есть возможность распределить функцию маршрутизации между каждым подключенным VTEP, что снизит нагрузку на один сетевой шлюз.

Как показано на рисунке выше, IP-B — это хост, подключенный к VTEP-2, идентификатор VXLAN — VXLAN-2. На основании приведенной выше информации мы можем настроить таблицу маршрутизации на входящем VTEP (который на рисунке 5 обозначен как VTEP-1), напрямую инкапсулировать пакеты и отправлять их на IP-B, чтобы снизить нагрузку на шлюз и одновременно уменьшить задержку пересылки. Подробный процесс пересылки выглядит следующим образом:

- Хост A отправляет пакет с Dst-ip равным IP-B. Поскольку IP-B и этот IP-адрес (IP-A) находятся в разных сетевых разделах, следовательно, Dst-mac — это MAC-адрес шлюза (Mac-C);

- Когда пакет достигает VTEP-1, VTEP-1 обнаруживает, что Dst-mac является MAC-адресом шлюза в сети VLAN, и затем проверяет наличие маршрутной информации IP-B в таблице маршрутизации. Если она существует, то осуществляется пересылка по таблице маршрутизации; эта запись маршрута включает информацию об идентификаторах VTEP и VXLAN, где находится

IP-B, и соответствующую информацию о MAC-адресе (Mac-B) IP-B. На VTEP-1 Dst-mac заменяется на Mac-B, добавляется соответствующая инкапсуляция в зависимости от информации внешнего пакета, после чего начинается пересылка; если же Dst-mac отсутствует, то пакет отбрасывается;

- Пересылка пакета будет осуществляться в соответствии с внешним тэгом;
- Пакет декапсулируется, когда достигает VETP-2; процесс декапсуляции аналогичен пересылке на уровне 2.

NOTE Распределённому шлюзу требуется поддержка протокола BGP EVPN для синхронизации элементов таблицы ARP, либо статическая настройка маршрутизации DVR.

12.1.2 Настройка VXLAN

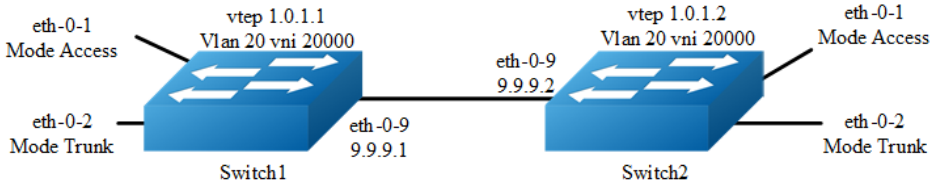


Рисунок 77 – Топология VXLAN

В следующем примере коммутаторы Switch1 и Switch2 соединены маршрутом уровня 3. Трафик VLAN 20 инкапсулируется в VNI 20000 для прохождения через сети уровня 3.

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах топологии.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN, включите Overlay для каждого VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 20
Switch(config-vlan)# vlan 20 overlay enable
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 20
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

```
Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.1/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 1.0.1.1/32
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.2/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 1.0.1.2/32
Switch(config-if)# exit
```

Шаг 4. Создайте статический маршрут.

Настройка коммутатора Switch1:

```
Switch(config)# ip route 1.0.1.2/32 9.9.9.2
```

Настройка коммутатора Switch2:

```
Switch(config)# ip route 1.0.1.1/32 9.9.9.1
```

Шаг 5. Настройка атрибутов Overlay

Switch1:

```
Switch(config)# overlay
Switch(config-overlay)# source 1.0.1.1
Switch(config-overlay)# remote-vtep 1 ip-address 1.0.1.2 type vxlan
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# exit
```

Switch2:

```
Switch(config)# overlay
Switch(config-overlay)# source 1.0.1.2
Switch(config-overlay)# remote-vtep 1 ip-address 1.0.1.1 type vxlan
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Switch1:

```
Switch# show overlay vlan 20
------------------------------------------------------------------------------
--
ECMP Mode         : Normal
Source VTEP       : 1.0.1.1
------------------------------------------------------------------------------
--
VLAN ID                         : 20
VNI                             : 20000
EVPN Tunnel Data-fdb Learning   : Enable
Remote VTEP NUM                 : 1
          Index: 1, Ip address: 1.0.1.2, Source ip: 1.0.1.1, Type: VxLAN,
Protocol: Static
DVR Gateway NUM: 0
------------------------------------------------------------------------------
```

Switch2:

```
Switch# show overlay vlan 20
------------------------------------------------------------------------------
```

```
--
ECMP Mode          : Normal
Source VTEP        : 1.0.1.2
------------------------------------------------------------------------------
--
VLAN ID                          : 20
VNI                              : 20000
EVPN Tunnel Data-fdb Learning    : Eanble
Remote VTEP NUM                  : 1
          Index: 1, Ip address: 1.0.1.1, Source ip: 1.0.1.2, Type: VxLAN,
Protocol: Static
DVR Gateway NUM: 0
------------------------------------------------------------------------------
--
```

12.1.2.1 Настройка VXLAN маршрутизации

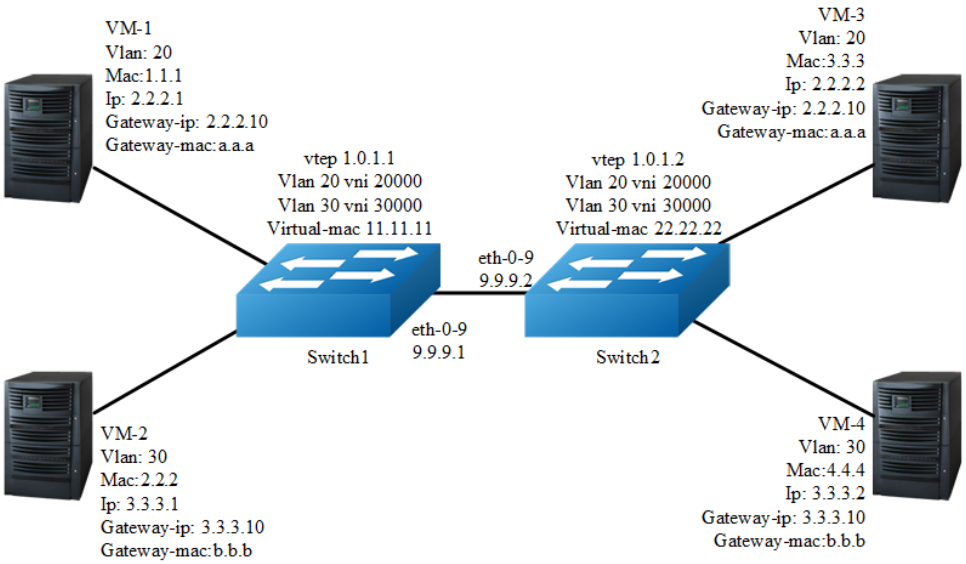


Рисунок 78 – Топология сети при VXLAN маршрутизации

В следующем примере VM-1 и VM-3 инкапсулированы в один и тот же VNI для формирования распределенного маршрута через VXLAN; VM-2 и VM-4 инкапсулированы в другой VNI для формирования распределенного маршрута через VXLAN.

Если идентификатор коммутатора не указан, следующие действия по настройке следует выполнить на всех коммутаторах топологии.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN, включите overlay для каждого VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 20,30
Switch(config-vlan)# vlan 20 overlay enable
Switch(config-vlan)# vlan 30 overlay enable
Switch(config-vlan)# exit
```

Шаг 3. Создайте экземпляр VRF.

```
Switch(config)# ip vrf tenant
Switch(config-vrf)# exit
```

Шаг 4. Создайте интерфейс уровня 3 и задайте IP-адрес.

Switch1:

```
Switch(config)# interface vlan 20
Switch(config-if)# ip vrf forwarding tenant
Switch(config-if)# ip address 2.2.2.111/24
Switch(config-if)# exit

Switch(config)# interface vlan 30
Switch(config-if)# ip vrf forwarding tenant
Switch(config-if)# ip address 3.3.3.111/24
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface  vlan 20
Switch(config-if)# ip vrf forwarding tenant
Switch(config-if)# ip address 2.2.2.222/24
Switch(config-if)# exit

Switch(config)# interface  vlan 30
Switch(config-if)# ip vrf forwarding tenant
Switch(config-if)# ip address 3.3.3.222/24
Switch(config-if)# exit
```

Шаг 5. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

```
Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add  30
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Switch1:

```
Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.1/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 1.0.1.1/32
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.2/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 1.0.1.2/32
Switch(config-if)# exit
```

Шаг 6. Настройка атрибутов Overlay.

Switch1:

```
Switch(config)# overlay
Switch(config-overlay)# source 1.0.1.1
Switch(config-overlay)# remote-vtep 1 ip-address 1.0.1.2 type vxlan
Switch(config-overlay)# remote-vtep 1 virtual-mac 22.22.22
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 30 vni 30000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# vlan 30 remote-vtep 1
Switch(config-overlay)# vlan 20 gateway-mac a.a.a
Switch(config-overlay)# vlan 30 gateway-mac b.b.b
Switch(config-overlay)# exit
```

Switch2:

```
Switch(config)# overlay
Switch(config-overlay)# source 1.0.1.2
Switch(config-overlay)# remote-vtep 1 ip-address 1.0.1.1 type vxlan
Switch(config-overlay)# remote-vtep 1 virtual-mac 11.11.11
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 30 vni 30000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# vlan 30 remote-vtep 1
Switch(config-overlay)# vlan 20 gateway-mac a.a.a
Switch(config-overlay)# vlan 30 gateway-mac b.b.b
Switch(config-overlay)# exit
```

Шаг 7. Создайте статические маршруты и маршруты VXLAN.

Switch1:

```
Switch(config)# ip route 1.0.1.2/32 9.9.9.2
Switch(config)# ip route vrf tenant 2.2.2.2/32 remote-vtep 1 vni 20000 inner-
macda 3.3.3
Switch(config)# ip route vrf tenant 3.3.3.2/32 remote-vtep 1 vni 30000 inner-
macda 4.4.4
```

Switch2:

```
Switch(config)# ip route 1.0.1.1/32 9.9.9.1
Switch(config)# ip route vrf tenant 2.2.2.1/32 remote-vtep 1 vni 20000 inner-
macda 1.1.1
Switch(config)# ip route vrf tenant 3.3.3.1/32 remote-vtep 1 vni 30000 inner-
macda 2.2.2
```

Шаг 8. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 9. Проверка.

Switch1:

```
Switch# show ip route vrf tenant
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       Dc - DHCP Client
       [*] - [AD/Metric]
       * - candidate default
S        2.2.2.2/32 is in overlay remote vxlan vtep:1.0.1.1->1.0.1.2,
```

```
vni:20000
S        3.3.3.2/32 is in overlay remote vxlan vtep:1.0.1.1->1.0.1.2,
vni:30000
```

Switch2:

```
Switch# show ip route vrf tenant
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       Dc - DHCP Client
       [*] - [AD/Metric]
       * - candidate default
S        2.2.2.1/32 is in overlay remote vxlan vtep:1.0.1.2->1.0.1.1,
vni:20000
S        3.3.3.1/32 is in overlay remote vxlan vtep:1.0.1.2->1.0.1.1,
vni:30000
```

Пользователи в одном сетевом сегменте обмениваются данными через сеть VXLAN

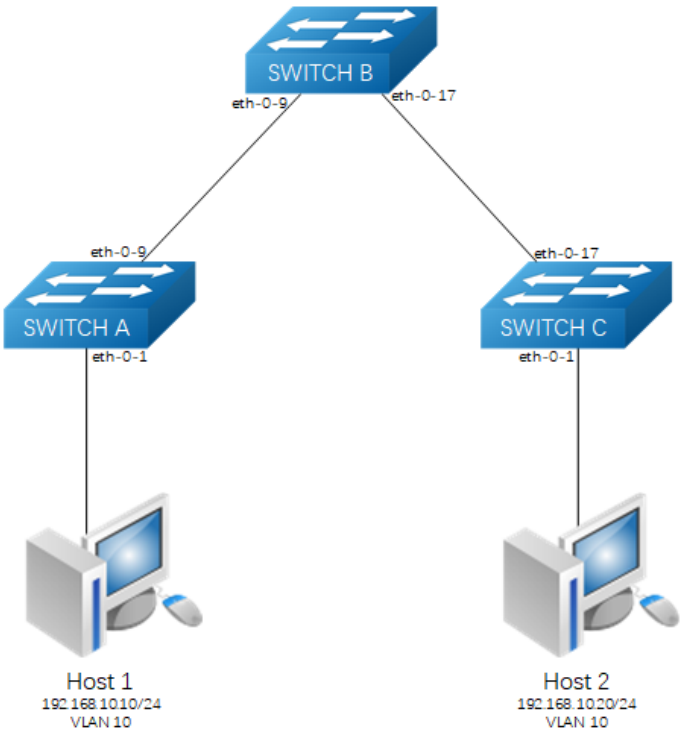


Рисунок 79 – Сетевая коммутация VXLAN

Хост 1 и Хост 2 находятся в одном сегменте, им необходимо обеспечить обмен данными через туннели VXLAN.

Шаг 1. Настройте маршрутизацию на коммутаторах A, B, C, убедитесь, что эти три коммутатора могут общаться друг с другом в сети уровня 3.

Настройка SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# interface loopback 0
SWITCH_A(config-if)# ip address 10.1.1.1/32
SWITCH_A(config-if)# exit
SWITCH_A(config)# interface eth-0-9
SWITCH_A(config-if)# no switchport
SWITCH_A(config-if)# ip address 192.168.1.1/24
SWITCH_A(config-if)# vxlan uplink enable
SWITCH_A(config-if)# no shutdown
SWITCH_A(config-if)# exit
SWITCH_A(config)# ip route 10.3.3.3/32 192.168.1.2
SWITCH_A(config)# end
```

Настройка SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# interface eth-0-9
SWITCH_B(config-if)# no switchport
SWITCH_B(config-if)# ip address 192.168.1.2/24
SWITCH_B(config-if)# no shutdown
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface eth-0-17
SWITCH_B(config-if)# no switchport
SWITCH_B(config-if)# ip address 192.168.2.1/24
SWITCH_B(config-if)# no shutdown
SWITCH_B(config-if)# exit
SWITCH_B(config)# ip route 10.1.1.1/32 192.168.1.1
SWITCH_B(config)# ip route 10.3.3.3/32 192.168.2.2
SWITCH_B(config)# end
```

Настройка SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# interface loopback 0
SWITCH_C(config-if)# ip address 10.3.3.3/32
SWITCH_C(config-if)# exit
SWITCH_C(config)# interface eth-0-17
SWITCH_C(config-if)# no switchport
SWITCH_C(config-if)# ip address 192.168.2.2/24
SWITCH_C(config-if)# vxlan uplink enable
SWITCH_C(config-if)# no shutdown
SWITCH_C(config-if)# exit
```

```
SWITCH_C(config)# ip route 10.1.1.1/32 192.168.2.1
SWITCH_C(config)# end
```

Шаг 2. Настройка VLAN на коммутаторах A и C.

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# vlan database
SWITCH_A(config-vlan)# vlan 10
SWITCH_A(config-vlan)# vlan 10 overlay enable
SWITCH_A(config-vlan)# exit
SWITCH_A(config)# interface eth-0-1
SWITCH_A(config-if)# switchport mode access
SWITCH_A(config-if)# switchport access vlan 10
SWITCH_A(config-if)# no shutdown
SWITCH_A(config-if)# end
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# vlan database
SWITCH_C(config-vlan)# vlan 10
SWITCH_C(config-vlan)# vlan 10 overlay enable
SWITCH_C(config-vlan)# exit
SWITCH_C(config)# interface eth-0-1
SWITCH_C(config-if)# switchport mode access
SWITCH_C(config-if)# switchport access vlan 10
SWITCH_C(config-if)# no shutdown
SWITCH_C(config-if)# end
```

Шаг 3. Настройка туннелей VXLAN на коммутаторах A и C.

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# overlay
SWITCH_A(config-overlay)# source 10.1.1.1
SWITCH_A(config-overlay)# remote-vtep 1 ip-address 10.3.3.3 type vxlan
SWITCH_A(config-overlay)# vlan 10 vni 10000
SWITCH_A(config-overlay)# vlan 10 remote-vtep 1
SWITCH_A(config-overlay)# end
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# overlay
```

```
SWITCH_C(config-overlay)# source 10.3.3.3
SWITCH_C(config-overlay)# remote-vtep 1 ip-address 10.1.1.1 type vxlan
SWITCH_C(config-overlay)# vlan 10 vni 10000
SWITCH_C(config-overlay)# vlan 10 remote-vtep 1
SWITCH_C(config-overlay)# end
```

Шаг 4. Проверка.

Проверьте взаимодействие между сетями

```
SWITCH_A# ping
Protocol [ip]:
Target IP address: 10.3.3.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Data pattern [0xABCD]:
PATTERN: 0xabcd
PING 10.3.3.3 (10.3.3.3) from 10.1.1.1 : 100(128) bytes of data.
108 bytes from 10.3.3.3: icmp_seq=0 ttl=63 time=775 ms
108 bytes from 10.3.3.3: icmp_seq=1 ttl=63 time=904 ms
108 bytes from 10.3.3.3: icmp_seq=2 ttl=63 time=768 ms
108 bytes from 10.3.3.3: icmp_seq=3 ttl=63 time=668 ms
108 bytes from 10.3.3.3: icmp_seq=4 ttl=63 time=723 ms

--- 10.3.3.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 668.636/768.201/904.300/78.078 ms, pipe 2
```

Проверьте правильность конфигурации туннелей

```
SWITCH_A# show overlay vlan 10
------------------------------------------------------------
ECMP Mode         : Normal
Source VTEP       : 10.1.1.1
------------------------------------------------------------
VLAN ID         : 10
VNI             : 10000
Remote VTEP NUM: 1
          Index: 1, Ip address: 10.3.3.3,  Type: VxLAN
DVR Gateway NUM: 0
------------------------------------------------------------
SWITCH_A#
SWITCH_A# show overlay uplink
------------------------------------------------------------
```

```
Uplink port:
    eth-0-9
-------------------------------------------------------------
```

12.1.2.2 Опорный (консолидирующий) шлюз VXLAN

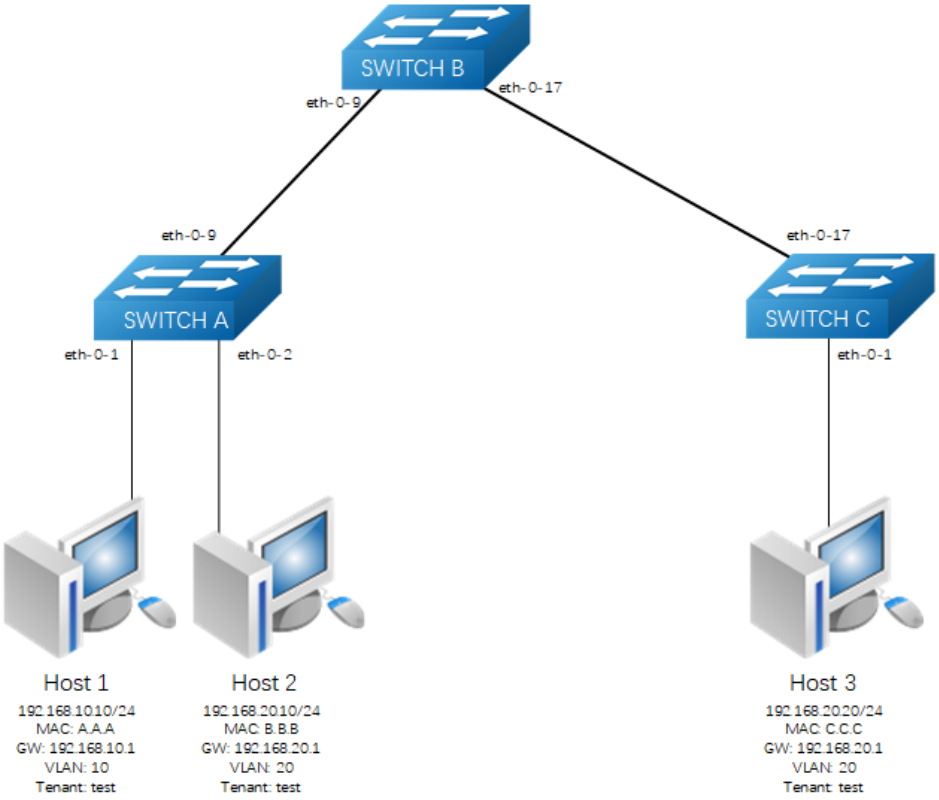


Рисунок 80 – Тополоигия сети при опорном (консолидирующим) шлюзе VXLAN

Как показано на рисунке, Хосты 1-3 относятся к тестовой топологии, где есть как одинаковые, так и различные сегменты, и все они нуждаются во взаимодействии друг с другом. Между коммутаторами A, B и C находится сеть уровня 3, поэтому необходимо создать туннели путем настройки VXLAN и реализовать сетевое взаимодействие между HOST через централизованный опорный сетевой шлюз.

NOTE В качестве такого шлюза можно выбрать коммутатор B.

Шаг 1. Настройте маршрутизацию на коммутаторах A, B и C, убедитесь, что эти три коммутатора могут общаться друг с другом в сети уровня 3.

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
SWITCH_A(config)# interface loopback 0
SWITCH_A(config-if)# ip address 10.1.1.1/32
SWITCH_A(config-if)# exit
SWITCH_A(config)# interface eth-0-9
SWITCH_A(config-if)# no switchport
SWITCH_A(config-if)# ip address 192.168.9.1/24
SWITCH_A(config-if)# no shutdown
SWITCH_A(config-if)# exit
SWITCH_A(config)# ip route 10.2.2.2/32 192.168.9.2
SWITCH_A(config)# ip route 10.3.3.3/32 192.168.9.2
SWITCH_A(config)# end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# interface loopback 0
SWITCH_B(config-if)# ip address 10.2.2.2/32
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface eth-0-9
SWITCH_B(config-if)# no switchport
SWITCH_B(config-if)# ip address 192.168.9.2/24
SWITCH_B(config-if)# no shutdown
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface eth-0-17
SWITCH_B(config-if)# no switchport
SWITCH_B(config-if)# ip address 192.168.17.2/24
SWITCH_B(config-if)# no shutdown
SWITCH_B(config-if)# exit
SWITCH_B(config)# ip route 10.3.3.3/32 192.168.17.1
SWITCH_B(config)# ip route 10.1.1.1/32 192.168.9.1
SWITCH_B(config)# end
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# interface loopback 0
SWITCH_C(config-if)# ip address 10.3.3.3/32
SWITCH_C(config-if)# exit
SWITCH_C(config)# interface eth-0-17
SWITCH_C(config-if)# no switchport
SWITCH_C(config-if)# ip address 192.168.17.1/24
SWITCH_C(config-if)# no shutdown
SWITCH_C(config-if)# exit
SWITCH_C(config)# ip route 10.1.1.1/32 192.168.17.2
SWITCH_C(config)# ip route 10.2.2.2/32 192.168.17.2
SWITCH_C(config)# end
```

Шаг 2. Настройте VLAN на коммутаторах A, B и C.

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# vlan database
SWITCH_A(config-vlan)# vlan 10,20
SWITCH_A(config-vlan)# vlan 10 overlay enable
SWITCH_A(config-vlan)# vlan 20 overlay enable
SWITCH_A(config-vlan)# exit
SWITCH_A(config)# interface eth-0-1
SWITCH_A(config-if)# switchport mode access
SWITCH_A(config-if)# switchport access vlan 10
SWITCH_A(config-if)# no shutdown
SWITCH_A(config-if)# exit
SWITCH_A(config)# interface eth-0-2
SWITCH_A(config-if)# switchport mode access
SWITCH_A(config-if)# switchport access vlan 20
SWITCH_A(config-if)# no shutdown
SWITCH_A(config-if)# end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# vlan database
SWITCH_B(config-vlan)# vlan 10,20
SWITCH_B(config-vlan)# vlan 10 overlay enable
SWITCH_B(config-vlan)# vlan 20 overlay enable
SWITCH_B(config-vlan)# exit
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# vlan database
SWITCH_C(config-vlan)# vlan 20
SWITCH_C(config-vlan)# vlan 20 overlay enable
SWITCH_C(config-vlan)# exit
SWITCH_C(config)# interface eth-0-1
SWITCH_C(config-if)# switchport mode access
SWITCH_C(config-if)# switchport access vlan 20
SWITCH_C(config-if)# no shutdown
SWITCH_C(config-if)# exit
```

Шаг 3. Создайте туннели VXLAN между коммутаторами A, B и C.

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# interface eth-0-9
SWITCH_A(config-if)# vxlan uplink enable
SWITCH_A(config-if)# exit
SWITCH_A(config)# overlay
SWITCH_A(config-overlay)# source 10.1.1.1
SWITCH_A(config-overlay)# remote-vtep 1 ip-address 10.2.2.2 type vxlan
SWITCH_A(config-overlay)# remote-vtep 2 ip-address 10.3.3.3 type vxlan
SWITCH_A(config-overlay)# vlan 10 vni 10000
SWITCH_A(config-overlay)# vlan 10 remote-vtep 1
SWITCH_A(config-overlay)# vlan 20 vni 20000
SWITCH_A(config-overlay)# vlan 20 remote-vtep 1
SWITCH_A(config-overlay)# vlan 20 remote-vtep 2
SWITCH_A(config-overlay)# end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# interface eth-0-9
SWITCH_B(config-if)# vxlan uplink enable
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface eth-0-17
SWITCH_B(config-if)# vxlan uplink enable
SWITCH_B(config-if)# exit
SWITCH_B(config)# overlay
SWITCH_B(config-overlay)# source 10.2.2.2
SWITCH_B(config-overlay)# remote-vtep 1 ip-address 10.1.1.1 type vxlan
SWITCH_B(config-overlay)# remote-vtep 2 ip-address 10.3.3.3 type vxlan
SWITCH_B(config-overlay)# vlan 10 vni 10000
SWITCH_B(config-overlay)# vlan 10 remote-vtep 1
SWITCH_B(config-overlay)# vlan 20 vni 20000
SWITCH_B(config-overlay)# vlan 20 remote-vtep 1
SWITCH_B(config-overlay)# vlan 20 remote-vtep 2
SWITCH_B(config-overlay)# end
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# interface eth-0-17
SWITCH_C(config-if)# vxlan uplink enable
SWITCH_C(config-if)# exit
SWITCH_C(config)# overlay
SWITCH_C(config-overlay)# source 10.3.3.3
SWITCH_C(config-overlay)# remote-vtep 1 ip-address 10.1.1.1 type vxlan
SWITCH_C(config-overlay)# remote-vtep 2 ip-address 10.2.2.2 type vxlan
SWITCH_C(config-overlay)# vlan 20 vni 20000
SWITCH_C(config-overlay)# vlan 20 remote-vtep 1
```

```
SWITCH_C(config-overlay)# vlan 20 remote-vtep 2
SWITCH_C(config-overlay)# end
```

Шаг 4. Настройте соответствующий шлюз для хоста на коммутаторе B и привяжите его к соответствующему VRF.

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# ip vrf test
SWITCH_B(config-vrf)# exit
SWITCH_B(config)# interface vlan 10
SWITCH_B(config-if)# ip vrf forwarding test
SWITCH_B(config-if)# ip address 192.168.10.1/24
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface vlan 20
SWITCH_B(config-if)# ip vrf forwarding test
SWITCH_B(config-if)# ip address 192.168.20./24
SWITCH_B(config-if)# end
```

На этом этапе настройка завершена; хосты 1-4 могут взаимодействовать друг с другом – пинг между ними есть.

NOTE В данном случае VRF используется для разделения сегментов сети. Конфигурация опциональна.

Шаг 5. Проверка.

Проверьте взаимодоступность сетей

```
SWITCH_A# ping -a 10.1.1.1 10.2.2.2
PING 10.2.2.2 (10.2.2.2) from 10.1.1.1 : 56(84) bytes of data.
64 bytes from 10.2.2.2: icmp_seq=1 ttl=64 time=2.57 ms
64 bytes from 10.2.2.2: icmp_seq=2 ttl=64 time=2.05 ms
64 bytes from 10.2.2.2: icmp_seq=3 ttl=64 time=2.29 ms
64 bytes from 10.2.2.2: icmp_seq=4 ttl=64 time=2.07 ms
64 bytes from 10.2.2.2: icmp_seq=5 ttl=64 time=2.44 ms

--- 10.2.2.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 2.059/2.287/2.573/0.210 ms

SWITCH_A# ping -a 10.1.1.1 10.3.3.3
PING 10.3.3.3 (10.3.3.3) from 10.1.1.1 : 56(84) bytes of data.
64 bytes from 10.3.3.3: icmp_seq=1 ttl=63 time=3.32 ms
64 bytes from 10.3.3.3: icmp_seq=2 ttl=63 time=2.45 ms
64 bytes from 10.3.3.3: icmp_seq=3 ttl=63 time=2.50 ms
```

```
64 bytes from 10.3.3.3: icmp_seq=4 ttl=63 time=2.42 ms
64 bytes from 10.3.3.3: icmp_seq=5 ttl=63 time=3.49 ms

--- 10.3.3.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 2.421/2.839/3.491/0.467 ms
```

Проверьте правильность конфигурации туннелей

```
SWITCH_B# show overlay
------------------------------------------------------------------------------
--
ECMP Mode          : Normal
Source VTEP        : 10.1.1.1

Vlan Vni        Type    Remote-vtep IP-Address        Src-Address       Head-end-
flooding Protocol
------------------------------------------------------------------------------
--
10    10000        VxLAN   1            10.2.2.2      10.1.1.1      Enable
Static
20    20000        VxLAN   1            10.2.2.2      10.1.1.1      Enable
Static
20    20000        VxLAN   2            10.3.3.3      10.1.1.1      Enable
Static
SWITCH_A# show overlay uplink
------------------------------------------------------------------------------
--
Uplink port:
    eth-0-9
------------------------------------------------------------------------------
--S
```

Проверьте таблицы ARP на коммутаторе B (шлюзе)

```
SWITCH_B # show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    192.168.9.2              -   001e.081b.bce0  eth-0-9
 Internet    192.168.9.1              0   001e.080a.a7fb  eth-0-9
 Internet    192.168.17.2             -   001e.081b.bce0  eth-0-17
 Internet    192.168.17.1             0   001e.081f.13bc  eth-0-17
 Internet    192.168.10.10            0   001e.080c.46ce  vlan10(tunnel)
 Internet    192.168.20.10            0   001e.0811.05f9  vlan20(tunnel)
 Internet    192.168.10.1             -   001e.081b.bce0  vlan10
Internet    192.168.20.1             -   001e.081b.bce0  vlan20
 Internet    192.168.20.20            0   001e.080c.755e  vlan20(tunnel)
```

12.1.3 Рекомендации по развертыванию

VXLAN при подключении типа Active-Active и распределенный шлюз

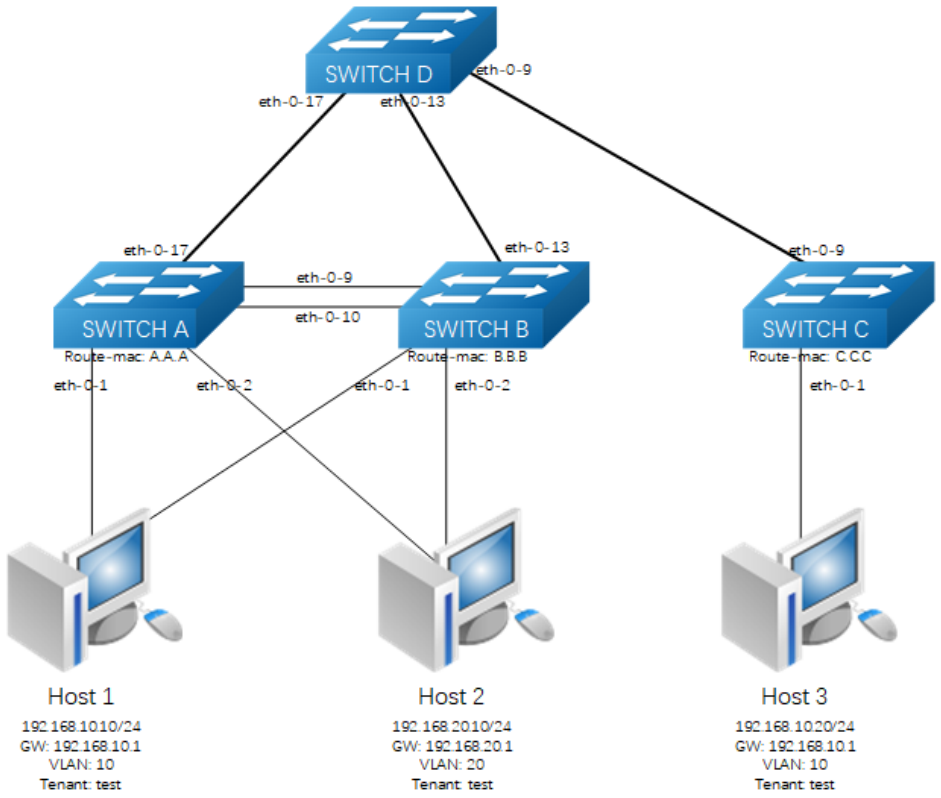


Рисунок 81 – Топология сети при режиме Active-Active и VXLAN

На схеме коммутаторы A, B и C — это коммутаторы TOR, между ними находится сеть уровня 3. Хосты находятся в тестовых участках сети, которые необходимо изолировать. Для обеспечения надежности часть хостов нуждается в активном соединении, поэтому необходимо настроить MLAG и указать виртуальный IP-адрес в качестве шлюза на коммутаторах A и B. Одновременно с этим необходимо убедиться, что адрес шлюза не изменится после миграции виртуальных машин, а затем развернуть распределенный шлюз на коммутаторах A, B и C.

Шаг 1. Настройте MLAG на коммутаторах A и B (используется для установления соединения к серверу типа актив-актив).

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A (config)# interface range eth-0-9 - 10
```

```
SWITCH_A(config-if-range)# no shutdown
SWITCH_A (config-if-range)# channel-group 55 mode active
SWITCH_A (config-if-range)# exit
SWITCH_A (config)# interface agg 55
SWITCH_A (config-if)# switchport mode trunk
SWITCH_A (config-if)# switchport trunk allowed vlan all
SWITCH_A (config-if)# spanning-tree port disable
SWITCH_A (config-if)# exit
SWITCH_A (config)# no ip igmp snooping
SWITCH_A (config)# mlag configuration
SWITCH_A (config-mlag)# peer-link agg 55
SWITCH_A (config-mlag)# end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# interface range eth-0-9 - 10
SWITCH_B(config-if-range)# no shutdown
SWITCH_B(config-if-range)# channel-group 55 mode active
SWITCH_B(config-if-range)# exit
SWITCH_B(config)# interface agg 55
SWITCH_B(config-if)# switchport mode trunk
SWITCH_B(config-if)# switchport trunk allowed vlan all
SWITCH_B(config-if)# spanning-tree port disable
SWITCH_B(config-if)# exit
SWITCH_B(config)# mlag configuration
SWITCH_B(config-mlag)# peer-link agg 55
SWITCH_B(config-mlag)# end
```

Настройка адресации peer-address

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# vlan database
SWITCH_A(config-vlan)# vlan 4094
SWITCH_A(config-vlan)# exit
SWITCH_A(config)# interface vlan 4094
SWITCH_A(config-if)# ip address 40.94.0.1/24
SWITCH_A(config-if)# exit
SWITCH_A(config)# mlag configuration
SWITCH_A(config-mlag)# peer-address 40.94.0.2
SWITCH_A(config-mlag)# end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# vlan database
vSWITCH_B(config-vlan)# vlan 4094
```

```
SWITCH_B(config-vlan)# exit
SWITCH_B(config)# interface vlan 4094
SWITCH_B(config-if)# ip address 40.94.0.2/24
SWITCH_B(config-if)# exit
SWITCH_B(config)# no ip igmp snooping
SWITCH_B(config)# mlag configuration
SWITCH_B(config-mlag)# peer-address 40.94.0.1
SWITCH_B(config-mlag)# end
```

Настройте интерфейс нисходящей связи: коммутаторы A и B используют агрегированную нисходящую связь MLAG, коммутатор C использует обычную одноканальную нисходящую связь

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# vlan database
SWITCH_A(config-vlan)# vlan 10,20,100
SWITCH_A(config-vlan)# exit
SWITCH_A(config)# interface eth-0-1
SWITCH_A(config-if)# switchport mode trunk
SWITCH_A(config-if)# switchport trunk allowed vlan add 10
SWITCH_A(config-if)# no shutdown
SWITCH_A(config-if)# static-channel-group 1
SWITCH_A(config-if)# exit
SWITCH_A(config)# interface eth-0-2
SWITCH_A(config-if)# switchport mode trunk
SWITCH_A(config-if)# switchport trunk allowed vlan add 20
SWITCH_A(config-if)# no shutdown
SWITCH_A(config-if)# static-channel-group 2
SWITCH_A(config-if)# exit
SWITCH_A(config)# interface agg 1
SWITCH_A(config-if)# mlag 1
SWITCH_A(config-if)# exit
SWITCH_A(config)# interface agg 2
SWITCH_A(config-if)# mlag 2
SWITCH_A(config-if)# end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# vlan database
SWITCH_B(config-vlan)# vlan 10,20,100
SWITCH_B(config-vlan)# exit
SWITCH_B(config)# interface eth-0-1
SWITCH_B(config-if)# switchport mode trunk
SWITCH_B(config-if)# switchport trunk allowed vlan add 10
SWITCH_B(config-if)# static-channel-group 1
SWITCH_B(config-if)# no shutdown
```

```
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface eth-0-2
SWITCH_B(config-if)# switchport mode trunk
SWITCH_B(config-if)# switchport trunk allowed vlan add 20
SWITCH_B(config-if)# static-channel-group 2
SWITCH_B(config-if)# no shutdown
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface agg 1
SWITCH_B(config-if)# mlag 1
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface agg 2
SWITCH_B(config-if)# mlag 2
SWITCH_B(config-if)# end
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# vlan database
SWITCH_C(config-vlan)# vlan 10
SWITCH_C(config-vlan)# exit
SWITCH_C(config)# interface eth-0-1
SWITCH_C(config-if)# switchport mode trunk
SWITCH_C(config-if)# switchport trunk allowed vlan add 10
SWITCH_C(config-if)# no shutdown
SWITCH_C(config-if)# end
```

Шаг 2. Настройте адрес сетевого шлюза, включите распределенный шлюз (используя виртуальный IP-адрес устройства MLAG).

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# ip vrf test
SWITCH_A(config-vrf)# exit
SWITCH_A(config)# interface vlan 10
SWITCH_A(config-if)# ip vrf forwarding test
SWITCH_A(config-if)# ip address 192.168.10.253/24
SWITCH_A(config-if)# ip virtual-router address 192.168.10.1
SWITCH_A(config-if)# overlay distributed-gateway enable
SWITCH_A(config-if)# exit
SWITCH_A(config)# interface vlan 20
SWITCH_A(config-if)# ip vrf forwarding test
SWITCH_A(config-if)# ip address 192.168.20.253/24
SWITCH_A(config-if)# ip virtual-router address 192.168.20.1
SWITCH_A(config-if)# overlay distributed-gateway enable
SWITCH_A(config-if)# exit
SWITCH_A(config)# ip virtual-router mac 0.0.1
```

```
SWITCH_A(config)# interface vlan 100
SWITCH_A(config-if)# end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# ip vrf test
SWITCH_B(config-vrf)# exit
SWITCH_B(config)# interface vlan 10
SWITCH_B(config-if)# ip vrf forwarding test
SWITCH_B(config-if)# ip address 192.168.10.254/24
SWITCH_B(config-if)# ip virtual-router address 192.168.10.1
SWITCH_B(config-if)# overlay distributed-gateway enable
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface vlan 20
SWITCH_B(config-if)# ip vrf forwarding test
SWITCH_B(config-if)# ip address 192.168.20.254/24
SWITCH_B(config-if)# ip virtual-router address 192.168.20.1
SWITCH_B(config-if)# overlay distributed-gateway enable
SWITCH_B(config-if)# exit
SWITCH_B(config)# ip virtual-router mac 0.0.1
SWITCH_B(config)# interface vlan 100
SWITCH_B(config)# end
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# ip vrf test
SWITCH_C(config-vrf)# exit
SWITCH_C(config)# interface vlan 10
SWITCH_C(config-if)# ip vrf forwarding test
SWITCH_C(config-if)# ip address 192.168.10.1/24
SWITCH_C(config-if)# overlay distributed-gateway enable
SWITCH_C(config-if)# end
```

Шаг 3. Настройка сети уровня 3 между коммутаторами.

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# interface loopback 0
SWITCH_A(config-if)# ip address 10.1.1.1/32
SWITCH_A(config-if)# exit
SWITCH_A(config)# interface eth-0-17
SWITCH_A(config-if)# no switchport
SWITCH_A(config-if)# no shutdown
SWITCH_A(config-if)# ip address 192.168.17.1/24
```

```
SWITCH_A(config-if)# exit
SWITCH_A(config)# ip route 10.3.3.3/32 192.168.17.2
SWITCH_A(config)# ip route 10.3.3.3/32 40.94.0.2 100
SWITCH_A(config)#end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# interface loopback 0
SWITCH_B(config-if)# ip address 10.1.1.1/32
SWITCH_B(config-if)# exit
SWITCH_B(config)# interface eth-0-13
SWITCH_B(config-if)# no switchport
SWITCH_B(config-if)# no shutdown
SWITCH_B(config-if)# ip address 192.168.13.1/24
SWITCH_B(config-if)# exit
SWITCH_B(config)# ip route 10.3.3.3/32 192.168.13.2
SWITCH_B(config)# ip route 10.3.3.3/32 40.94.0.1 100
SWITCH_B(config)# end
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# interface loopback 0
SWITCH_C(config-if)# ip address 10.3.3.3/32
SWITCH_C(config-if)# exit
SWITCH_C(config)# interface eth-0-9
SWITCH_C(config-if)# no shutdown
SWITCH_C(config-if)# no switchport
SWITCH_C(config-if)# ip address 192.168.9.1/24
SWITCH_C(config-if)# exit
SWITCH_C(config)# ip route 10.1.1.1/32 192.168.9.2
SWITCH_C(config)# end
```

SWITCH D

```
SWITCH_D# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_D(config)# interface eth-0-17
SWITCH_D(config-if)# no shutdown
SWITCH_D(config-if)# no switchport
SWITCH_D(config-if)# ip address 192.168.17.2/24
SWITCH_D(config-if)# exit
SWITCH_D(config)# interface eth-0-13
SWITCH_D(config-if)# no shutdown
SWITCH_D(config-if)# no switchport
SWITCH_D(config-if)# ip address 192.168.13.2/24
SWITCH_D(config-if)# exit
SWITCH_D(config)# interface eth-0-9
```

```
SWITCH_D(config-if)# no shutdown
SWITCH_D(config-if)# no switchport
SWITCH_D(config-if)# ip address 192.168.9.2/24
SWITCH_D(config-if)# exit
SWITCH_D(config)# ip route 10.1.1.1/32 192.168.17.1
SWITCH_D(config)# ip route 10.1.1.1/32 192.168.13.1
SWITCH_D(config)# ip route 10.3.3.3/32 192.168.9.1
SWITCH_D(config)# end
```

Шаг 4. Настройка туннелей VXLAN.

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# vlan database
SWITCH_A(config-vlan)# vlan 10 overlay enable
SWITCH_A(config-vlan)# vlan 100 overlay enable
SWITCH_A(config-vlan)# exit
SWITCH_A(config)# overlay
SWITCH_A(config-overlay)# source 10.1.1.1
SWITCH_A(config-overlay)# remote-vtep 1 ip-address 10.3.3.3 type vxlan
SWITCH_A(config-overlay)# vlan 10 vni 10000
SWITCH_A(config-overlay)# vlan 10 remote-vtep 1
SWITCH_A(config-overlay)# vlan 100 vni 100
SWITCH_A(config-overlay)# vlan 100 remote-vtep 1
SWITCH_A(config-overlay)# exit
SWITCH_A(config)# interface eth-0-17
SWITCH_A(config-if)# vxlan uplink enable
SWITCH_A(config-if)# end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# vlan database SWITCH_B(config-vlan)# vlan 10 overlay enable
SWITCH_B(config-vlan)# vlan 100 overlay enable
SWITCH_B(config-vlan)# exit
SWITCH_B(config)# overlay
SWITCH_B(config-overlay)# source 10.1.1.1
SWITCH_B(config-overlay)# remote-vtep 1 ip-address 10.3.3.3 type vxlan
SWITCH_B(config-overlay)# vlan 10 vni 10000
SWITCH_B(config-overlay)# vlan 10 remote-vtep 1
SWITCH_B(config-overlay)# vlan 100 vni 100
SWITCH_B(config-overlay)# vlan 100 remote-vtep 1
SWITCH_B(config-overlay)# exit
SWITCH_B(config)# interface eth-0-13
SWITCH_B(config-if)# vxlan uplink enable
SWITCH_B(config-if)# end
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# vlan database
SWITCH_C(config-vlan)# vlan 10,100
SWITCH_C(config-vlan)# vlan 10 overlay enable
SWITCH_C(config-vlan)# vlan 100 overlay enable
SWITCH_C(config-vlan)# exit
SWITCH_C(config)# overlay
sSWITCH_C(config-overlay)# source 10.3.3.3
SWITCH_C(config-overlay)# remote-vtep 1 ip-address 10.1.1.1 type vxlan
SWITCH_C(config-overlay)# vlan 10 vni 10000
SWITCH_C(config-overlay)# vlan 10 remote-vtep 1
SWITCH_C(config-overlay)# vlan 100 vni 100
SWITCH_C(config-overlay)# vlan 100 remote-vtep 1
SWITCH_C(config-overlay)# exit
SWITCH_C(config)# interface eth-0-9
SWITCH_C(config-if)# vxlan uplink enable
SWITCH_C(config-if)# end
```

Шаг 5. Настройте маршрутизацию DVR, обеспечьте взаимосвязность коммутаторов и хостов из разных сегментов.

SWITCH A

```
SWITCH_A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_A(config)# ip route vrf test 192.168.10.20/32 remote-vtep 1 vni 100
inner-macda c.c.c
SWITCH_A(config)# end
```

SWITCH B

```
SWITCH_B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_B(config)# ip route vrf test 192.168.10.20/32 remote-vtep 1 vni 100
inner-macda c.c.c
SWITCH_B(config)# end
```

SWITCH C

```
SWITCH_C# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH_C(config)# ip route vrf test 192.168.20.10/32 remote-vtep 1 vni 100
inner-macda 0.0.1
SWITCH_C(config)# end
```

Шаг 6. Проверка.

Проверьте статус MLAG

```
SWITCH_A# show mlag peer
MLAG neighbor is 40.94.0.2, MLAG version 1
MLAG state = Established, up for 23:41:26
Last read 00:00:42, hold time is 240, keepalive interval is 60 seconds
Received 1652 messages,Sent 1654 messages
Open      : received 1, sent 2
KAlive    : received 1646, sent 1646
Fdb sync  : received 0, sent 0
Failover  : received 0, sent 0
Conf      : received 2, sent 2
Syspri    : received 1, sent 1
Peer fdb  : received 15, sent 15
STP Total: received 2, sent 3
 Global   : received 2, sent 3
 Packet   : received 0, sent 0
 Instance: received 0, sent 0
 State    : received 0, sent 0

Connections established 1; dropped 0
Local host: 40.94.0.1, Local port: 61000
Foreign host: 40.94.0.2, Foreign port: 42371
remote_sysid: 06a8.c402.0300
```

Проверьте состояние нисходящего интерфейса MLAG

```
SWITCH_A# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up
2       agg2      up             up
```

Проверьте состояние VXLAN

```
SWITCH_A# show overlay
-------------------------------------------------------------
ECMP Mode         : Normal
Source VTEP       : 10.1.1.1

Vlan Vni         Type   Remote-vtep IP-Address
-------------------------------------------------------------
10   10000       VxLAN  1           10.3.3.3
100   100       VxLAN  1           10.3.3.3
```

Проверьте состояние маршрутов DVR

```
SWITCH_A# show ip route vrf test
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       Dc - DHCP Client
       [*] - [AD/Metric]
       * - candidate default

C        192.168.10.0/24 is directly connected, vlan10
C        192.168.10.253/32 is in local loopback, vlan10
C        192.168.10.1/32 is directly connected, vlan10
S        192.168.10.20/32 is in overlay remote vxlan vtep:10.3.3.3, vni:100
C        192.168.20.0/24 is directly connected, vlan20
C        192.168.20.253/32 is in local loopback, vlan20
C        192.168.20.1/32 is directly connected, vlan20
```

12.2 Настройка GENEVE

12.2.1 Общие положения

12.2.1.1 Описание функции

Generic Network Virtualization Encapsulation (GENEVE) — это сетевая технология, которая инкапсулирует кадры Ethernet уровня 2 на основе MAC-адресов в пакеты UDP уровня 3 для объединения и туннелирования нескольких сетей уровня 2 через инфраструктуру уровня 3. GENEVE масштабируется до 16 миллионов логических сетей и поддерживает смежность уровня 2 в IP-сетях. Для широковещательных/многоадресных/неизвестных пакетов используется архитектура многоадресной передачи.

12.2.2 Настройка

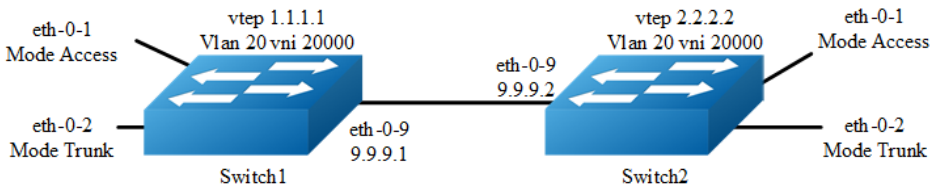


Рисунок 82 – Топология GENEVE туннеля

В следующем примере коммутаторы Switch1 и Switch2 соединены маршрутом уровня 3. Трафик VLAN 20 инкапсулируется в VNI 20000 для прохождения через сети уровня 3.

Если идентификатор коммутатора не указан, на всех коммутаторах топологии следует выполнить следующие действия по настройке.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN, включив Overlay для каждого VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 20
Switch(config-vlan)# vlan 20 overlay enable
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Конфигурация интерфейса для коммутатора Switch1:

```
Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.1/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 1.1.1.1/32
Switch(config-if)# exit
```

Конфигурация интерфейса для коммутатора Switch2:

```
Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.2/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 2.2.2.2/32
```

```
Switch(config-if)# exit
```

Шаг 4. Создайте статический маршрут.

Настройка коммутатора Switch1:

```
Switch(config)# ip route 2.2.2.0/24 9.9.9.2
```

Настройка коммутатора Switch2:

```
Switch(config)# ip route 1.1.1.0/24 9.9.9.1
```

Шаг 5. Настройка атрибутов Overlay.

Настройка коммутатора Switch1:

```
Switch(config)# overlay
Switch(config-overlay)# source 1.1.1.1
Switch(config-overlay)# remote-vtep 1 ip-address 2.2.2.2 type geneve
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# exit
```

Настройка коммутатора Switch2:

```
Switch(config)# overlay
Switch(config-overlay)# source 2.2.2.2
Switch(config-overlay)# remote-vtep 1 ip-address 1.1.1.1 type geneve
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Switch1:

```
Switch# show overlay vlan 20
------------------------------------------------------------------------------
--
ECMP Mode         : Normal
Source VTEP       : 1.1.1.1
------------------------------------------------------------------------------
--
VLAN ID                         : 20
VNI                             : 20000
EVPN Tunnel Data-fdb Learning : Eanble
Remote VTEP NUM: 1
```

```
          Index: 1, Ip address: 2.2.2.2, Source ip: 1.1.1.1, Type: GENEVE,
Protocol: Static
DVR Gateway NUM: 0
-------------------------------------------------------------------------
```

Switch2:

```
Switch# show overlay vlan 20
-------------------------------------------------------------------------------
--
ECMP Mode         : Normal
Source VTEP       : 2.2.2.2
-------------------------------------------------------------------------------
--
VLAN ID                          : 20
VNI                              : 20000
EVPN Tunnel Data-fdb Learning    : Enable
Remote VTEP NUM: 1
          Index: 1, Ip address: 1.1.1.1, Source ip: 2.2.2.2, Type: GENEVE,
Protocol: Static
DVR Gateway NUM: 0
-------------------------------------------------------------------------
```

12.2.2.1 Настройка маршрутизации GENEVE

VM-1 и VM-3 инкапсулированы в один и тот же VNI для формирования распределенного маршрута через GENEVE; VM-2 и VM-4 инкапсулированы в другой VNI для формирования распределенного маршрута GENEVE.

Если идентификатор коммутатора не указан, на всех коммутаторах топологии следует выполнить следующие действия по настройке.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN, включив Overlay для каждого VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 20,30
Switch(config-vlan)# vlan 20 overlay enable
Switch(config-vlan)# vlan 30 overlay enable
Switch(config-vlan)# exit
```

Шаг 3. Создайте экземпляр VRF.

```
Switch(config)# ip vrf tenant
Switch(config-vrf)# exit
```

Шаг 4. Создайте интерфейс уровня 3 и задайте IP-адрес.

Настройка коммутатора Switch1:

```
Switch(config)# interface vlan 20
Switch(config-if)# ip vrf forwarding tenant
Switch(config-if)# ip address 2.2.2.111/24
Switch(config-if)# exit

Switch(config)# interface vlan 30
Switch(config-if)# ip vrf forwarding tenant
Switch(config-if)# ip address 3.3.3.111/24
Switch(config-if)# exit
```

Настройка коммутатора Switch2:

```
Switch(config)# interface vlan 20
Switch(config-if)# ip vrf forwarding tenant
Switch(config-if)# ip address 2.2.2.222/24
Switch(config-if)# exit

Switch(config)# interface vlan 30
Switch(config-if)# ip vrf forwarding tenant
Switch(config-if)# ip address 3.3.3.222/24
Switch(config-if)# exit
```

Шаг 5. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add  30
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Switch1:

```
Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.1/24
```

```
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 1.1.1.1/32
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.2/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 2.2.2.2/32
Switch(config-if)# exit
```

Шаг 6. Настройка атрибутов Overlay.

Switch1:

```
Switch(config)# overlay
Switch(config-overlay)# source 1.1.1.1
Switch(config-overlay)# remote-vtep 1 ip-address 2.2.2.2 type geneve
Switch(config-overlay)# remote-vtep 1 virtual-mac 22.22.22
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 30 vni 30000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# vlan 30 remote-vtep 1
Switch(config-overlay)# vlan 20 gateway-mac a.a.a
Switch(config-overlay)# vlan 30 gateway-mac b.b.b
Switch(config-overlay)# exit
```

Switch2:

```
Switch(config)# overlay
Switch(config-overlay)# source 2.2.2.2
Switch(config-overlay)# remote-vtep 1 ip-address 1.1.1.1 type geneve
Switch(config-overlay)# remote-vtep 1 virtual-mac 11.11.11
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 30 vni 30000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# vlan 20 gateway-mac a.a.a
Switch(config-overlay)# vlan 30 gateway-mac b.b.b
Switch(config-overlay)# exit
```

Шаг 7. Создайте статические маршруты и маршруты GENEVE.

Switch1:

```
Switch(config)# ip route 2.2.2.0/24 9.9.9.2
Switch(config)# ip route vrf tenant 2.2.2.2/32 remote-vtep 1 vni 20000 inner-
macda 3.3.3
Switch(config)# ip route vrf tenant 3.3.3.2/32 remote-vtep 1 vni 30000 inner-
macda 4.4.4
```

Switch2:

```
Switch(config)# ip route 1.1.1.0/24 9.9.9.1
Switch(config)# ip route vrf tenant 2.2.2.1/32 remote-vtep 1 vni 20000 inner-
macda 1.1.1
Switch(config)# ip route vrf tenant 3.3.3.1/32 remote-vtep 1 vni 30000
```

Шаг 8. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 9. Проверка.

Switch1:

```
switch# show ip route vrf tenant
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       Dc - DHCP Client
       [*] - [AD/Metric]
       * - candidate default
S        2.2.2.2/32 is in overlay remote geneve vtep:1.1.1.1->2.2.2.2,
vni:20000
S        3.3.3.2/32 is in overlay remote geneve vtep:1.1.1.1->2.2.2.2,
vni:30000
```

Switch2:

```
switch# show ip route vrf tenant
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
```

```
       Dc - DHCP Client
       [*] - [AD/Metric]
       * - candidate default
S        2.2.2.1/32 is in overlay remote geneve vtep:2.2.2.2->1.1.1.1,
vni:20000
S        3.3.3.1/32 is in overlay remote geneve vtep:2.2.2.2->1.1.1.1,
vni:30000
```

12.3 Настройка Overlay

12.3.1 Общие положения

12.3.1.1 Описание функции

Функция оверлея поддерживает несколько IP-адресов источника для VTEP, что позволяет при необходимости устанавливать разные IP-адреса источника для разных сетей. Функция оверлея поддерживает туннелирование без включения опции Split-horizon. Таким образом порт исходящего канала связи принимает туннельные пакеты и декапсулирует их, а затем отправляет их в другой туннель для инкапсуляции.

12.3.2 Настройка

12.3.2.1 Overlay и несколько IP-адресов источника

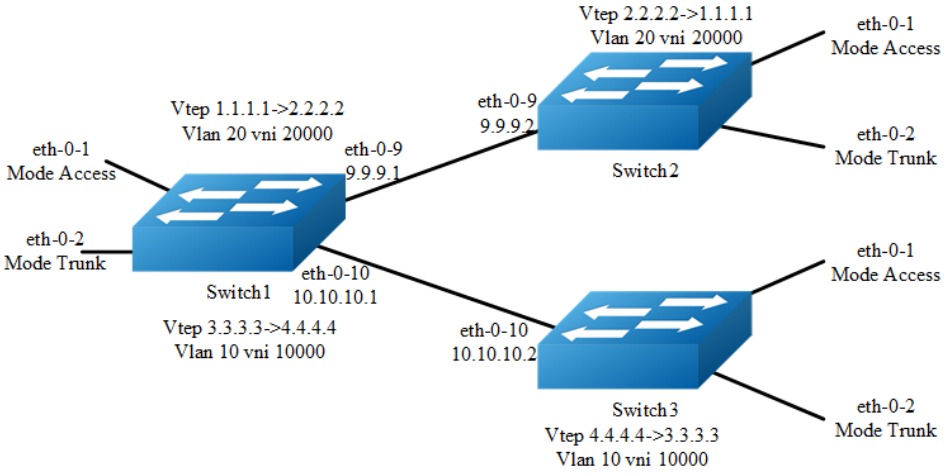


Рисунок 83 – Топология Overlay и несколько IP-адресов источника

В следующем примере для настройки оверлей используется VXLAN. Конфигурации NVGRE и GENEVE аналогичны при использовании VXLAN.

Если идентификатор коммутатора не указан, на всех коммутаторах топологии следует выполнить следующие действия по настройке.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN, включив Overlay для каждого VLAN.

Switch1:

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 20,10
Switch(config-vlan)# vlan 20 overlay enable
Switch(config-vlan)# vlan 10 overlay enable
Switch(config-vlan)# exit
```

Switch2:

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 20
Switch(config-vlan)# vlan 20 overlay enable
Switch(config-vlan)# exit
```

Switch3:

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# vlan 10 overlay enable
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.1/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

```
Switch(config)# interface eth-0-10
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 1.1.1.1/32
Switch(config)# interface loopback1
Switch(config-if)# ip address 3.3.3.3/32
Switch(config-if)# exit
```

Switch2:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.2/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 2.2.2.2/32
Switch(config-if)# exit
```

Switch3:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10
Switch(config-if)# no shutdown
```

```
Switch(config-if)# exit

Switch(config)# interface eth-0-10
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.2/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 4.4.4.4/32
Switch(config-if)# exit
```

Шаг 4. Создайте статические маршруты.

Настройка Switch1:

```
Switch(config)# ip route 2.2.2.0/24 9.9.9.2
Switch(config)# ip route 4.4.4.0/24 10.10.10.2
```

Настройка Switch2:

```
Switch(config)# ip route 1.1.1.0/24 9.9.9.1
```

Настройка Switch3:

```
Switch(config)# ip route 3.3.3.0/24 10.10.10.1
```

Шаг 5. Настройка атрибутов Overlay.

Switch1:

```
Switch(config)# overlay
Switch(config-overlay)# source 1.1.1.1
Switch(config-overlay)# remote-vtep 1 ip-address 2.2.2.2 type vxlan
Switch(config-overlay)# remote-vtep 2 ip-address 4.4.4.4 type vxlan src-ip
3.3.3.3
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 10 vni 10000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# vlan 10 remote-vtep 2
Switch(config-overlay)# exit
```

Switch2:

```
Switch(config)# overlay
Switch(config-overlay)# source 2.2.2.2
Switch(config-overlay)# remote-vtep 1 ip-address 1.1.1.1 type vxlan
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# exit
```

Switch3:

```
Switch(config)# overlay
Switch(config-overlay)# source 4.4.4.4
Switch(config-overlay)# remote-vtep 1 ip-address 3.3.3.3 type vxlan
Switch(config-overlay)# vlan 10 vni 10000
Switch(config-overlay)# vlan 10 remote-vtep 1
Switch(config-overlay)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Switch1:

```
switch# show overlay vlan 20
------------------------------------------------------------
ECMP Mode         : Normal
Source VTEP       : 1.1.1.1
------------------------------------------------------------
VLAN ID                         : 2
VNI                             : 20000
EVPN Tunnel Data-fdb Learning : Eanble
Remote VTEP NUM: 1
          Index: 1, Ip address: 2.2.2.2, Source ip: 1.1.1.1, Type: VxLAN,
Protocol: Static
          Index: 2, Ip address: 2.2.2.2, Source ip: 3.3.3.3, Type: VxLAN,
Protocol: Static
DVR Gateway NUM: 0
------------------------------------------------------------
```

12.3.2.2 Настройка Overlay без использования Horizon-Split

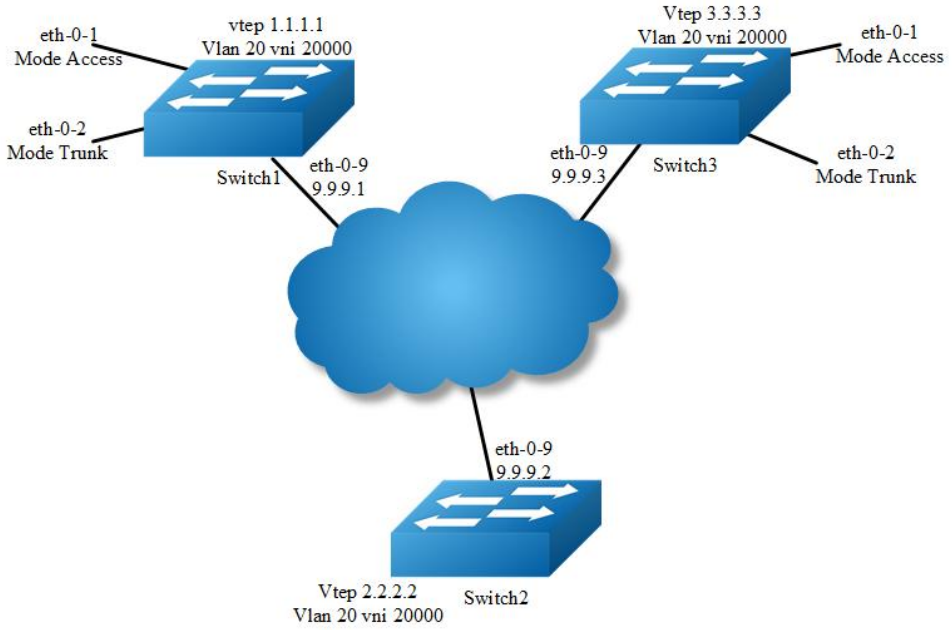


Рисунок 84 – Топология Overlay без использования опции Horizon Split

В следующем примере между коммутаторами Switch1 и Switch2 существует туннель, и ещё один туннель настроен между Switch2 и Switch3. На Switch2 отключено разделение горизонта, поэтому пакеты из одного туннеля могут перенаправляться в другой туннель.

В следующем примере для настройки оверлей используется VXLAN. Конфигурации NVGRE и GENEVE аналогичны при использовании VXLAN.

Если идентификатор коммутатора не указан, на всех коммутаторах топологии следует выполнить следующие действия по настройке.

Шаг 1. Войдите в режим настройки.

```
Switch# configure terminal
```

Шаг 2. Войдите в режим настройки VLAN и создайте VLAN, включив Overlay для каждого VLAN.

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 20
Switch(config-vlan)# vlan 20 overlay enable
Switch(config-vlan)# exit
```

Шаг 3. Войдите в режим настройки интерфейса и задайте атрибуты интерфейса.

Switch1:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.1/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 1.1.1.1/32
Switch(config-if)# exit
```

Switch2:

```
Switch(config-if)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# ip address 9.9.9.2/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 2.2.2.2/32
Switch(config-if)# exit
```

Switch3:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 20
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip address 9.9.9.3/24
Switch(config-if)# overlay uplink enable
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface loopback0
Switch(config-if)# ip address 3.3.3.3/32
Switch(config-if)# exit
```

Шаг 4. Создайте статический маршрут.

Настройка Switch1:

```
Switch(config)# ip route 2.2.2.0/24 9.9.9.2
```

Настройка Switch2:

```
Switch(config)# ip route 1.1.1.0/24 9.9.9.1
Switch(config)# ip route 3.3.3.3/24 9.9.9.3
```

Настройка Switch3:

```
Switch(config)# ip route 2.2.2.0/24 9.9.9.2
```

Шаг 5. Настройка атрибутов Overlay.

Switch1:

```
Switch(config)# overlay
Switch(config-overlay)# source 1.1.1.1
Switch(config-overlay)# remote-vtep 1 ip-address 2.2.2.2 type vxlan
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# exit
```

Switch2:

```
Switch(config)# overlay
Switch(config-overlay)# source 2.2.2.2
Switch(config-overlay)# remote-vtep 1 ip-address 1.1.1.1 type vxlan horizon-
split-disable
Switch(config-overlay)# remote-vtep 2 ip-address 3.3.3.3 type vxlan horizon-
split-disable
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# vlan 20 remote-vtep 2
Switch(config-overlay)# exit
```

Switch3:

```
Switch(config)# overlay
Switch(config-overlay)# source 3.3.3.3
Switch(config-overlay)# remote-vtep 1 ip-address 2.2.2.2 type vxlan
```

```
Switch(config-overlay)# vlan 20 vni 20000
Switch(config-overlay)# vlan 20 remote-vtep 1
Switch(config-overlay)# exit
```

Шаг 6. Выйдите из режима настройки.

```
Switch(config)# end
```

Шаг 7. Проверка.

Switch2:

```
switch# show overlay remote-vtep
Index Type   Virtual-Mac    IP-Address  Source-Ip   Split-Horizon Keep-vtag
Dscp-strategy
-------------------------------------------------------------------------------
--------------
1     VxLAN        -        1.1.1.1     2.2.2.2      Disable        Disable
Dscp-copy

2     VxLAN        -        3.3.3.3     2.2.2.2      Disable        Disable
Dscp-copy
```