Зелакс ММ

Краткое руководство по настройке
ММ-41xx

Редакция 04 от 18.04.2024 г.

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

Оглавление

1 Введение

Настоящее руководство предназначено для ознакомления пользователей с основными принципами настройки маршрутизатора ММ-41xx (далее — устройство), а также для пояснения использования основных команд настройки устройства.

Технические параметры устройства приведены в техническом описании.

2 Интерфейс пользователя и режимы работы

Интерфейс пользователя основан на использовании командной строки (CLI — Command Line Interface). Пользователь вводит команду в виде последовательности символов в командной строке, расположенной в нижней части экрана терминала. Результаты выполнения команды выводятся в оставшуюся часть экрана, при этом текст сообщений сдвигается снизу (от командной строки) вверх по мере его поступления.

Для разграничения прав доступа к командам управления существуют два режима:

- пользовательский режим, при котором разрешён доступ к командам мониторинга. В этом режиме нельзя изменять конфигурацию изделия;
- привилегированный режим, при котором разрешён доступ к командам мониторинга и изменения конфигурации изделия.

В Табл. 1 приведены основные режимы управления, команды входа и выхода из них и состояние командной строки.

Табл. 1 — Режимы управления

Режим	Вход осуществляется	Вид командной строки	Описание	Выход из режима выполняется
Пользовательский	Нажатием клавиши “Enter”	router>	Доступны команды мониторинга	Командой exit
Привилегированный	Из пользовательского режима выполнением команды enable	router#	Доступны команды мониторинга и служебные операции, такие как перезагрузка и сброс к заводским настройкам	Командой exit
Конфигурирования общесистемных параметров	Из привилегированного режима выполнением команды configure terminal	router(config)#	Доступны команды настройки общесистемных параметров	Командой exit
Конфигурирования интерфейсов	Из режима конфигурирования общесистемных параметров выполнением команды interface с указанием типа и номера интерфейса	router(config-if)#	Доступны команды настройки параметров интерфейсов	Командой exit
Настройки пула адресов DHCP	Из режима конфигурирования общесистемных параметров выполнением команды ip dhcp pool <name>	router(dhcp-config)#	Доступны команды настройки параметров пула dhcp	Командой exit
Настройки списков доступа	Из режима конфигурирования общесистемных параметров выполнением команды ip access-list {standard | extended} <name>	router(config-std-nacl)# или router(config-ext-nacl)#	Доступны команды настройки параметров стандартных и расширенных списков доступа	Командой exit
Настройки параметров протокола маршрутизации (на примере протокола RIP)	Из режима конфигурирования общесистемных параметров выполнением команды router rip | router ipv6 rip	router(config-rip)#	Доступны команды настройки параметров протокола маршрутизации	Командой exit

2.1 Синтаксис команд

Синтаксис команд, вводимых в командной стоке:

команда <переменная> { параметр | … | параметр } [параметр]

где:

Команда — строго заданная последовательность символов, определяющая дальнейшие параметры.

Параметр — ключевое слово, IP-адрес, маска сети, IP-адрес с маской, MAC-адрес, число, слово, строка.

Команда и параметры отделяются друг от друга пробелами.

При описании синтаксиса команд используются следующие обозначения:
- в фигурных скобках {} указываются обязательные параметры;
- в квадратных скобках [] указываются необязательные параметры;
- символ “|” обозначает логическое “или” — выбор между различными параметрами.

Для исполнения набранной команды необходимо нажать клавишу “Enter”.

Для получения контекстной справки используется символ “?”.

При нажатии клавиши табуляции “Tab” происходит автоматическое дополнение сокращенных названий команд и некоторых типов параметров до их полного вида, или, в случае, когда несколько команд начинаются с одинаковых символов, до их общей части.

Последние десять введенных команд хранятся в буфере. Чтобы воспользоваться ранее введенной командой, необходимо нажать клавишу “↑” (вверх) или “↓” (вниз).

2.2 Контекстная справка

Для получения контекстной справки используется символ “?”. Данная операция доступна во всех режимах.

При вводе символа “?” выводится список команд, доступных в данном режиме.

Пример. Использование контекстной справки для получения списка команд, доступных в пользовательском режиме:

```
router>?
    clear                Command clear
    debug                Command debug
    disable              Turn off privileged commands
    enable               Turn on privileged commands mode
    exit                 Exit from current EXEC mode
    groupping            Send echo messages
    help                 Description of the interactive help system
    logout               Exit from EXEC shell
    no                   Command no
    ping                 Send echo messages
    show                 Command show
    telnet               Open a telnet connection
    test                 Command test
    tracepath            Trace path to destination
    traceroute           Trace route to destination
    who                  Show who is logged on
    whoami               Who am i
```

При вводе символа “?” через пробел после команды, выводится список параметров данной команды.

Пример. Использование контекстной справки для получения списка параметров команды copy:

```
router#copy ?
    file-system          Copy from file system
    ftp                  Copy from ftp: file system
    ftps                 Copy from ftps: file system
    running-config       Copy from running configuration
    sftp                 Copy from sftp: file system
    startup-config       Copy from startup configuration
    tftp                 Copy from tftp: file system
```

2.3 Сообщения об ошибках

В Табл. 2 приведены сообщения об ошибках, которые могут выводиться во время работы с командной строкой.

Табл. 2 — Сообщения об ошибках при работе с командной строкой

Сообщение об ошибке	Описание ошибки
% Unknown command	Команда не распознана
Type " ?" for a list of subcommands	Команда была распознана, но при вводе команды не были указаны все необходимые параметры
% Invalid input detected at '^' marker	Введенная команда или оператор, начинающийся со знака '^', не существует, введен с ошибками или введен не в соответствующем режиме управления

3 Обозначения

3.1 Обозначение типов портов

Порты маршрутизаторов MM-41xx могут иметь следующие типы:

- WAN-порт (L3);
- LAN-порт (L2);
- WAN/LAN-порт (L3/L2).

WAN/LAN-порты могут работать в двух режимах:

- WAN/LAN-порт в режиме WAN (L3);
- WAN/LAN-порт в режиме LAN (L2).

Информация о типах портов, поддерживаемых на модификациях маршрутизаторов MM-41xx, содержится в техническом описании.

Описание метода обозначения типа портов в последующих разделах настоящего руководства приведено в Табл. 3.

Табл. 3 — Обозначения типов портов

Обозначение типа порта в настоящем руководстве	Типы портов, к которым применяется указанное обозначение
WAN-порт	WAN-порт или WAN/LAN-порт в режиме WAN, если не указано иначе в описании функции
LAN-порт	LAN-порт или WAN/LAN-порт в режиме LAN, если не указано иначе в описании функции
WAN/LAN-порт в режиме LAN	WAN/LAN-порт в режиме LAN
WAN/LAN-порт в режиме WAN	WAN/LAN-порт в режиме WAN

3.2 Обозначение доступности функций

В каждом разделе настоящего руководства, описывающем настройку определенной функции, указана информация о том, на каких модификация маршрутизаторов MM-41xx доступна эта функция. В случае, если в разделе нет указаний о том, на каких модификациях доступна функция, то эта функция доступна на всех модификациях маршрутизаторов MM-41xx.

4 Базовые параметры

4.1 Текущая конфигурация и версия устройства

Отображение текущей конфигурации устройства:

```
router#sh run
Building Configuration...
done

! Current configuration : 862 bytes
!
! No configuration change since last restart
! Configuration version 0.0
!

!software version 8.11.32.70
!software image file flash0: /flash/rp37-g-8.11.32.70(R).pck
!compiled on Jun 18 2023, 14:24:12




role audit-admin
 exit
role network-admin
 exit
role network-operator
 exit
role security-admin
 exit


edp enable

ip load-sharing per-destination
ipv6 load-sharing per-destination




domain system
 exit



vlan 1
 exit



!slot_0_2_5GE
interface gigabitethernet0/0
 exit
interface gigabitethernet0/1
 exit
interface gigabitethernet0/2
 exit
interface gigabitethernet0/3
 exit
interface gigabitethernet0/4
 exit
!end




!slot_0_1_1GE

interface gigabitethernet0
 media-type auto
 exit

!end
```

```
interface null0
 exit




!chassis config

!chassis end

!end
```

Текущая версия программного обеспечения и аппаратная ревизия устройства:

```
router##show version
               Zelax Operating System Software
MM-4122 system image file (flash0: /flash/rp37-g-8.11.32.70(R).pck), version 8.11.32.70, Compiled on
Jun 18 2023, 14:24:12
Copyright (C) 2022 Zelax

MM-4122 Version Information
        System ID           : 001a81020975
        Hardware Model      : MM-4122(E1) with 512 MBytes SDRAM, 128 MBytes flash
        Hardware Version    : 1(Hotswap Unsupported)
        Bootloader Version  : 1.0.8.02
        Software Version    : 8.11.32.70
        Software Image File : flash0: /flash/rp37-g-8.11.32.70(R).pck
        Compiled            : Jun 18 2023, 14:24:12

Local MPU Uptime is 2 days 2 hours
System Uptime is 2 days 2 hours
```

4.2 Имя устройства

Настройка имени устройства:

```
router(config)#hostname Zelax
```

5 Функции управления

5.1 Учетные записи

Создание учетной записи для доступа к маршрутизатору с незашифрованным паролем и уровнем привилегий 15. Пароль не должен совпадать с именем пользователя. Пароль должен содержать буквы и цифры, при этом количество символов должно быть не менее 6:

```
router(config)#local-user zelax class manager
router(config-user-manager-zelax)#password 0 password123
```

Включение доступа к маршрутизатору по протоколу telnet:

```
router(config-user-manager-zelax)#service-type telnet
router(config-user-manager-zelax)#exit
router(config)#line vty 0 15
router(config-line)#login aaa default
router(config-line)#exit
router(config)#enable password password123
```

5.2 SSH

По умолчанию доступ к маршрутизатору по протоколу SSH выключен. Включение доступа к маршрутизатору по протоколу SSH:

```
router(config)#ip ssh server
```

5.3 SNMPv2

Настройка доступа к маршрутизатору по протоколу SNMP v2c.

Включение SNMP-сервера:

```
router(config)#snmp-server start
router(config)#snmp-server view default 1.3.6.1 include
```

Задание значений community для доступа на чтение и запись:

```
router(config)#snmp-server community public1 ro
router(config)#snmp-server community private1 rw
```

Разрешение отправки TRAP-сообщений, указание IP-адреса назначения и соответствующего SNMP-Community:

```
router(config)#snmp-server enable traps
router(config)#snmp-server host 192.168.135.254 traps community public1 version 2
```

Результирующий пример минимально необходимых настроек протокола SNMP:

```
router(config)#snmp-server start
router(config)#snmp-server community public1 ro
router(config)#snmp-server community private1 rw
router(config)#snmp-server enable traps
router(config)#snmp-server host 192.168.135.254 traps community public1 version 2
```

5.4 SNMPv3

Пример настройки протокола SNMPv3 с аутентификацией и шифрованием (AuthPriv):

```
router(config)#snmp-server start
router(config)#snmp-server view default 1.3.6.1 include
router(config)#snmp-server group public v3 authpriv read default write default notify default
router(config)#snmp-server user public public v3 auth md5 admin123 encrypt des admin123
router(config)#snmp-server enable traps
router(config)#snmp-server host 192.168.0.254 traps user public authpriv version 3
```

6 Функции 2-го уровня

6.1 Переключение режима порта WAN/LAN

Функция доступна в модификациях MM-4122, MM-4102. Команды доступны на WAN/LAN-портах.

Перевод порта из режима WAN в режим LAN:

```
router(config-if-gigabitethernet0/0)#switchport
```

Перевод порта из режима LAN в режим WAN:

```
router(config-if-gigabitethernet0/0)#no switchport
```

6.2 Bridging

Команды доступны на WAN-портах (во всех модификациях) и на интерфейсах VLAN (в модификациях MM-4122, MM-4102 и MM-4112).

Объединение L3 интерфейсов в группу bridge-group позволяет прозрачно пересылать кадры Ethernet между разными WAN-портами в пределах одной группы.

Добавление WAN-портов в bridge-group 1:

```
router(config)#interface gigabitethernet 0
router(config-if-gigabitethernet0)#bridge-group 1
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#bridge-group 1
```

6.3 VLAN

Функция доступна в модификациях MM-4122, MM-4102 и MM-4112. Команды доступны на LAN-портах.

6.3.1 Access

Перевод порта в режим access:

```
router(config-if-gigabitethernet0/0)#switchport mode access
```

Изменение VLAN, к которому принадлежит порт:

```
router(config-if-gigabitethernet0/0)#switchport access vlan 10
```

6.3.2 Trunk

Перевод порта в режим trunk:

```
router(config-if-gigabitethernet0/0)#switchport mode trunk
```

При переводе порта в этот режим, на порту разрешается передача VLAN 1. Для добавления разрешенных к передаче VLAN необходимо использовать следующую команду:

```
router(config-if-gigabitethernet0/0)#switchport trunk allowed vlan add 10,20-30,100
```

По умолчанию все нетегированные кадры, входящие на устройство через этот порт, тегируются меткой VLAN 1 (Native VLAN). Для изменения Native VLAN нужно использовать команду:

```
router(config-if-gigabitethernet0/0)#switchport trunk pvid vlan 50
```

6.4 xSTP

Функция доступна в модификациях MM-4122, MM-4102 и MM-4112.

6.4.1 Выбор протокола xSTP

Включение протокола связующего дерева:

```
router(config)#spanning-tree enable
```

После ввода данной команды по умолчанию включается протокол MSTP. Выбранный протокол связующего дерева можно изменить. Встроенный коммутатор поддерживает ряд протоколов связующего дерева:

```
router(config)#spanning-tree mode mstp|rstp|stp
```

6.4.2 Настройка instance в MSTP

На встроенном коммутаторе созданы VLAN 10,20-30. VLAN 10 помещен в Instance 1, а VLAN 20-30 помещены в Instance 2:

```
router(config)#spanning-tree mst configuration
router(config-mst)#instance 1 vlan 10
router(config-mst)#instance 2 vlan 20-30
router(config-mst)#active configuration pending
```

6.4.3 Настройка таймеров MSTP

Настройка Hello-интервала:

```
router(config)#spanning-tree mst hello-time 5
```

Настройка таймера Max Age:

```
router(config)#spanning-tree mst max-age 15
```

Настройка таймера Forward Delay:

```
router(config)#spanning-tree mst forward-time 10
```

6.4.4 Настройка приоритета MSTP

Настройка приоритета коммутатора для Instance 0 в протоколе MSTP:

```
router(config)#spanning-tree mst instance 0 priority 4096
```

6.4.5 Настройка стоимости интерфейсов MSTP

Команда доступна на LAN-портах.

Изменение стоимости интерфейса gigabitethernet0/0 в протоколе MSTP:

```
router(config-if-gigabitethernet0/0)#spanning-tree mst instance 0 cost 2000
```

6.4.6 BPDU guard

Команда доступна на LAN-портах.

Настройка функции BPDU guard на интерфейсе gigabitethernet0/0:

```
router(config-if-gigabitethernet0/0)#spanning-tree bpdu guard
```

6.4.7 Root guard

Команда доступна на LAN-портах.

Включение Root guard на интерфейсе gigabitethernet0/0:

```
router(config-if-gigabitethernet0/0)#spanning-tree guard root
```

6.5 Агрегирование каналов L2

Функция доступна в модификациях MM-4122, MM-4102 и MM-4112.

6.5.1 Создание группы агрегирования каналов

Создание группы агрегирования каналов в глобальном режиме конфигурации с выбором режима работы LACP или без протокола согласования:

```
router(config)#link-aggregation 1 mode lacp|manual
```

6.5.2 Без протоколов согласования

Команда доступна на LAN-портах.

Данную настройку нужно производить с обеих сторон канала для исключения возможности возникновения петли:

```
router(config)#interface gigabitethernet 0/2,0/3
router(config-if-range)#link-aggregation 1 manual
```

6.5.3 LACP

Команды доступны на LAN-портах.

При использовании протокола LACP, порты на одной стороне канала переводятся в режим активного согласования параметров, а на другой стороне канала — в режим пассивного согласования параметров.

LAN-порты локального маршрутизатора переводятся в режим активного согласования:

```
router(config)#interface gigabitethernet 0/2,0/3
router(config-if-range)#link-aggregation 1 active
```

LAN-порты соседнего маршрутизатора переводятся в режим пассивного согласования:

```
router(config)#interface gigabitethernet 0/2,0/3
router(config-if-range)#link-aggregation 2 passive
```

6.5.4 Балансировка нагрузки

Балансировка нагрузки в группе агрегирования каналов L2 может производиться на основании ряда параметров трафика. Доступный набор параметров, по которым может производиться балансировка, зависит от модификации маршрутизатора.

Настройка балансировки в группе агрегирования каналов L2 на MM-4112:

```
router(config)#link-aggregation load-balance dst-ip|dst-mac|src-dst-ip|src-dst-mac|src-ip|src-mac
```

Настройка балансировки в группе агрегирования каналов L2 на MM-4122:

```
router(config)#link-aggregation load-balance dst-mac|src-dst-mac|src-mac
```

Настройка балансировки в группе агрегирования каналов L2 на MM-4102:

```
router(config)#link-aggregation load-balance src-dst-mac
```

6.6 LLDP

6.6.1 Базовая настройка

Глобальное включение протокола LLDP:

```
router(config)#lldp run
```

Включение протокола LLDP на интерфейсах:

```
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#lldp enable
router(config)#interface gigabitethernet 0/1
router(config-if-gigabitethernet0/1)#lldp enable
```

6.6.2 Настройка передаваемых TLV

Можно настроить несколько типов передаваемых TLV.

Настройка передаваемых TLV на LAN-портах:

```
router(config-if-gigabitethernet0/1)#lldp tlv-select basic-tlv|dot1-tlv|dot3-tlv
```

Настройка передаваемых TLV на WAN-портах:

```
router(config-if-gigabitethernet1)#lldp tlv-select basic-tlv|dot3-tlv
```

Для передачи IP-адреса управления необходимо добавить команду:

```
router(config)#lldp management-address <ip address>
```

7 Функции безопасности 2-го уровня

Команды из этого раздела доступны на LAN-портах.

7.1 DHCP Snooping

Функция доступна в модификации MM-4112.

Глобальное включение функции DHCP Snooping:

```
router(config)#dhcp-snooping
```

Перевод LAN-порта, подключенного к DHCP-серверу, в доверенный режим:

```
router(config)#interface gigabitethernet 0/5
router(config-if-gigabitethernet0/5)#dhcp-snooping trust
```

Включение передачи опции 82:

```
router(config)#dhcp-snooping information enable
```

7.2 ARP Inspection

Функция доступна в модификации MM-4112.

Данная функция работает в паре с функцией DHCP Snooping. Настройка ARP Inspection на LAN-порту gigabitethernet0/5:

```
router(config)#interface gigabitethernet 0/5
router(config-if-gigabitethernet0/5)#ip arp inspection
```

7.3 Loopback Detection

Функция доступна в модификациях MM-4122, MM-4102 и MM-4112.

Глобальное включение функции Loopback Detection:

```
router(config)#loopback-detection enable
```

Включение функции Loopback Detection на LAN-порту gigabitethernet0/5:

```
router(config)#interface gigabitethernet 0/5
router(config-if-gigabitethernet0/5)#loopback-detection enable control
```

7.4 Storm Control

Функция доступна в модификациях MM-4102 и MM-4112.

Ограничение количества пакетов Broadcast и Multicast на LAN-порту gigabitethernet0/1 в пакетах/сек:

```
router(config)#interface gigabitethernet 0/1
router(config-if-gigabitethernet0/1)#storm-control broadcast pps 2000
router(config-if-gigabitethernet0/1)#storm-control multicast pps 3000
```

7.5 Port Isolation

Функция доступна в модификациях MM-4122, MM-4102 и MM-4112.

При использовании функции Port Isolation, LAN-порты, входящие в одну группу изоляции, не могут обмениваться данными между собой.

Создание группы изоляции портов и добавление LAN-портов gigabitethernet0/1 и gigabitethernet0/2 в группу изоляции:

```
router(config)#isolate group 1
router(config-isolate-group1)#interface gigabitethernet 0/1,0/2
```

8 Списки контроля доступа (ACL)

8.1 Стандартные ACL

Стандартные нумерованные списки контроля доступа имеют диапазон номеров от 1 до 1000 включительно. Пример настройки стандартного нумерованного ACL:

```
router(config)#access-list 1 permit host 192.168.2.254
router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
router(config)#access-list 1 deny any
```

Пример настройки стандартного именованного ACL:

```
router(config)#ip access-list standard mgmt_acl
router(config-std-nacl)#permit host 192.168.2.100
```

8.2 Расширенные ACL

Расширенные нумерованные списки контроля доступа имеют диапазон номеров от 1001 до 2000 включительно. Пример настройки расширенного нумерованного ACL:

```
router(config)#access-list 1001 permit tcp host 192.168.10.55 host 192.168.11.55 eq 22
```

Пример настройки расширенного именованного ACL:

```
router(config)#ip access-list extended deny_icmp
router(config-ext-nacl)#deny icmp any any
router(config-ext-nacl)#permit ip any any
```

8.3 Назначение ACL

Пример назначения списка контроля доступа на WAN-порт gigabitethernet1:

```
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#ip access-group 1 in
```

Пример назначения списка контроля доступа на интерфейс VLAN 1:

```
router(config)#interface vlan 1
router(config-if-vlan1)#ip access-group 1 in
```

Пример назначения списка контроля доступа на LAN-порт gigaitethernet0/0 (Только для модификаций MM-4112):

```
router(config)#interface gigabitethernet 0/1
router(config-if-gigabitethernet0/1)#ip access-group 1 in
```

Назначение стандартного списка контроля доступа на управление маршрутизатором:

```
router(config)#line vty 0 15
router(config-line)#access-class mgmt_acl in
```

9 Функции 3-го уровня

9.1 Интерфейс VLAN

Функция доступна в модификациях MM-4122, MM-4102 и MM-4112.

Создание интерфейса VLAN 100 и присвоение ему IP-адреса:

```
router(config)#interface vlan 100
router(config-if-vlan100)#ip address 192.168.1.1 255.255.255.0
```

9.2 Интерфейс BVI

Интерфейс BVI — это виртуальный L3-интерфейс, который используется для маршрутизации трафика из bridge-group с соответствующим номером. Добавление интерфейсов в bridge-group описано в пункте 6.2.

В данном примере WAN-интерфейсы объединяются в bridge-group 1, а интерфейс BVI служит виртуальным L3-интерфейсом для обоих портов, добавленных в bridge-group 1:

```
router(config)#interface bvi 1
router(config-if-bvi1)#ip address 192.168.1.1 255.255.255.0
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#bridge-group 1
router(config)#interface gigabitethernet 2
router(config-if-gigabitethernet2)#bridge-group 1
```

9.3 Создание подинтерфейсов

Команды доступны на WAN-портах.

Создание подинтерфейса с номером 200 на WAN-порту gigabitethernet2:

```
router(config)#interface gigabitethernet 2.200
```

Настройка инкапсуляции с VLAN ID 200 на подинтерфейсе gigabitethernet2.200 и задание IP-адреса на этот подинтерфейс:

```
router(config-if-gigabitethernet2.200)#encapsulation dot1q 200
router(config-if-gigabitethernet2.200)#ip address 192.168.1.1 255.255.255.0
```

9.4 Агрегирование каналов L3

Функция доступна в модификациях MM-4122, MM-4102 и MM-4112.

9.4.1 Создание группы агрегирования каналов L3

Создание группы агрегирования каналов L3, настройка IP-адреса и выбор метода согласования параметров:

```
router(config)#interface route-aggregation 1
router(config-if-route-aggregation1)#ip address 192.168.1.1 255.255.255.0
router(config-if-route-aggregation1)#route-aggregation mode manual|lacp
```

9.4.2 Настройка интерфейсов группы агрегирования

9.4.2.1 Без протокола согласования

Команда доступна на WAN-портах.

WAN-порты нужно добавлять в группу агрегирования L3 в режиме без протокола согласования, когда группа агрегирования L3 настроена в режиме manual.

Добавление WAN-портов gigabitethernet0 и gigabitethernet1 в группу агрегирования каналов L3 без протокола согласования:

```
router(config)#interface gigabitethernet 0
router(config-if-gigabitethernet0)#route-aggregation group 1 manual
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#route-aggregation group 1 manual
```

9.4.2.2 LACP

Команды доступны на WAN-портах.

WAN-порты нужно добавлять в группу агрегирования L3 в этом режиме, когда группа агрегирования L3 настроена в режиме lacp.

Добавление WAN-портов gigabitethernet0 и gigabitethernet1 в группу агрегирования каналов L3 в режиме активного согласования параметров:

```
router(config)#interface gigabitethernet 0
router(config-if-gigabitethernet0)#route-aggregation group 1 active
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#route-aggregation group 1 active
```

Добавление WAN-портов gigabitethernet0 и gigabitethernet1 в группу агрегирования каналов L3 в режиме пассивного согласования параметров:

```
router(config)#interface gigabitethernet 0
router(config-if-gigabitethernet0)#route-aggregation group 1 passive
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#route-aggregation group 1 passive
```

9.4.3 Балансировка нагрузки

Настройка балансировки нагрузки в группе агрегирования каналов L3:

```
router(config)#interface route-aggregation 1
router(config-if-route-aggregation1)#route-aggregation load-sharing destination-ip|flowid|per-packet|source-destination-ip|source-ip
```

9.5 DHCP-сервер

Функцию DHCP-сервера можно настроить на WAN-портах (для всех модификаций) и на интерфейсах VLAN (только для модификаций MM-4122, MM-4102 и MM-4112).

Настройка пула DHCP:

```
router(config)#ip dhcp pool pool1
router(dhcp-config)#network 192.168.1.0 255.255.255.0
router(dhcp-config)#dns-server 192.168.1.50
router(dhcp-config)#default-router 192.168.1.1
```

Настройка статических записей DHCP:

```
router(config)#ip dhcp pool pool1
router(dhcp-config)#bind 192.168.1.253 0013.46ec.f355
router(dhcp-config)#bind 192.168.1.254 e411.5b58.d1f9
```

Настройка исключенных IP-адресов, которые не будут выдаваться DHCP-сервером:

```
router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.50
```

Включение функции DHCP-сервера на WAN-интерфейсе:

```
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#ip dhcp server
```

9.6 NAT

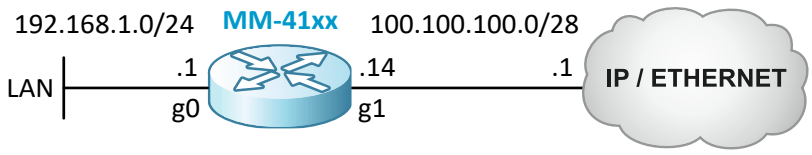

Рисунок 1 — Схема применения NAT

9.6.1 Настройка ролей интерфейсов NAT

Команды доступны на WAN-портах (для всех модификаций) и на интерфейсах VLAN (только для модификаций MM-4122, MM-4102 и MM-4112). Роли интерфейсов NAT нужно настраивать для всех типов NAT.

Настройка WAN-порта gigabitethernet0 в роли внутреннего интерфейса NAT:

```
router(config)#interface gigabitethernet0
```

```
router(config-if-gigabitethernet0)#ip nat inside
```

Настройка WAN-порта gigabitethernet1 в роли внешнего интерфейса NAT:

```
router(config)#interface gigabitethernet1
router(config-if-gigabitethernet1)#ip nat outside
```

9.6.2 Настройка Статического NAT

Статический NAT позволяет сделать внутренний ресурс, имеющий IP-адрес из частного диапазона, доступным из внешней сети путем однозначного преобразования публичного IP-адреса в соответствующий частный IP-адрес.

Настройка преобразования внешнего публичного IP-адреса 100.100.100.13 во внутренний частный IP-адрес 192.168.1.254:

```
router(config)#ip nat inside source static 192.168.1.254 100.100.100.13
```

9.6.3 Настройка Динамического NAT

Динамический NAT позволяет устройствам внутренней сети, имеющим IP-адреса из частного диапазона, получать доступ к ресурсам во внешней сети путем динамического преобразования частного IP-адреса в публичный IP-адрес из настроенного пула публичных IP-адресов.

Настройка пула публичных IP-адресов с именем dnat_pool:

```
router(config)#ip nat pool dnat_pool
router(config-nat-pool)#address 100.100.100.2 100.100.100.13
```

Настройка стандартного списка доступа для внутренних устройств, которым нужно получать доступ к внешним ресурсам:

```
router(config)#ip access-list standard dnat_acl
router(config-ext-nacl)#permit 192.168.1.0 0.0.0.255
```

Настройка правила динамического NAT:

```
router(config)#ip nat inside source list dnat_acl pool dnat_pool
```

9.6.4 Настройка PAT

Данный тип NAT позволяет преобразовать диапазон частных IP-адресов внутренней сети в публичный IP-адрес WAN-интерфейса, используя порты транспортного уровня.

Настройка стандартного списка доступа для внутренних устройств, которым нужно получать доступ к внешним ресурсам:

```
router(config)#ip access-list standard pat_acl
router(config-ext-nacl)#permit 192.168.1.0 0.0.0.255
```

Настройка правила PAT для внешнего WAN-интерфейса gigabitethernet1:

```
router(config)#ip nat inside source list pat_acl interface gigabitethernet 1 overload
```

9.7 VRRP

Протокол VRRP позволяет зарезервировать шлюз по умолчанию, используя два или более маршрутизатора. Команды доступны на WAN-интерфейсах (для всех модификаций) и на интерфейсах VLAN (только для модификаций MM-4122, MM-4102 и MM-4112).

Настройка виртуального IP-адреса протокола VRRP и приоритета VRRP на WAN-порту активного маршрутизатора (Master):

```
router(config)#interface gigabitethernet 0
router(config-if-gigabitethernet0)#ip address 192.168.1.1 255.255.255.0
router(config-if-gigabitethernet0)#vrrp 1 ip 192.168.1.3
router(config-if-gigabitethernet0)#vrrp 1 priority 110
```

Настройка виртуального IP-адреса протокола VRRP и приоритета VRRP на интерфейсе VLAN запасного маршрутизатора (Backup):

```
router(config)#interface vlan 1
router(config-if-vlan1)#ip address 192.168.1.2 255.255.255.0
router(config-if-vlan1)#vrrp 1 ip 192.168.1.3
router(config-if-vlan1)#vrrp 1 priority 90
```

9.8 Статическая маршрутизация

Настройка статического маршрута:

```
router(config)#ip route 172.16.1.0 255.255.255.0 10.10.10.2
```

9.9 RIP

Настройка непосредственно подключенной сети, которая будет передаваться в маршрутных обновлениях протокола RIP соседним маршрутизаторам:

```
router(config)#router rip
router(config-rip)#network 192.168.1.0
```

Для работы протокола RIP нужно также анонсировать сеть, которая используется между маршрутизаторами RIP:

```
router(config-rip)#network 192.168.10.0
```

9.10 RIPv2

Настройка непосредственно подключенной сети, которая будет передаваться в маршрутных обновлениях протокола RIPv2 соседним маршрутизаторам. Маска подсети, настроенная на соответствующем сетевом интерфейсе, также будет передаваться в маршрутных обновлениях протокола RIPv2:

```
router(config)#router rip
router(config-rip)#version 2
router(config-rip)#network 192.168.1.0
```

Для работы протокола RIPv2 нужно анонсировать сеть, которая используется между маршрутизаторами RIPv2:

```
router(config-rip)#network 192.168.10.0
```

9.11 OSPF

Запуск процесса OSPF 1 и настройка непосредственно подключенной сети, которая будет передаваться в маршрутных обновлениях протокола OSPF соседним маршрутизаторам:

```
router(config)#router ospf 1
router(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
```

Для установления соседства с другим маршрутизатором по протоколу OSPF, нужно анонсировать подсеть, которая используется между маршрутизаторами:

```
router(config-ospf)#network 10.10.10.0 0.0.0.3 area 0
```

Для подавления отправки Hello-сообщений и блокировки установления соседства через определенный интерфейс, этот интерфейс можно настроить как пассивный:

```
router(config-ospf)#passive-interface gigabitethernet 1
```

9.12 BGP

Настройка соседства по eBGP:

```
router(config)#router bgp 65000
router(config-bgp)#neighbor 100.100.100.2 remote-as 65100
```

Настройка соседства по iBGP:

```
router(config)#router bgp 65000
router(config-bgp)#neighbor 10.10.10.2 remote-as 65000
```

Указание префикса, который будет передаваться соседям BGP. Данный префикс должен присутствовать в таблице маршрутизации:

```
router(config-bgp)#network 192.168.10.0 255.255.255.0
```

Протокол BGP анонсирует только префиксы, которые присутствуют в таблице маршрутизации. В случае если нужно анонсировать суммарный маршрут по BGP, нужно создать суммарную маршрутную запись:

```
router(config)#ip route 192.168.0.0 255.255.0.0 null 0
router(config)#router bgp 65000
router(config-bgp)#network 192.168.0.0 255.255.0.0
```

10 Firewall

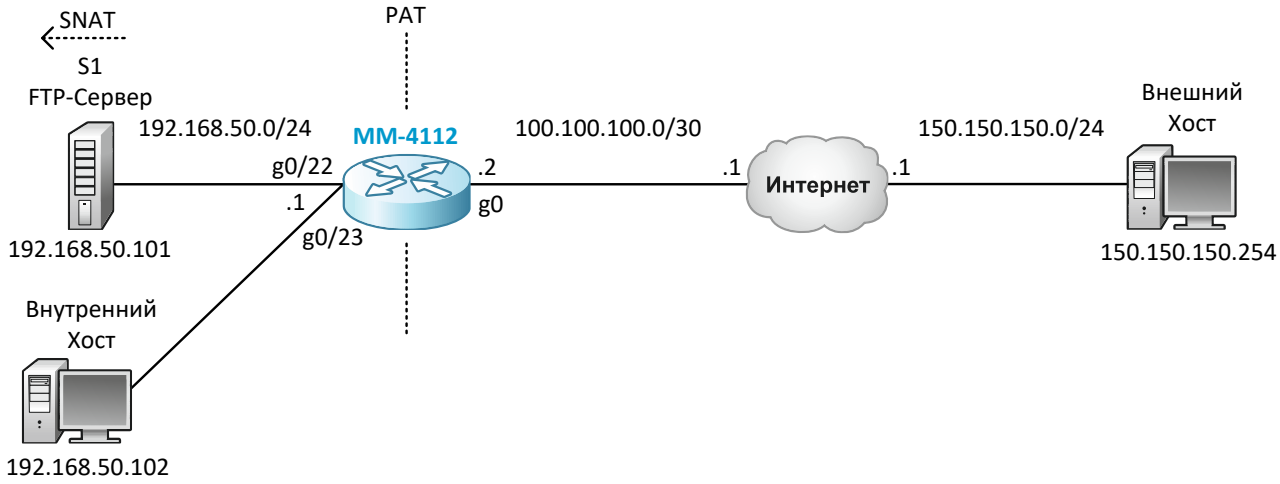

Рисунок 2 — Схема настройки Firewall

В данном примере во внутренней сети настроен FTP-сервер S1, который должен быть доступен для внешних хостов, а также внутренний хост, который должен получать доступ к ресурсам внешней сети. На маршрутизаторе настраивается PAT для внутреннего хоста и трансляция портов для FTP-сервера. Firewall реализуется на основе Reflexive ACL. В примере сервер S1 и внутренний хост подключаются ко встроенному коммутатору маршрутизатора MM-4112. Пример подразумевает наличие базовых настроек IP-связности.

10.1 Настройка PAT для внутренних хостов

Настройка ACL для PAT:

```
router(config)#ip access-list extended pat_acl
router(config-ext-nacl)#10 permit ip host 192.168.50.102 any
router(config-ext-nacl)#20 deny ip any any
```

Настройка пула внешних IP-адресов и портов транспортного уровня для PAT:

```
router(config)#ip nat pool pat_pool
router(config-nat-pool)#port-range 5000 65535
router(config-nat-pool)#address 100.100.100.2 100.100.100.2
```

Настройка ролей портов в PAT:

```
router(config)#interface gigabitethernet0
router(config-if-gigabitethernet0)#ip nat outside
router(config)#interface vlan10
router(config-if-vlan10)#ip nat inside
```

Применение правила преобразования PAT:

```
router(config)#ip nat inside source list pat_acl pool pat_pool overload
```

10.2 Настройка проброса портов для внутреннего FTP-сервера

Настройка трансляции TCP-порта 21 (управляющий трафик протокола FTP):

```
router(config)#ip nat inside source static tcp 192.168.50.101 21 100.100.100.2 21
```

Настройка трансляции TCP-портов 4000-4100 (порты пассивного режима обмена, настроенные на FTP-сервере):

```
router(config)#ip nat inside source static tcp range 192.168.50.101 4000 4100 100.100.100.2 4000 4100
```

10.3 Настройка Firewall на основе Reflexive ACL

Настройка исходящего ACL, который будет захватывать весь исходящий трафик и создавать на его основе Reflexive ACL «outbound_traffic»:

```
router(config)#ip access-list extended outbound_acl
router(config-ext-nacl)#10 permit ip any any reflect outbound_traffic timeout 30
```

В данном примере правила в Reflexive ACL будут храниться в течение 30-ти секунд.

Настройка входящего ACL, который будет пропускать во внутреннюю сеть трафик, предназначенный FTP-серверу, а также ответный трафик на основании Reflexive ACL:

```
router(config)#ip access-list extended inbound_acl
router(config-ext-nacl)#10 evaluate outbound_traffic
router(config-ext-nacl)#20 permit tcp any host 100.100.100.2 eq ftp
router(config-ext-nacl)#30 permit tcp any host 100.100.100.2 range 4000 4100
router(config-ext-nacl)#100 deny ip any any
```

Весь остальной входящий трафик будет запрещен.

Применение созданных ACL на WAN-порту маршрутизатора:

```
router(config)#interface gigabitethernet0
router(config-if-gigabitethernet0)#ip access-group inbound_acl in
router(config-if-gigabitethernet0)#ip access-group outbound_acl out
```

11 QoS

11.1 Классификация

Для настройки классификации трафика используется Class Map. Class Map позволяет выделить нужный трафик из общего потока трафика. Выделение трафика возможно на основании широкого набора параметров.

Пример настройки классификации трафика на основании списка контроля доступа:

```
router(config)#ip access-list extended qos_acl
router(config-ext-nacl)#permit tcp host 192.168.1.100 any eq 443
router(config)#class-map class_map_1
router(config-cmap)#match access-group qos_acl
```

11.2 Маркировка

Для настройки маркировки трафика используется Policy Map. Policy Map позволяет настроить действие, которое будет производиться над трафиком, выделенным с помощью Class Map. В данном примере — маркировка выделенного трафика меткой DSCP.

Пример настройки маркировки трафика, выделенного class_map_1, меткой DSCP 46:

```
router(config)#policy-map policy_map_1
router(config-pmap)#class class_map_1
router(config-pmap-c)#set ip dscp 46
```

11.3 Применение политики

Команды доступны на WAN-портах и интерфейсах VLAN (применение политик на интерфейсах VLAN доступно только в модификациях MM-4122 и MM-4112).

Для того чтобы настроенные Class Map и Policy Map начали работать, нужно применить Policy Map на соответствующем интерфейсе во входящем или исходящем направлении.

Пример применения политики policy_map_1 на интерфейсе VLAN 10 во входящем направлении:

```
router(config)#interface vlan 10
routerconfig-if-vlan10)# service-policy input policy_map_1
```

Пример применения политики policy_map_2 на WAN-порт gigabitethernet 1 в исходящем направлении:

```
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)# service-policy output policy_map_2
```

12 AAA

12.1 TACACS+

Настройка сервера TACACS+ и ключа, которые будут использоваться маршрутизатором:

```
router#configure terminal
router(config)#aaa server group tacacs TG1
router(config-sg-tacacs-TG1)#server 192.168.135.254 port 49 key secret123
router(config-sg-tacacs-TG1)#exit
```

Настройка способа аутентификации и авторизации (в случае недоступности сервера TACACS+, для аутентификации и авторизации будет использоваться локальная база пользователей) и настройка аккаунтинга:

```
router#configure terminal
router(config)#domain zelax
router(config-isp-test)#aaa authentication login tacacs-group TG1 local
router(config-isp-test)#aaa authorization login tacacs-group TG1 local
router(config-isp-test)#aaa accounting login start-stop tacacs-group TG1
router(config-isp-test)#exit
router(config)#line vty 0 15
router(config-line)#login aaa zelax
router(config-line)#exit
```

12.2 RADIUS

Настройка сервера RADIUS и ключа, которые будут использоваться маршрутизатором:

```
router#configure terminal
router(config)#aaa server group radius RG1
router(config-sg-radius-RG1)#server 192.168.135.254 auth-port 1812 acct-port 1813 key secret123
router(config-sg-radius-RG1)#exit
```

Настройка способа аутентификации и авторизации (в случае недоступности сервера RADIUS, для аутентификации и авторизации будет использоваться локальная база пользователей) и настройка аккаунтинга:

```
router(config)#domain zelax
router(config-isp-test)#aaa authentication login radius-group RG1 local
router(config-isp-test)#aaa authorization login radius-group RG1 local
router(config-isp-test)#aaa accounting login start-stop radius-group RG1
router(config-isp-test)#exit
router(config)#line vty 0 15
router(config-line)#login aaa zelax
router(config-line)#exit
```

13 VPN

13.1 Туннель GRE

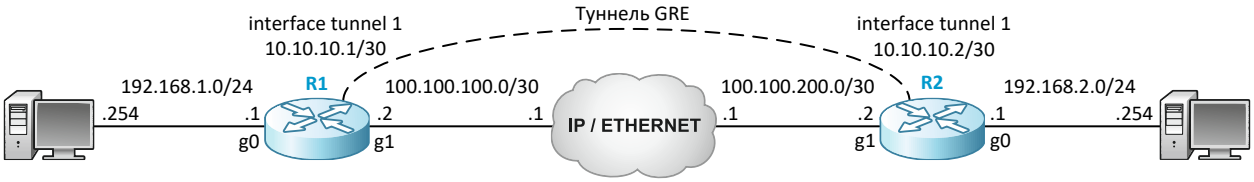

Рисунок 3 — Схема применения туннеля GRE

Настройка туннеля GRE на маршрутизаторе R1:

```
router(config)#interface tunnel 1
router(config-if-tunnel1)#ip address 10.10.10.1 255.255.255.252
router(config-if-tunnel1)#tunnel source 100.100.100.2
router(config-if-tunnel1)#tunnel destination 100.100.200.2
```

Настройка маршрута через GRE-туннель на маршрутизаторе R1:

```
router(config)#ip route 192.168.2.0 255.255.255.0 10.10.10.2
```

На ответном маршрутизаторе MM-41xx R2 выполняются симметричные настройки.

13.2 Настройка туннеля IPsec

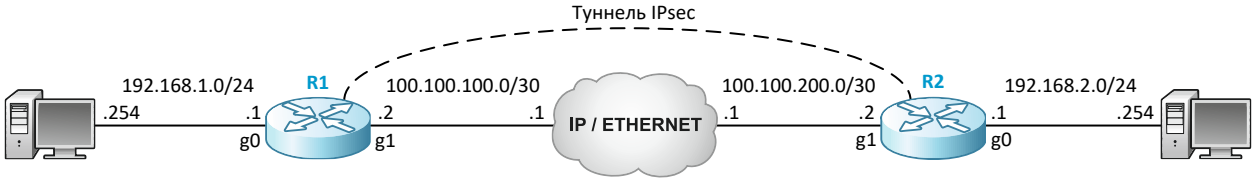

Рисунок 4 — Схема применения туннеля IPsec

Настройка предложения IKE с именем «ikepro» с использованием алгоритма шифрования 3DES, алгоритма аутентификации SHA1 и группы Диффи-Хеллмана 2:

```
ROUTER1#configure terminal
ROUTER1(config)#crypto ike proposal ikepro
ROUTER1(config-ike-prop)#encryption 3des
ROUTER1(config-ike-prop)#group group2
ROUTER1(config-ike-prop)#integrity sha1
ROUTER1(config-ike-prop)#exit
```

Настройка предложения IPsec с именем «ippro», с использованием алгоритма шифрования 3DES и аутентификации SHA1:

```
ROUTER1(config)#crypto ipsec proposal ippro
ROUTER1(config-ipsec-prop)#esp 3des sha1
ROUTER1(config-ipsec-prop)#exit
```

Настройка предопределенного ключа:

```
ROUTER1(config)#crypto ike key secret123 any
```

Настройка IPsec туннеля:

```
ROUTER1(config)#crypto tunnel crtun
ROUTER1(config-tunnel)#local address 100.100.100.2
ROUTER1(config-tunnel)#peer address 100.100.200.2
ROUTER1(config-tunnel)#set authentication preshared
ROUTER1(config-tunnel)#set ike proposal ikepro
ROUTER1(config-tunnel)#set ipsec proposal ippro
ROUTER1(config-tunnel)#set auto-up
ROUTER1(config-tunnel)#exit
ROUTER1(config)#crypto policy crpol
ROUTER1(config-policy)#flow 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 ip ipv4-tunnel crtun
ROUTER1(config-policy)#set reverse-route
ROUTER1(config-policy)#exit
```

Противоположный маршрутизатор MM-41xx R2 настраивается симметричным образом.

13.3 Настройка L2TP

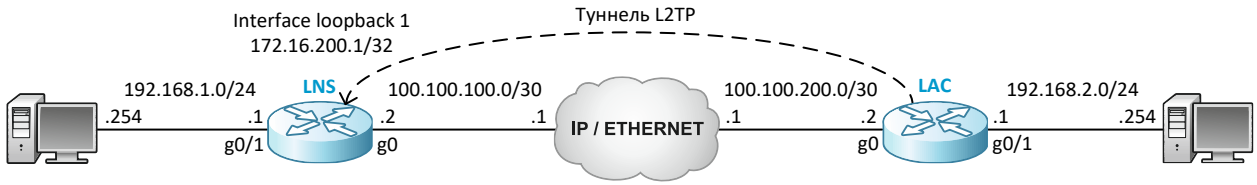

Рисунок 5 — Схема применения туннеля L2TP

Для построения туннеля протокол L2TP использует два типа устройств VPDN: LAC (L2TP Access Concentrator) и LNS (L2TP Network Server). LNS выступает в качестве сервера, к которому подключаются клиенты LAC.

13.3.1 Настройка маршрутизатора LNS

Настройка интерфейса loopback0, IP-адрес которого будет использоваться в качестве туннельного IP-адреса сервера LNS:

```
LNS(config)#interface loopback0
LNS(config-if-loopback0)#ip address 172.16.200.1 255.255.255.255
```

Настройка пользователя, который будет использоваться для аутентификации LAC по PPP:

```
LNS(config)#local-user user123 class network
LNS(config-user-network-admin)#password 0 user123
LNS(config-user-network-admin)#service-type ppp
```

Настройка пула IP-адресов, которые будут выдаваться виртуальным интерфейсам подключающихся LAC:

```
LNS(config)#ip local pool l2tp_pool 172.16.200.10 172.16.200.20
```

Настройка интерфейса virtual-template 1, который будет использоваться для подключения LAC, с аутентификацией MS-CHAPv2:

```
LNS(config)#interface virtual-template 1
LNS(config-if-virtual-template0)#encapsulation ppp
LNS(config-if-virtual-template0)#ppp authentication ms-chap-v2
LNS(config-if-virtual-template0)#ip unnumbered loopback0
LNS(config-if-virtual-template0)#peer default ip address pool l2tp_pool
LNS(config-if-virtual-template0)#keepalive 1
```

Включение VPDN:

```
LNS(config)#vpdn enable
```

Настройка VPDN-группы и разрешение принимать запросы удаленного доступа:

```
LNS(config)#vpdn-group 1
LNS(config-vpdn)#accept-dialin
LNS(config-vpdn-acc-in)#protocol l2tp
LNS(config-vpdn-acc-in)#virtual-template 1
```

Настройка пароля для аутентификации туннеля L2TP:

```
LNS(config-vpdn)#local name lns
LNS(config-vpdn)#l2tp tunnel password vpdn_pass
```

Настройка протокола OSPF для автоматического добавления маршрутов после установления соединения по L2TP:

```
LNS(config)#router ospf 1
LNS(config-ospf)#passive-interface gigabitethernet0
LNS(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
LNS(config-ospf)#network 172.16.200.1 0.0.0.0 area 0
```

13.3.2 Настройка маршрутизатора LAC

Для подключения к LNS, на LAC нужно настроить pseudowire-class, в котором указывается тип инкапсуляции, пароль аутентификации туннеля L2TP, имя участника L2TP-сессии и локальный интерфейс:

```
LAC(config)#pseudowire-class pw_class
LAC(config-pw-class)#encapsulation l2tpv2
LAC(config-pw-class)#password 0 vpdn_pass
LAC(config-pw-class)#hostname lac
LAC(config-pw-class)#ip local interface gigabitethernet0
```

Настройка виртуального интерфейса virtual-ppp1 с инкапсуляцией PPP и аутентификацией MS-CHAPv2 для установления соединения с LNS по адресу 100.100.100.2:

```
LAC(config)#interface virtual-ppp 1
LAC(config-if-virtual-ppp0)#encapsulation ppp
LAC(config-if-virtual-ppp0)#ppp authentication ms-chap-v2
LAC(config-if-virtual-ppp0)#ppp chap hostname user123
LAC(config-if-virtual-ppp0)#ppp chap password 0 user123
LAC(config-if-virtual-ppp0)#ip address negotiated
LAC(config-if-virtual-ppp0)#pseudowire 100.100.100.2 1 pw-class pw_class
LAC(config-if-virtual-ppp0)#keepalive 1
```

Цифра «1» в команде pseudowire задает виртуальный идентификатор туннеля L2TP, который должен быть одинаковым с обеих сторон туннеля L2TP.

Настройка протокола OSPF для автоматического добавления маршрутов после установления соединения по L2TP:

```
LAC(config)#router ospf 1
LAC(config-ospf)#passive-interface gigabitethernet0
LAC(config-ospf)#network 192.168.2.0 0.0.0.255 area 0
LAC(config-ospf)#network 172.16.200.0 0.0.0.255 area 0
```

14 MPLS

14.1 LDP

Стоит обратить внимание, что для связности по протоколу LDP необходима предварительная настройка протокола IGP.

Глобальное включение LDP, назначение идентификатора маршрутизатора и транспортного адреса:

```
router(config)#mpls ldp
router(config-ldp)#router-id 1.1.1.1
router(config-ldp)#address-family ipv4
router(config-ldp-af4)#transport-address 1.1.1.1
```

Включение LDP на интерфейсе gigabitethernet 0:

```
router(config)#interface gigabitethernet 0
router(config-if-gigabitethernet0)#mpls ldp
```

14.2 MPLS

Глобальное включение MPLS:

```
router(config)#mpls ip
```

Включение MPLS на интерфейсе gigabitethernet 0:

```
router(config)#interface gigabitethernet 0
router(config-if-gigabitethernet0)#mpls ip
```

14.3 VRF

Создание VRF с заданным именем:

```
router(config)#ip vrf vrf_A
```

Назначение Route Distinguisher, который будет использоваться для идентификации данного VRF:

```
router(config-vrf)#rd 65000:100
```

Назначение порта в определенный VRF:

```
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#ip vrf forwarding vrf_A
```

14.4 L2VPN

Команды доступны на портах WAN (во всех модификациях) и интерфейсах VLAN (в модификациях MM-4122, MM-4112 и MM-4131). Команды недоступны на портах WAN/LAN в режиме WAN.

Перед настройкой MPLS L2VPN необходимо обеспечить связность устройств по протоколам LDP и MPLS.

14.4.1 VPWS

При настройке L2VPN нужно указать IP-адрес целевого устройства, с которым будет установлен туннель VPWS:

```
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet1)#mpls ip
router(config-if-gigabitethernet1)#xconnect 3.3.3.3 1 encapsulation mpls ethernet
```

Просмотр состояния VPWS:

```
router#show mpls ldp l2-circuit
VC-ID     Interface           State     Type         Local-Label    Remote-Label   Destination-Address
1         gigabitethernet     UP        ethernet     17             17             3.3.3.3
Statistics for L2-circuit:
       L2-circuit up: 1
       L2-circuit down: 0
```

14.4.2 VPLS

Данный пример реализует схему hub-and-spoke, в которой один маршрутизатор выступает в роли концентратора для остальных устройств, на которых настраивается VPWS.

Создание экземпляра VPLS с именем vpls_A:

```
router(config)#mpls vpls vpls_A manual
router(config-vpls)#vpn-id 10
router(config-vpls)#peer 3.3.3.3 tagged
```

Привязка определенного интерфейса к VPLS:

```
router(config)#interface gigabitethernet 2
router(config-if-gigabitethernet2)#mpls ip
router(config-if-gigabitethernet2)#mpls vpls vpls_A ethernet
```

Просмотр состояния VPLS:

```
router#show mpls ldp vpls
VPLS-ID     Peer Address      State            Type       Local-MTU   Remote-MTU  Label-Sent   Label-
Rcvd
10          3.3.3.3           Up               tag        1500        1500        24000        24000
Statistics for ldp vpls:
    LDP VPLS up: 1
    LDP VPLS down: 0
```

14.5 L3VPN

Команды доступны на портах WAN (во всех модификациях) и интерфейсах VLAN (в модификациях MM-4122, MM-4112 и MM-4131). Команды недоступны на портах WAN/LAN в режиме WAN.

Перед настройкой MPLS L3VPN необходимо обеспечить связность устройств по протоколам LDP и MPLS.

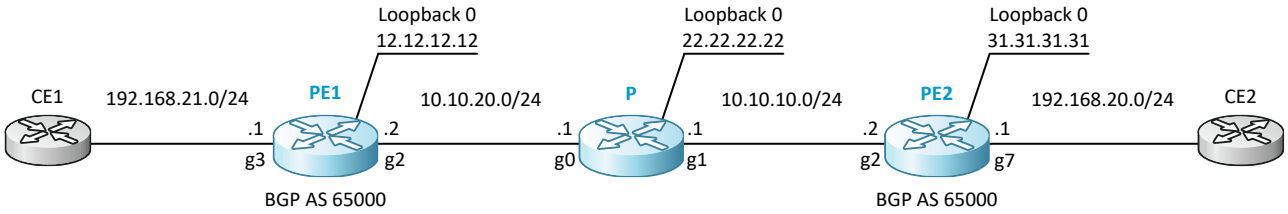

Рисунок 6 — Схема применения MPLS L3 VPN

14.5.1 Пример настройки маршрутизатора PE1

Создание интерфейса Loopback и присвоение ему IP-адреса:

```
PE1(config)#interface loopback 0
PE1(config-if-loopback0)#ip address 12.12.12.12 255.255.255.255
```

Настройка процесса OSPF 50 для внутренней сети провайдера:

```
PE1(config)#router ospf 50
PE1(config-ospf)# network 10.10.20.0 0.0.0.255 area 0
PE1(config-ospf)# network 12.12.12.12 0.0.0.0 area 0
```

Настройка MPLS и LDP в глобальном режиме:

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 12.12.12.12
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 12.12.12.12
```

Настройка MPLS и LDP на интерфейсе:

```
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#mpls ip
PE1(config-if-gigabitethernet2)#mpls ldp
```

Создание VRF с именем vrf_A:

```
PE1(config)#ip vrf vrf_A
```

Назначение идентификатора Route Distinguisher и настройка Route Target для VRF vrf_A:

```
PE1(config-vrf)#rd 65000:100
PE1(config-vrf)#route-target import 65000:100
PE1(config-vrf)#route-target export 65000:100
```

Помещение интерфейса в сторону CE в VRF и назначение этому интерфейсу IP-адреса:

```
PE1(config)#interface gigabitethernet 3
PE1(config-if-gigabitethernet3)#ip vrf forwarding vrf_A
PE1(config-if-gigabitethernet3)#ip address 192.168.21.1 255.255.255.0
```

Настройка MBGP и настройка редистрибуции маршрутов в BGP из процесса OSPF 100:

```
PE1(config)#router bgp 65000
PE1(config-bgp)#network 12.12.12.12 255.255.255.255
PE1(config-bgp)#neighbor 31.31.31.31 remote-as 65000
PE1(config-bgp)#neighbor 31.31.31.31 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 31.31.31.31 activate
PE1(config-bgp-af)#neighbor 31.31.31.31 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf vrf_A
PE1(config-bgp-af)#redistribute connected
PE1(config-bgp-af)#redistribute ospf 100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp-af)#exit
```

Настройка процесса OSPF 100 для обмена маршрутами с CE в VRF vrf_A и настройка редистрибуции маршрутов в процесс OSPF 100 из BGP:

```
PE1(config)#router ospf 100 vrf vrf_A
PE1(config-ospf)#network 192.168.21.0 0.0.0.255 area 0
PE1(config-ospf)#redistribute bgp 65000
PE1(config-ospf)#exit
```

14.5.2 Пример настройки маршрутизатора P

Создание Loopback интерфейса и присвоение ему IP-адреса:

```
P(config)#interface loopback 0
P(config-if-loopback0)#ip address 22.22.22.22 255.255.255.255
```

Настройка процесса OSPF 50 для внутренней сети провайдера:

```
P(config)#router ospf 50
P(config-ospf)#network 10.10.10.0 0.0.0.255 area 0
P(config-ospf)#network 10.10.20.0 0.0.0.255 area 0
P(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
```

Настройка MPLS и LDP в глобальном режиме:

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 22.22.22.22
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 22.22.22.22
```

Настройка MPLS и LDP на интерфейсах:

```
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
```

14.5.3 Пример настройки маршрутизатора PE2

Маршрутизатор PE2 настраивается аналогичным с PE1 образом:

```
hostname PE2
!
ip vrf vrf_A
 rd 65000:100
 route-target export 65000:100
 route-target import 65000:100
 exit
!
mpls ip
!
interface loopback0
 ip address 31.31.31.31 255.255.255.255
```

```
 exit
!
interface gigabitethernet2
 ip address 10.10.10.2 255.255.255.0
 mpls ip
 mpls ldp
 exit
!
interface gigabitethernet7
 ip vrf forwarding vrf_A
 ip address 192.168.22.1 255.255.255.0
 exit
!
router ospf 50
 network 10.10.10.0 0.0.0.255 area 0
 network 31.31.31.31 0.0.0.0 area 0
 exit
!
router ospf 100 vrf vrf_A
 network 192.168.22.0 0.0.0.255 area 0
 redistribute bgp 65000
 exit
!
router bgp 65000
 no auto-summary
 no synchronization
 network 31.31.31.31 255.255.255.255
 neighbor 12.12.12.12 remote-as 65000
 neighbor 12.12.12.12 update-source loopback0
 address-family vpnv4
  neighbor 12.12.12.12 activate
  neighbor 12.12.12.12 send-community extended
  exit-address-family
 address-family ipv4 vrf vrf_A
  redistribute connected
  redistribute ospf 100
  exit-address-family
 exit
!
mpls ldp
 router-id 31.31.31.31
 address-family ipv4
  transport-address 31.31.31.31
  exit
 exit
```

14.5.4 Диагностические команды для просмотра состояния работы MPLS L3VPN

Вывод маршрутов BGP vpnv4 для VRF vrf_A:

```
PE1#show ip bgp vpnv4 vrf vrf_A
BGP table version is 6, local router ID is 12.12.12.12
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network             Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 65000:100 (Default for VRF vrf_A)
[C]*> 192.168.21.0/24     0.0.0.0                  0             32768 ?
[B]*>i192.168.22.0/24     31.31.31.31              0        100      0 ?
[O]*> 192.168.121.0/24    192.168.21.250          12             32768 ?
[B]*>i192.168.122.0/24    31.31.31.31             12        100      0 ?

Total number of prefixes 4
```

Вывод маршрутов в VRF vrf_A:

```
PE1#show ip route vrf vrf_A
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   192.168.21.0/24 is directly connected, 04:34:48, gigabitethernet3
L   192.168.21.1/32 is directly connected, 04:34:48, gigabitethernet3
B   192.168.22.0/24 [200/0] via 31.31.31.31, 04:02:59, gigabitethernet2
O   192.168.121.0/24 [110/11] via 192.168.21.250, 04:33:54, gigabitethernet3
B   192.168.122.0/24 [200/12] via 31.31.31.31, 04:02:59, gigabitethernet2
```

Вывод установленных LDP-сессий:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type     My Role   State         DS Cap    DeadTime
22.22.22.22        Multicast     Passive   OPERATIONAL   Disabled  00:02:37
Statistics for ldp sessions:
       Multicast sessions: 1
       Targeted sessions: 0
```

15 Функции диагностики

15.1 Локальный журнал событий

По умолчанию на маршрутизаторах настроено логирование событий во flash-память с уровнем Notifications и выше. Изменение уровня логирования выполняется с помощью команды:

```
router(config)#logging source default file level ?
    <0-7>                Num of severity
    alerts               Alert:action must be taken immediately  (severity=1)
    critical             Critical:critical conditions            (severity=2)
    debugging            Debug:debug-level messages              (severity=7)
    emergencies          Emergency:system is unusable            (severity=0)
    errors               Error:error conditions                  (severity=3)
    informational        Informational:informational messages    (severity=6)
    notifications        Notice:normal but significant condition (severity=5)
    warnings             Warning:warning conditions              (severity=4)
```

Возможные уровни логирования:

- Alerts;
- Critical;
- Debugging;
- Informational;
- Warnings;
- Notifications;
- Errors;
- Emergencies.

Просмотр локального журнала событий выполняется с помощью команды:

```
router#show logging file
```

15.2 Syslog

Настройка сервера Syslog, на который будет производиться логирование:

```
router(config)#logging server syslog1 ip 192.168.1.200
```

Изменение IP-адреса отправителя для сообщений Syslog:

```
router(config)#logging server source ip 192.168.1.1
```

15.3 Зеркалирование трафика SPAN

Функция SPAN позволяет зеркалировать трафик в пределах одного маршрутизатора. Команды доступны на LAN-портах и WAN-портах. Команды не доступны для интерфейсов VLAN и подинтерфейсов.

Настройка зеркалирования трафика SPAN на LAN-портах:

```
router(config)#monitor session 1 source interface gigabitethernet 0/1
router(config)#monitor session 1 destination interface gigabitethernet 0/2
```

Настройка зеркалирования трафика SPAN на WAN-портах:

```
router(config)#monitor-l3 session 1 source interface gigabitethernet 2
router(config)#monitor-l3 session 1 destination interface gigabitethernet 3
```

15.4 Зеркалирование трафика RSPAN

Функция доступна в модификации MM-4112.

Функция RSPAN позволяет зеркалировать трафик в пределах одного LAN-сегмента.

15.4.1 Настройка RSPAN на маршрутизаторе-источнике

Настройка VLAN для RSPAN:

```
router(config)#vlan 20
router(config-vlan20)#remote-span
%SPAN : vlan 20 is remote-vlan now, mac learning forbid.
%SPAN : remote-vlan should be a free vlan, used for RSPAN only.
```

Настройка выходного LAN-порта на маршрутизаторе-источнике, в который будет направляться зеркалированный трафик:

```
router(config)#interface gigabitethernet 0/3
router(config-if-gigabitethernet0/3)#switchport mode trunk
router(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 20
```

Настройка сессии RSPAN на маршрутизаторе-отправителе. Указание порта-источника и выходного LAN-порта, через который зеркалированный трафик будет отправляться в сторону маршрутизатора-получателя:

```
router(config)#monitor session 1 source interface gigabitethernet 0/2
router(config)#monitor session 1 destination remote vlan 20 interface gigabitethernet 0/3
```

15.4.2 Настройка RSPAN на маршрутизаторе-получателе

Настройка VLAN для RSPAN:

```
router(config)#vlan 20
router(config-vlan20)#remote-span
%SPAN : vlan 20 is remote-vlan now, mac learning forbid.
%SPAN : remote-vlan should be a free vlan, used for RSPAN only.
```

Настройка LAN-порта, через который на маршрутизатор-получатель будет поступать зеркалированный трафик:

```
router(config)#interface gigabitethernet 0/3
router(config-if-gigabitethernet0/3)#switchport mode trunk
router(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 20
```

Настройка LAN-порта на маршрутизаторе-получателе, из которого зеркалированный трафик будет выдаваться в сторону системы мониторинга:

```
router(config)#interface gigabitethernet 0/2
router(config-if-gigabitethernet0/2)#switchport mode hybrid
router(config-if-gigabitethernet0/2)#exit
```

Настройка сессии RSPAN на маршрутизаторе-получателе. Указание RSPAN VLAN в качестве источника сессии и выходного LAN-порта в качестве назначения сессии:

```
router(config)#monitor session 1 source remote vlan 20
router(config)#monitor session 1 destination interface gigabitethernet 0/2
```

15.5 DDMI

Просмотр текущих параметров оптического интерфейса:

```
router#show optical interface gigabitethernet 3
Name              VendorName  LaserWaveLen(nm)  Temperature(C) Voltage(V) TxPower(dBm) RxPower(dBm)
-------------------------------------------------------------------------------------------------
gigabitethernet3  Zelax       1310              30.375000      3.332700   -6.882462    -6.358243
```