Зелакс ММ

Краткое руководство по настройке
ММ-41xx

© 1998 — 2021 Zelax. Все права защищены.

Редакция 02 от 30.11.2021 г.
ПО 7.5.3.14

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 маршрутизаторов MM-4102 и MM-4112, а также для пояснения содержания и использования основных команд, обеспечивающих необходимую настройку аппаратуры.

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	-
Привилегированный	в пользовательском режиме выполнением команды enable	router#	Доступны команды мониторинга и настройки, а также режимы конфигурирования	командой exit
Конфигурирования общесистемных параметров	в привилегированном режиме выполнением команды configure terminal	router(config)#	Доступны команды настройки общесистемных параметров	командой exit
Конфигурирования интерфейсов	в режиме 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	в режиме конфигурирования общесистемных параметров выполнением команды ip dhcp pool <name>	router(dhcp-name-config)#	Доступны команды настройки параметров пула dhcp	командой exit
Настройки списков доступа	в режиме конфигурирования общесистемных параметров выполнением команды ip access-list {standard | extended} <name>	router(config-std-nacl)# или router(config-ext-nacl)#	Доступны команды настройки параметров стандартного и расширенного списков доступа	командой exit
Настройки маршрутизации RIP	в режиме конфигурирования общесистемных параметров выполнением команды router rip | router ipv6 rip	router(config-rip)#	Доступны команды настройки параметров протокола маршрутизации RIP	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;
- ключевые слова выделяются жирным шрифтом.

Для исполнения набранной команды необходимо нажать клавишу “Enter”.

Для получения контекстной справки используется символ “?”.

При нажатии клавиши табуляции “Tab” происходит автоматическое доопределение 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
    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
    language             Set help information language
    logout               Exit from EXEC shell
    ping                 Send echo messages
    set                  Command set
    show                 Command show
    telnet               Open a telnet connection
    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 master MPU file system
    ftp                  Copy from ftp: file system
    ftps                 Copy from ftps: file system
    running-config       Copy from running configuration
    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, выводимые при работе с командной строкой

Сообщение об ошибке	Описание ошибки
Invalid input detected at '^' marker	Введенная команда не существует, либо имеется ошибка в области значений параметра, его формате или типе
Type "?" for a list of subcommands	Возможно не менее двух интерпретаций введенной команды

3 Базовые параметры

3.1 Текущая конфигурация и версия устройства

Отображение текущей конфигурации устройства.

```
router#show running-config
Building Configuration...done

! Current configuration : 1851 bytes
!
! Last configuration change at UTC Tue Aug 17 21:30:34 2021
! Flash config last updated at UTC Tue Aug 17 21:07:38 2021
! Configuration version 0.1
!

!software version 7.5.3.16(R)(integrity)
!software image file flash0: /flash/rp34-7.5.3.16(R).pck
!compiled on Jun 28 2019, 14:25:15

hostname router

exception reboot all
exception reboot

ip ctrl-protocol unicast
ip ctrl-protocol multicast

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

vlan 1
 exit

!slot_0_3_24GE
interface gigabitethernet0/0
 exit
interface gigabitethernet0/1
 exit
interface gigabitethernet0/2
 exit
interface gigabitethernet0/3
 exit
interface gigabitethernet0/4
 exit
interface gigabitethernet0/5
 exit
interface gigabitethernet0/6
 exit
interface gigabitethernet0/7
 exit
interface gigabitethernet0/8
 exit
interface gigabitethernet0/9
 exit
interface gigabitethernet0/10
 exit
interface gigabitethernet0/11
 exit
interface gigabitethernet0/12
 exit
interface gigabitethernet0/13
 exit
interface gigabitethernet0/14
 exit
interface gigabitethernet0/15
 exit
interface gigabitethernet0/16
 exit
interface gigabitethernet0/17
 exit
interface gigabitethernet0/18
 exit
interface gigabitethernet0/19
 exit
interface gigabitethernet0/20
```

```
 exit
interface gigabitethernet0/21
 exit
interface gigabitethernet0/22
 exit
interface gigabitethernet0/23
 exit
!end

!slot_0_1_4GE

interface gigabitethernet0
 media-type auto
 exit

interface gigabitethernet1
 media-type auto
 exit

interface gigabitethernet2
 media-type auto
 exit

interface gigabitethernet3
 media-type auto
 exit

!end

interface null0
 exit

!end
```

Текущая версия программного обеспечения и аппаратная ревизия устройства.

```
router#show version
               Operating System Software
MM-4112-AC220(V1)   system   image   file   (flash0:   /flash/rp34-7.5.3.16(R).pck),   version
7.5.3.16(R)(integrity), Compiled on Jun 28 2019, 14:25:15
Copyright(C)2019 OOO NPP Zelax

MM-4112-AC220(V1) Version Information
        System ID           : 001a81018068
        Hardware Model      : MM-4112-AC220(V1) with 1024 MBytes SDRAM, 8192 MBytes flash
        Hardware Version    : 002(Hotswap Supported)
        MPU CPLD Version    : 105
        Bootloader Version  : 1.21
        Software Version    : 7.5.3.16(R)(integrity)
        Software Image File : flash0: /flash/rp34-7.5.3.16(R).pck
        Compiled            : Jun 28 2019, 14:25:15

System Uptime is 0 hour 40 minutes 9 seconds
```

3.2 Имя устройства

Задание имени устройства.

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

4 Функции управления.

4.1 Учетные записи

Создание учетной записи для доступа к коммутатору с нешифрованным паролем и уровнем привилегий 15.

```
router(config)#username Zelax privilege 15 password 0 zelax
```

4.2 Telnet

Включение доступа к коммутатору по протоколу telnet. Доступ включен по-умолчанию.

```
router(config)#telnet server enable
```

4.3 SSH

Включение доступа к коммутатору по протоколу SSH. Доступ выключен по-умолчанию.

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

4.4 SNMPv2

Настройка доступа к маршрутизатору по протоколу SNMP v2c.

Включение SNMP-сервера на коммутаторе.

```
router(config)#snmp-server start
```

Задание значений community для доступа на чтение и запись.

```
router(config)#snmp-server community public ro
router(config)#snmp-server community private rw
```

Разрешение отправки trap-сообщений, указание IP-адреса назначения и соответствующего community.

```
router(config)#snmp-server enable traps
router(config)#snmp-server host 192.168.0.131 version 2
router(config)#snmp-server host 192.168.0.131 community public
```

Результирующий пример минимально необходимых настроек протокола SNMP.

```
snmp-server start
snmp-server community public ro
snmp-server community private rw
snmp-server enable traps
snmp-server host 192.168.0.105 version 2
snmp-server host 192.168.0.105 community public
```

4.5 SNMPv3

Пример настройки SNMPv3 с аутентификацией, но без шифрования.

```
router(config)#snmp-server start
router(config)#snmp-server view TESTVIEW 1 include
router(config)#snmp-server group TESTGROUP v3 authnopriv read TESTVIEW write TESTIIEW notify
TESTVIEW
router(config)#snmp-server user TESTUSER TESTGROUP v3 auth md5 TESTPASS
router(config)#snmp-server context public
router(config)#snmp-server enable traps
router(config)#snmp-server host 192.168.0.131 version 3 user TESTUSER authnopriv
```

5 Функционал L2.

Настройка функционала L2 возможна только на bridge group и на LAN портах маршрутизатора.

5.1 Переключение режима порта WAN/LAN

Перевод порта WAN в режим LAN.

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

Перевод порта LAN в режим WAN.

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

Изменение VLAN, к которому принадлежит порт.

5.2 Объединение L3 интерфейсов в bridge group

Объединение L3 интерфейсов в bridge group позволяет прозрачно пересылать кадры Ethernet между разными WAN портами в одной группе.

Добавление WAN портов в bridge-group 1.

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

5.3 VLAN

5.3.1 Access

Перевод порта в режим access.

```
router(config-if-gigabitethernet1/0/1)#switchport mode access
```

Изменение VLAN, к которому принадлежит порт.

```
router(config-if-gigabitethernet1/0/1)#switchport access vlan 10
```

5.3.2 Trunk

Перевод порта в режим trunk.

```
router(config-if-gigabitethernet1/0/1)#switchport mode trunk
```

При переводе в этот режим на порту разрешается передача всех VLAN, созданных на коммутаторе. Для ограничения этих VLAN необходимо использовать allowed list.

```
router(config-if-gigabitethernet1/0/1)#switchport trunk allowed vlan 10,20-30,100
```

По-умолчанию все нетегированные кадры, пришедшие на этот порт, тегируются меткой VLAN 1. Изменение native vlan.

```
router(config-if-gigabitethernet1/0/1)#switchport trunk pvide vlan 50
```

5.4 xSTP

5.4.1 Выбор протокола xSTP

Включение протоколов связующего дерева.

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

После ввода данной команды включается протокол MSTP. Его можно изменить. Для конфигурации на коммутаторах доступны несколько протоколов связующего дерева.

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

5.4.2 Настройка таймеров xSTP

Настройка hello-интервала.

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

Настройка forward delay.

```
router(config)#spanning-tree mst forward-time 30
```

Настройка «времени жизни».

```
router(config)#spanning-tree mst max-age 40
```

5.4.3 Настройка приоритета xSTP

Настройка приоритета коммутатора для instance 0 в STP.

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

5.4.4 Настройка стоимости интерфейсов

Изменение стоимости интерфейса.

```
router(config-if-gigabitethernet0/10)#spanning-tree mst instance 0 cost 2000
```

5.4.5 Настройка instance в MSTP

До этой настройки на коммутаторе созданы VLAN 10,20-30. Размещение по instance указано ниже.

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

5.4.6 BPDU guard

Настройка BPDU guard.

```
router(config-if-gigabitethernet0/10)#spanning-tree bpdu guard
```

5.4.7 Root guard

Включение Root guard на интерфейсе ethernet1/0/10.

```
router(config-if-gigabitethernet0/10)#spanning-tree guard root
```

5.5 Агрегирование каналов

5.5.1 Создание link-aggregation group

Создание link-aggregation group в глобальном режиме конфигурации, с выбором режима работы LACP или без протокола согласования.

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

5.5.2 Без протоколов согласования

Данную настройку стоит производить с обеих сторон для исключения возникновения петли.

```
router(config)#interface gigabitethernet 0/6,0/7
router(config-if-range)#link-aggregation 1 manual
```

5.5.3 LACP

При использовании данного протокола автосогласования, порты первого коммутатора переводятся в режим активного согласования параметров.

```
router(config)#interface gigabitethernet 0/6,0/7
router(config-if-range)#link-aggregation 1 active
```

Порты второго коммутатора переводятся в режим пассивного ожидания.

```
router(config)#interface gigabitethernet 0/6,0/7
router(config-if-range)#link-aggregation 2 passive
```

5.5.4 Балансировка нагрузки

Балансировка потоков может производиться на основании разных параметров. В зависимости от местоположения и потребностей необходимо выбирать наиболее подходящий.

```
router(config)#link-aggregation 2 load-balance dst-ip|dst-mac|dst-src-ip
|dst-src-mac|src-ip|src-mac
```

5.6 LLDP

5.6.1 Базовая настройка

Протокол необходимо включать как глобально, так и непосредственно на инерфейсе.

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

5.6.2 Настройка передаваемых TLV

Можно настроить несколько типов передаваемых TLV.

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

Для передачи IP-адреса управления необходимо добавить команду.

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

6 Функции безопасности L2

6.1 DHCP snooping

Для настройки dhcp snooping необходимо включить данную функцию глобально.

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

Интерфейс, подключенный к DHCP-серверу, необходимо перевести в доверенный режим.

```
router(config)#interface gigabitethernet 1/0/11
router(config-if-gigabitethernet0/10)#dhcp snooping trust
```

Включение передачи опции 82.

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

6.2 ARP inspection

Данная функция работает в паре с dhcp snooping. Настройка arp inspection на определенном интерфейсе.

```
router(config)#interface gigabitethernet 0/6
router(config-if-gigabitethernet0/6)#ip arp inspection
```

6.3 Loopback detection

Включение функции Loopback detection в VLAN 1 и настройка блокировки порта, при обнаружении петли.

```
router(config)#loopback-detection enable
router(config)#interface gigabitethernet 0/1
router(config-if-gigabitethernet0/1)#loopback-detection enable control
```

6.4 Storm-control

Ограничение количества broadcast и multicast пакетов на интерфейсе 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
```

6.5 Port-isolate

При использовании функции port-isolate порты, входящие в одну группу изоляции, не могут обмениваться данными между собой.

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

7 Списки контроля доступа

7.1 Standard ACL

Для указания адреса источника можно использовать как единичный хост, так и определенные подсети.

```
router(config)#access-list 10 permit host 192.168.0.10
router(config)#access-list 10 permit 192.168.0.128 0.0.0.127
router(config)#access-list 10 deny any
```

7.2 Extended ACL

Расширенные списки доступа можно использовать как нумерованные

```
router(config)#access-list 1002 permit tcp any host 192.168.100.100 range 10000 20000
```

так и именованные.

```
router(config)#ip access-list extended ICMP
router(config-ext-nacl)#permit icmp any host 192.168.100.100
```

8 NAT

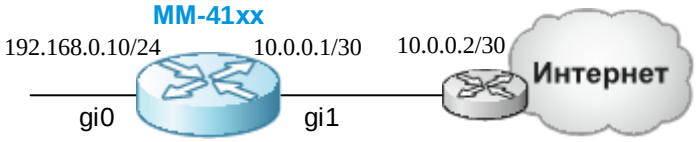

Рис. 1 Пример схемы применения NAT

8.1 Настройка ролей интерфейсов

Настройка WAN порта в роли внутреннего интерфейса.

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

Настройка WAN порта в роли внешнего интерфейса.

```
router(config)#interface gigabitethernet1
router(config-if-gigabitethernet0)#ip nat outside
```

8.2 Настройка Static NAT

Статический NAT позволяет преобразовать частный ip-адрес локальной сети 192.168.0.1 в публичный ip-адрес настроенный на WAN порту маршрутизатора 10.0.0.1.

```
router(config)#ip nat inside source static 192.168.0.1 10.0.0.1
```

8.3 Настройка Dynamic NAT

Динамический NAT позволяет преобразовать определенный диапазон локальных ip-адресов в определенный диапазон публичных адресов.

Создаем пул адресов с именем pool1, в котором указаны публичные ip-адреса:

```
router((config)#ip nat pool pool1 10.0.0.1 10.0.0.2 netmask 255.255.255.0
```

Создаем расширенный список доступа 1001, в котором указываем диапазон локальных адресов, которые будут преобразованы в публичные адреса из ранее созданного pool1:

```
router(config)#ip access-list extended 1001
router(config-ext-nacl)#permit ip 192.168.0.0 0.0.0.255 any
```

Применяем правило динамического NAT:

```
router((config)#ip nat inside source list 1001 pool pool1
```

8.4 Настройка PAT

Данный тип NAT позволяет преобразовать определенный диапазон локальных ip-адресов в определенный публичный ip-адрес.

Создаем пул адресов с именем pool1, в котором указан публичный ip-адрес:

```
router((config)#ip nat pool pool1 10.0.0.1 10.0.0.1 netmask 255.255.255.0
```

Создаем расширенный список доступа 1001, в котором указываем диапазон локальных адресов, которые будут преобразованы в публичный адрес из ранее созданного pool1:

```
router(config)#ip access-list extended 1001
router(config-ext-nacl)#permit ip 192.168.0.0 0.0.0.255 any
```

Применяем правило PAT:

```
router((config)#ip nat inside source list 1001 pool pool1 overload
```

9 Quality of Service

9.1 Классификация

Пример классификации по номеру VLAN.

```
router(config)#class-map TEST
router(config-cmap)#match vlan 200
```

9.2 Маркировка

Маркировка трафика, соответствующего классу TEST.

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

9.3 Политики

Применение политики на WAN интерфейсе.

```
router(config)#int gigabitethernet 0
router(config-if-gigabitethernet0)#service-policy input MARK
```

Применение политики на LAN интерфейсе.

```
router(config)#int vlan 100
router(config-if-vlan100)#service-policy input MARK
router(config-if-vlan100)#exit
router(config)#int gigabitethernet 0/10
router(config-if-gigabitethernet0/10)#switchport access vlan 100
```

10 Функционал AAA

10.1 TACACS+

Выбор способа аутентификации.

```
router(config)#aaa new-model
router(config)#aaa authentication login TEST tacacs
```

Указание сервера tacacs и ключа.

```
router(config)#tacacs-server host 192.168.0.100 key 0 testkey
```

10.2 RADIUS

Выбор способа аутентификации.

```
router(config)#aaa new-model
router(config)#aaa authentication login TEST radius
```

Указание RADIUS-серверов и ключа.

```
router(config)#radius-server host 192.168.0.100 key 0 testkey
```

11 Функционал L3

11.1 Interface VLAN

Для каждого VLAN можно создать L3-интерфейс и присвоить ему IP-адрес.

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

11.2 Interface BVI

Интерфейс BVI – это виртуальный L3 интерфейс Ethernet, который используется для маршрутизации трафика из bridge-group с соответствующим номером.

```
router(config)# interface bvi 1
router(config-if-bvi1)#ip address 192.168.1.1 255.255.255.0
```

11.3 VRRP

Настройка виртуального IP-адреса и VLAN, который будет участвовать в протоколе VRRP.

```
router(config)#interface gigabitethernet 0
router(config-if-gigabitethernet0)#ip address 10.0.0.1 255.255.255.0
router(config-if-gigabitethernet0)#vrrp 1 ip 10.0.0.5
router(config-if-gigabitethernet0)#vrrp 1 priority 110
```

Верификация настроек.

```
router#show vrrp
Interface gigabitethernet0 (Flags 0x0)
  Pri-addr : 10.0.0.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.0.0.5
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:10.0.0.1/24
    State : Init
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None
```

11.4 Статическая маршрутизация

Создание статического маршрута.

```
router (config)#ip route 172.16.0.0 255.255.0.0 192.168.10.4
```

11.5 RIP

Минимальная настройка.

```
router(config)#router rip
router(config-rip)#network 192.168.5.0
```

Указание определенного соседа. При данной настройке служебные сообщения будут отправляться на unicast адрес соседа.

```
router(config-rip)#neighbor 192.168.10.99
```

11.6 OSPF

Для настройки OSPF достаточно указать сети, которые будут анонсироваться.

```
router(config)#router ospf 100
router(config-ospf)#network 192.168.20.0 0.0.0.255 area 0
```

Для отключения отправки служебных сообщений на определенный интерфейс указывается пассивный интерфейс.

```
router(config-ospf)#passive-interface gigabitethernet 2
router(config-ospf)#passive-interface vlan 100
```

11.7 BGP

Указание соседа в протоколе BGP.

```
router(config)#router bgp 3000
router(config-bgp)#neighbor 192.168.100.100 remote-as 3500
```

Указание анонсируемых сетей.

```
router(config-bgp)#network 10.200.200.0 255.255.255.0
```

11.8 Таблица маршрутизации

Просмотр таблицы маршрутизации.

```
router#sh ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   10.0.0.0/24 [20/1] via 200.0.0.1, 00:06:52, gigabitethernet1
OE  10.0.1.0/24 [150/20] via 192.168.1.6, 00:00:00, vlan4
C   127.0.0.0/8 is directly connected, 19:34:18, lo0
B   192.168.1.0/30 [20/0] via 200.0.0.1, 00:06:52, gigabitethernet1
C   192.168.1.4/30 is directly connected, 01:07:38, vlan4
C   200.0.0.0/30 is directly connected, 00:10:03, gigabitethernet1
B   172.16.0.99/32 [20/1] via 200.0.0.1, 00:06:52, gigabitethernet1
OE  172.16.0.199/32 [150/20] via 192.168.1.6, 01:00:09, vlan4
C   172.16.0.200/32 is directly connected, 01:09:16, loopback1
```

12 VPN

12.1 Настройка туннеля GRE

Рис. 2 Пример схемы применения туннеля GRE

Для настройки туннеля GRE нужно выполнить следующие настройки:

```
router(config)#interface tunnel 1
router(config-if-tunnel1)#tunnel source 10.0.12.1
router(config-if-tunnel1)#tunnel destination 10.0.23.1
router(config-if-tunnel1)#ip address 192.168.0.1 255.255.255.0
```

На маршрутизаторе с противоположной стороны выполняются аналогичные настройки.

12.2 Настройка туннеля IPsec

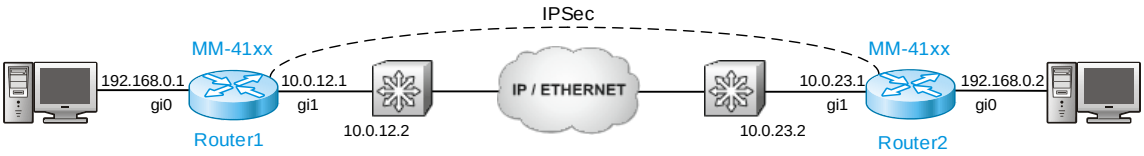

Рис. 3 Пример схемы применения туннеля IPsec

Настройка предложения IKE с именем «ikepro» с использованием алгоритма шифрования 3DES и аутентификации MD5

```
Router1(config)#crypto ike proposal ikepro
Router1(config-ike-prop)#encryption 3des
Router1(config-ike-prop)#integrity md5
```

Настройка предложения IPsec с именем «ippro» , с использованием алгоритма шифрования 3DES и аутентификации MD5

```
Router1(config)#crypto ip proposal ippro
Router1(config-ipsec-prop)#esp 3des md5
Router1(config-ipsec-prop)#exit
```

Настройка предопределенного ключа pre-share key

```
Router1(config)#crypto ike key admin any
```

Настройка IPsec туннеля

```
Router1(config)#crypto tunnel tun
Router1(config-tunnel)#local address 10.0.12.1
Router1(config-tunnel)#peer address 10.0.23.1
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
```

На маршрутизаторе с противоположной стороны выполняются аналогичные настройки.

12.3 Настройка L2TP

L2TP (Layer 2 Tunneling Protocol) - является одной из технологий VPDN. Технология VPDN (Virtual Private Dial-up Network) предоставляет услуги подключения для удаленных пользователей, которые подключаются к корпоративной сети через интернет-провайдера.

L2TP для построения туннеля использует два типа устройств VPDN: LAC (L2TP Access Concentrator) и LNS (L2TP Network Server). Когда пользователь запрашивает удаленное соединение, LAC инициирует туннельное соединение L2TP с LNS.

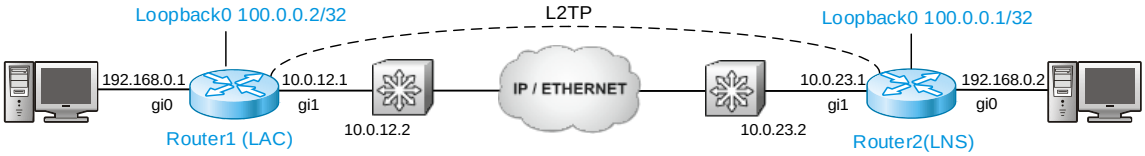

Рис. 4 Пример схемы применения туннеля L2TP

Настройка маршрутизатора Router 1 в роли LAC:

Настройка шаблона pseudowire с именем «l2tp-1», используя инкапсуляцию l2tpv2, локальное имя «lac» и пароль «vpdntun»

```
Router1(config)#pseudowire-class l2tp-1
Router1(config-pw-class)#encapsulation l2tpv2
Router1(config-pw-class)#password 0 vpdntun
Router1(config-pw-class)#hostname lac
Router1(config-pw-class)#ip local interface gigabitethernet1
Router1(config-pw-class)#exit
```

Настройка виртуального интерфейса virtual-ppp0 с инкапсуляцией протокола PPP, аутентификацией PAP и отправляемым именем «admin» и паролем «lac»

```
Router1(config)#interface virtual-ppp0
Router1(config-if-virtual-ppp0)#encapsulation ppp
Router1(config-if-virtual-ppp0)#ip address negotiated
Router1(config-if-virtual-ppp0)#ppp pap sent-username admin password 0 lac
Router1(config-if-virtual-ppp0)#pseudowire 10.0.23.1 1 pw-class l2tp-1
Router1(config-if-virtual-ppp0)#exit
```

Настройка исходящего интерфейса virtual-ppp0 для маршрута по умолчанию

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 virtual-ppp0
```

Настройка маршрутизатора Router 2 в роли LNS:

Настройка аутентификации PPP с именем пользователя «admin» и паролем «lac»

```
Router2#configure terminal
Router2(config)#user admin password 0 lac
```

Настройка виртуального шаблона virtual-template 0 с аутентификацией PAP

```
Router2(config)#interface virtual-template 0
Router2(config-if-virtual-template0)#encapsulation ppp
Router2(config-if-virtual-template0)#ip unnumber loopback0
Router2(config-if-virtual-template0)#peer default ip address 100.0.0.2
Router2(config-if-virtual-template0)#ppp authentication pap
```

Включаем VPDN. Настраиваем VPDN группу с именем «lns» и разрешением принимать запросы удаленного доступа.

```
Router2(config)#vpdn enable
Router2(config)#vpdn-group lns
Router2(config-vpdn)#accept-dialin
Router2(config-vpdn-acc-in)#protocol l2tp
Router2(config-vpdn-acc-in)#virtual-template 0
```

Настройка пароля «vpdntun» для обмена между LAC и LNS

```
router(config-vpdn)#local name lns
router(config-vpdn)#l2tp tunnel password vpdntun
```

13 Функции диагностики

13.1 Локальный журнал событий

По-умолчанию во flash журналируются события с уровнем notifications. Изменение этого уровня.

```
router(config)#logging file ?
    <0-7>                Logging severity level
    alerts               Immediate action needed           (severity=1)
    critical             Critical conditions               (severity=2)
    debugging            Debugging messages                (severity=7)
    emergencies          System is unusable                (severity=0)
    errors               Error conditions                  (severity=3)
    informational        Informational messages            (severity=6)
    max-size             Set max-size parameters
    notifications        Normal but significant conditions (severity=5)
    warning              Report Warning when logging file size reached warning
                         threshold
    warnings             Warning conditions                (severity=4)
```

Возможные уровни журналирования: critical, debugging, informational, warnings, notifications, errors, emergencies.

Просмотр локального журнала событий.

```
router#show logging file
```

13.2 Syslog

Настройка удаленного сервера журналирования.

```
router(config)#logging 192.168.2.100
```

Изменения адреса отправителя.

```
router(config)#logging source-ip 13.13.13.13
```

13.3 Зеркалирование трафика

Зеркалирование трафика в пределах одного маршрутизатора. Зеркалирование трафика можно включить только на LAN портах.

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

13.4 DDMI

Просмотр текущих параметров оптического интерфейса.

```
router#show optical interface gigabitethernet 1

Name                          VendorName       LaserWaveLen(nm) Temperature(C)   Voltage(V)   TxPower(dBm) RxPower(dBm)
 ------------------------------------------------------------------------------------------------------------------------
 gigabitethernet1              Zelax            1310             48.937500        3.281600     -6.013657    -9.514095
```

14 MPLS

14.1 LDP

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

Глобальное включение LDP.

```
router(config)#mpls ldp
```

Назначение идентификатора.

```
router(config-ldp)#router-id 1.1.1.1
router(config-ldp)#transport-address 1.1.1.1
```

Включение LDP на определенном интерфейсе.

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

14.2 MPLS adjacency

Включение MPLS глобально.

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

Включение MPLS на определенном интерфейсе.

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

14.3 VRF

Создание VRF.

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

Назначение порта в определенный VRF.

```
router(config-if-gigabitethernet1)#ip vrf forwarding NAME_OF_VRF
```

14.4 L2VPN

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

14.4.1 VPWS

При создании L2VPN через несколько MPLS устройств необходимо указывать IP-адрес целевого устройства, с которым будет установлено соседство по протоколу LDP.

```
router(config)#interface gigabitethernet 1
router(config-if-gigabitethernet0)#mpls ip
router(config-if-gigabitethernet0)#xconnect 3.3.3.3 1 encapsulation mpls
```

Просмотр состояния VPWS.

```
MM-4112#show mpls ldp l2-circuit
VC-ID           Interface                  State                 Type            Local-Label
Remote-Label   Destination-Address
1               gigabitethernet1         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 машрутизатор выступает в роли концентратора для остальных устройств, на которых настраивается VPWS.

Создание VPLS инстанса.

```
router(config)#mpls vpls 1
router(config)#vpn-id 1
```

```
router(config)#peer 2.2.2.2 tagged
router(config)#peer 4.4.4.4 tagged
```

Привязка определенного интерфейса к VPLS.

```
router(config)#interface gigabitethernet 2
router(config-if-gigabitethernet2)#mpls ip
router(config-if-gigabitethernet2)#mpls vpls 1 vlan
```

Просмотр состояния VPLS

```
MM-4102#show mpls ldp vpls
VPLS-ID     Peer Address      State             Type       Local-MTU   Remote-MTU  Label-Sent
Label-Rcvd
1             2.2.2.2            Up                  tag         1500         1500         16
16
1             4.4.4.4            Up                  tag         1500         1500         20
1281
Statistics for ldp vpls:
    LDP VPLS up: 2
    LDP VPLS down: 0
```

14.5 L3VPN

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

Создание VRF.

```
router(config)#ip vrf 1
```

Назначение Route Distinguisher и Route Target.

```
router(config-vrf)#rd 100:1
router(config-vrf)#route-target import 100:1
router(config-vrf)#route-target export 100:1
```

Назначение интерфейсу определенного vrf.

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

Настройка MBGP.

```
router(config)#router bgp 65000
router(config-bgp)#neighbor 3.3.3.3 update-source lo
router(config-bgp)#neighbor 3.3.3.3 update-source loopback 0
router(config-bgp)#address-family vpnv4
router(config-bgp-af)#neighbor 3.3.3.3 activate
router(config-bgp-af)#neighbor 3.3.3.3 send-community both
router(config-bgp-af)#exit-address-family
router(config-bgp)#address-family ipv4 vrf 1
router(config-bgp-af)#redistribute connected
router(config-bgp-af)#redistribute ospf 2
router(config-bgp-af)#exit-address-family
```