

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
ИМЕНИ ПАТРИСА ЛУМУМБЫ

Факультет физико-математических и естественных наук
Кафедра теории вероятностей и кибербезопасности

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5

Дисциплина «Сетевые технологии»

Тема «Простые сети в GNS3. Анализ трафика»

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

МОСКВА

2023 г.

Цель работы

Построение простейших моделей сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, анализ трафика посредством Wireshark.

Выполнение работы

1. Моделирование простейшей сети на базе коммутатора в GNS3

1.1. Постановка задачи

1. Построить в GNS3 топологию сети, состоящей из коммутатора Ethernet и двух оконечных устройств.
2. Задать оконечным устройствам IP-адреса в сети 192.168.1.0/24. Проверить связь.

1.2. Выполнение

1. Запустила GNS3 VM и GNS3. Создала новый проект под названием «Lab_5».
2. В рабочей области GNS3 разместила коммутатор Ethernet и два VPCS. Изменила названия устройств в соответствии с требованиями. Соединила VPCS с коммутатором и отобразила обозначение интерфейсов соединения (рис. 1.1).

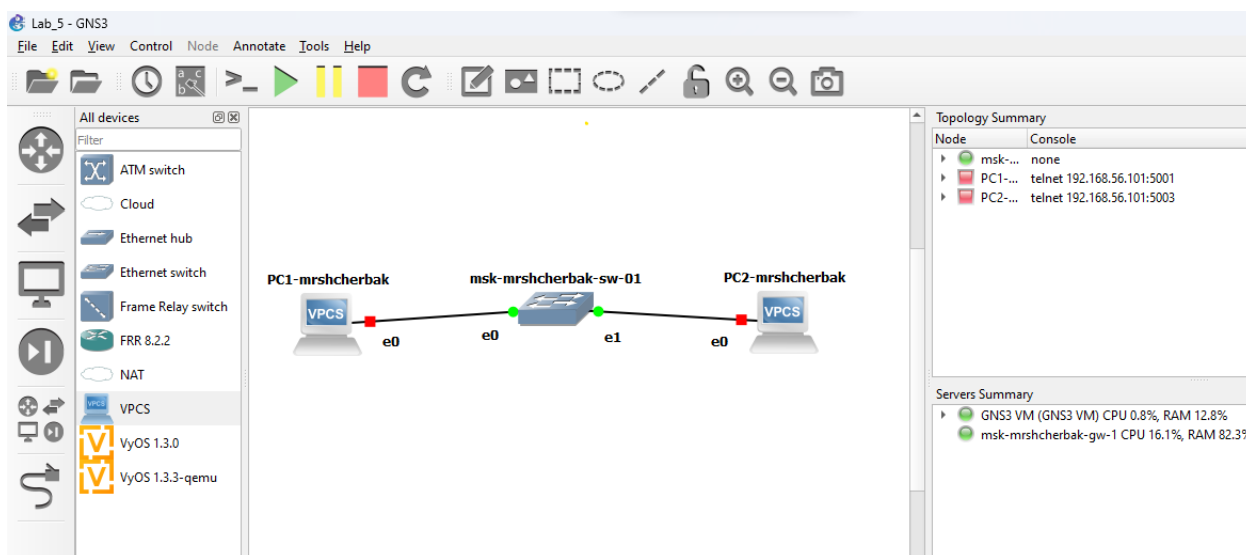
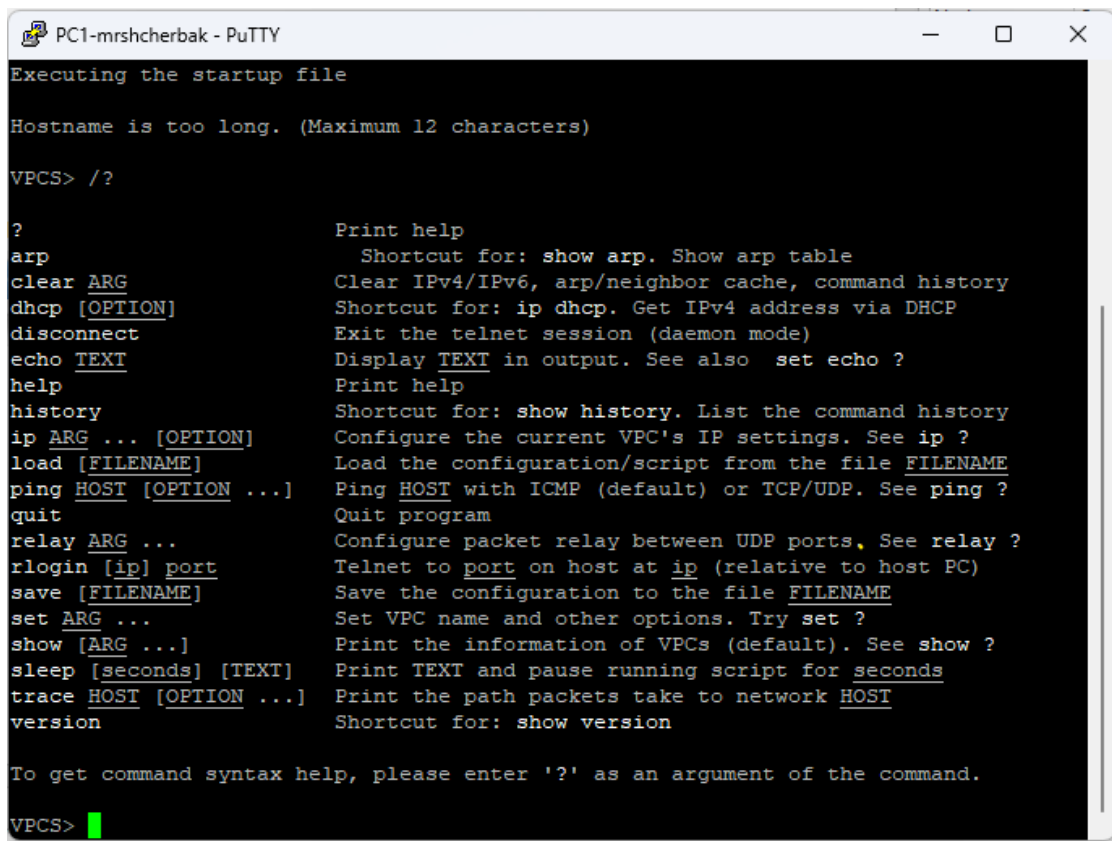


Рис.1.1. Топология простейшей сети в GNS3

3. Задала IP-адреса VPCS. Запустила PC-1, затем вызвала его терминал. Команда для просмотра синтаксиса возможных для ввода команд изображена на рис 1.2.



```
PC1-mrshcherbak - PuTTY
Executing the startup file
Hostname is too long. (Maximum 12 characters)
VPCS> /?

?                Print help
arp              Shortcut for: show arp. Show arp table
clear ARG        Clear IPv4/IPv6, arp/neighbor cache, command history
dhcp [OPTION]    Shortcut for: ip dhcp. Get IPv4 address via DHCP
disconnect       Exit the telnet session (daemon mode)
echo TEXT        Display TEXT in output. See also set echo ?
help             Print help
history          Shortcut for: show history. List the command history
ip ARG ... [OPTION] Configure the current VPC's IP settings. See ip ?
load [FILENAME]  Load the configuration/script from the file FILENAME
ping HOST [OPTION ...] Ping HOST with ICMP (default) or TCP/UDP. See ping ?
quit            Quit program
relay ARG ...    Configure packet relay between UDP ports. See relay ?
rlogin [ip] port Telnet to port on host at ip (relative to host PC)
save [FILENAME]  Save the configuration to the file FILENAME
set ARG ...      Set VPC name and other options. Try set ?
show [ARG ...]   Print the information of VPCs (default). See show ?
sleep [seconds] [TEXT] Print TEXT and pause running script for seconds
trace HOST [OPTION ...] Print the path packets take to network HOST
version          Shortcut for: show version

To get command syntax help, please enter '?' as an argument of the command.
VPCS> █
```

Рис.1.2. Просмотр синтаксиса возможных для ввода команд VPCS в GNS3

Для задания IP-адреса 192.168.1.11 в сети 192.168.1.0/24 ввела команду, представленную на рис.1.3, выполнена первой. Здесь 192.168.1.1 — адрес шлюза. Для сохранения конфигурации ввела команду save.

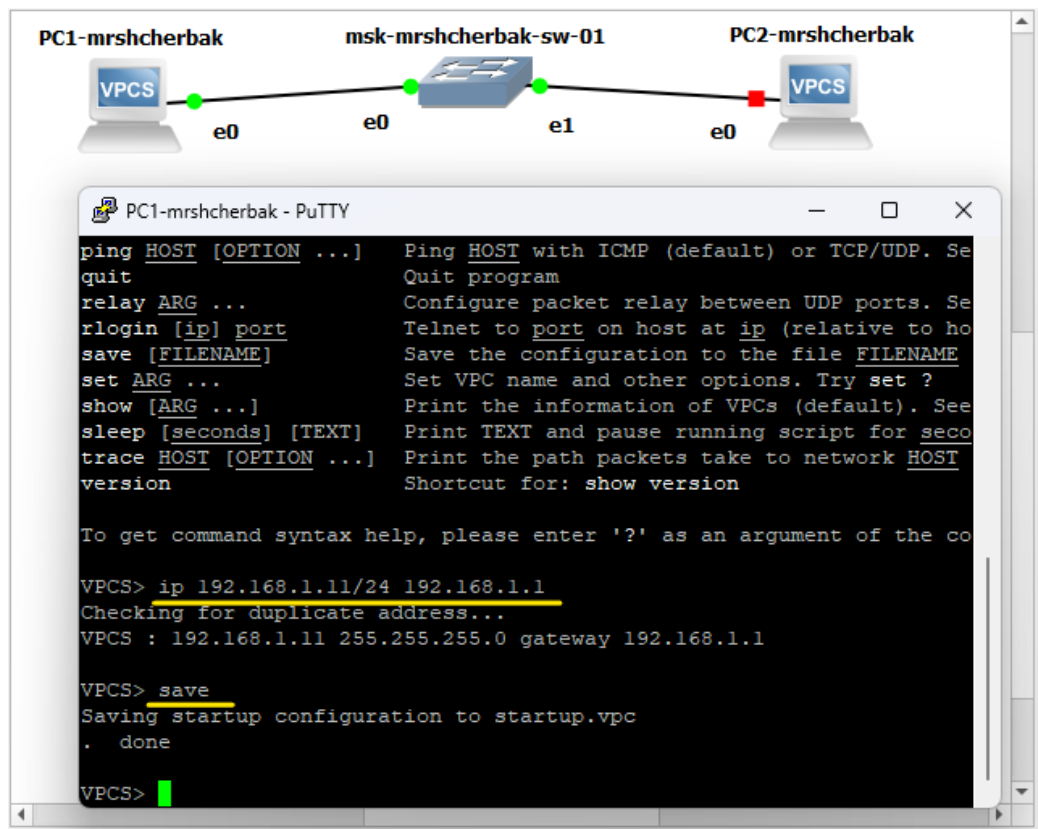


Рис.1.3. Задание IP-адреса и сохранение конфигурации VPCS в GNS3

Аналогичным образом задала IP-адрес 192.168.1.12 для PC-2 (рис.1.4).

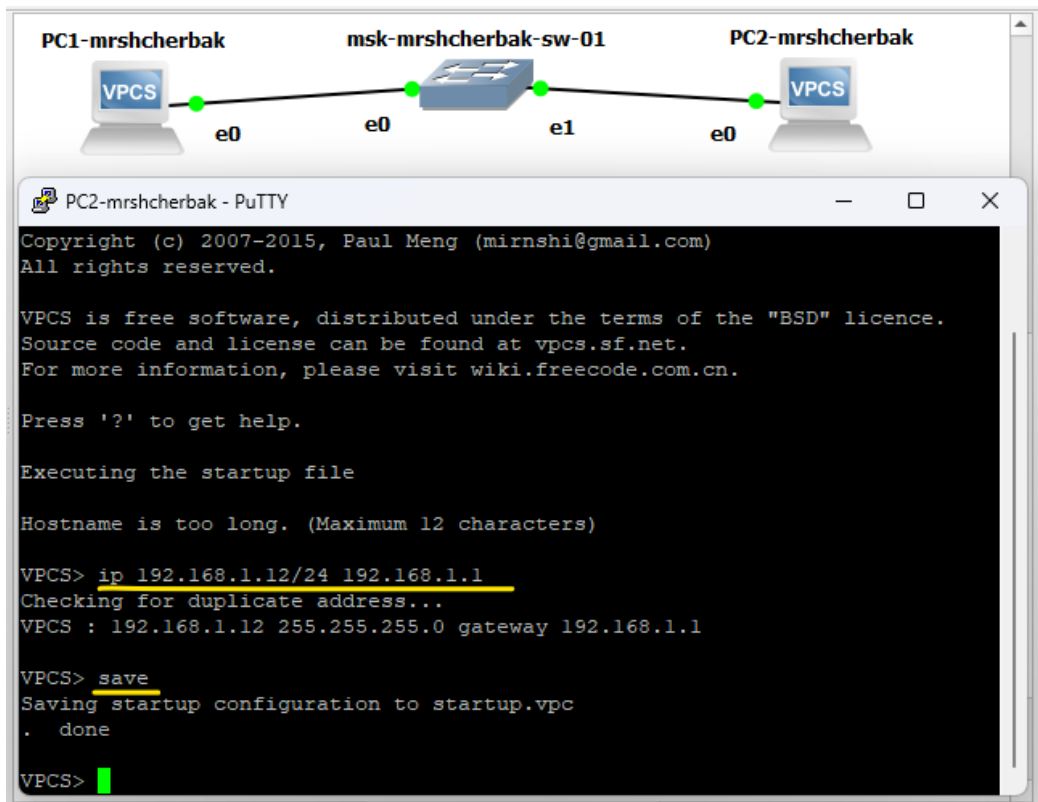


Рис.1.4. Задание IP-адреса и сохранение конфигурации VPCS в GNS3

4. Проверила работоспособность соединения между PC-1 и PC-2 с помощью команды ping (рис.1.5).

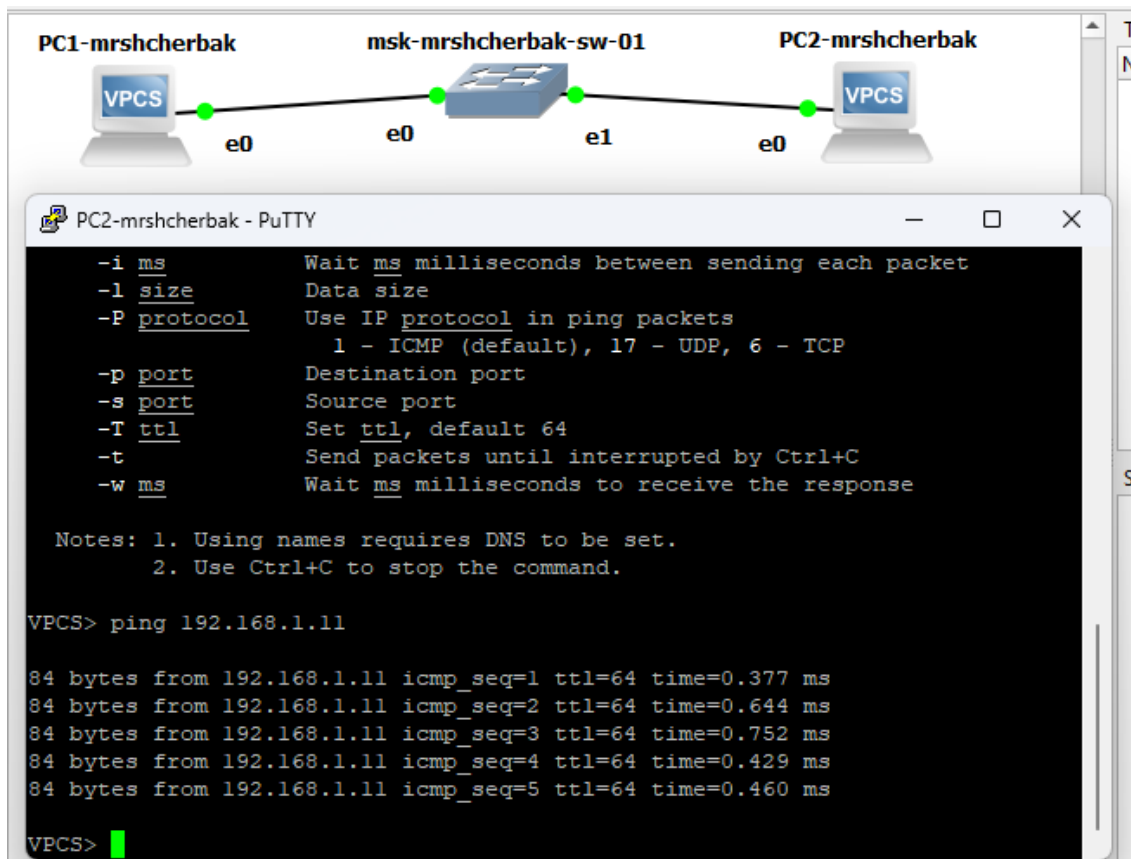


Рис.1.5. Проверка работоспособности соединения между PC-1 и PC-2

5. Остановила в проекте все узлы (рис.1.6).



Рис.1.6. Остановка всех узлов

2. Анализ трафика в GNS3 посредством Wireshark

2.1. Постановка задачи

1. С помощью Wireshark захватить и проанализировать ARP-сообщения.
2. С помощью Wireshark захватить и проанализировать ICMP-сообщения.

2.2. Выполнение

1. Запустила на соединении между PC-1 и коммутатором анализатор трафика (рис.2.1).
2. В проекте GNS3 стартовала все узлы. В окне Wireshark отобразилась информация по протоколу ARP (рис.2.2).



Рис.2.1. Запуск анализатора трафика на соединении между PC-1 и коммутатором

Изучила кадры данных протокола ARP (рис.2.2). Длина кадра = 64 байта. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (00:50:79:66:68:00) и назначения Destination — широковещательный адрес. В заголовке ARP основные поля — это Hardware type Ethernet канальный уровень, Protocol type IPv4 сетевой уровень, Hardware size 6 байт = 48 бит, Protocol size 4 байта = 32 бита, Opcode код операции — запрос. Мы видим разницу в типе адресов: Source Address индивидуальный и глобально администрируемый, а Destination Address групповой и локально администрируемый.

Lab5_Wireshark_next.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::2	ICMPv6	62	Router Solicitation
2	0.045061	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
3	1.045762	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
4	2.046071	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
5	51.912147	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
6	52.912941	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
7	53.913128	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
8	278.046281	::	ff02::16	ICMPv6	130	Multicast Listener Report Message v2

> Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0

▼ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Address: Broadcast (ff:ff:ff:ff:ff:ff)
.... ..1. = LG bit: Locally administered address (this is NOT the factory default)
.... ..1. = IG bit: Group address (multicast/broadcast)

▼ Source: Private_66:68:00 (00:50:79:66:68:00)
Address: Private_66:68:00 (00:50:79:66:68:00)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000
Frame check sequence: 0x00000000 [unverified]
[FCS Status: Unverified]

▼ Address Resolution Protocol (request/gratuitous ARP)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
[Is gratuitous: True]
Sender MAC address: Private_66:68:00 (00:50:79:66:68:00)
Sender IP address: 192.168.1.10
Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
Target IP address: 192.168.1.10

Рис.2.2. Информация по протоколу ARP

3. В терминале PC-2 посмотрела информацию по опциям команды ping, введя «ping /?» (рис.2.3). Затем сделала один эхо-запрос в ICMP-моду к узлу PC-1, один эхо-запрос в UDP-моду к узлу PC-1 и один эхо-запрос в TCP-моду к узлу PC-1. Выполнение данных эхо-запросов представлено на рис.2.4 соответственно.

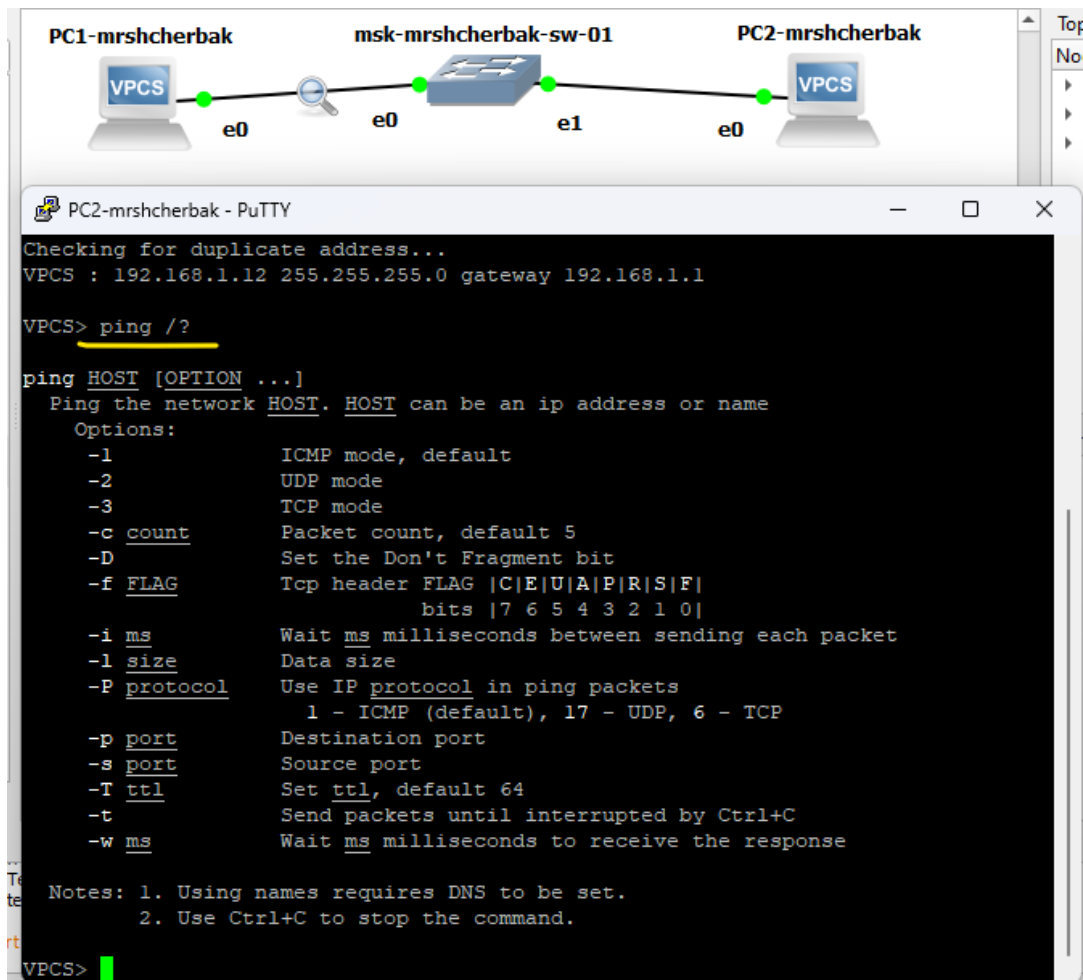


Рис.2.3. Просмотр информации по опциям команды ping

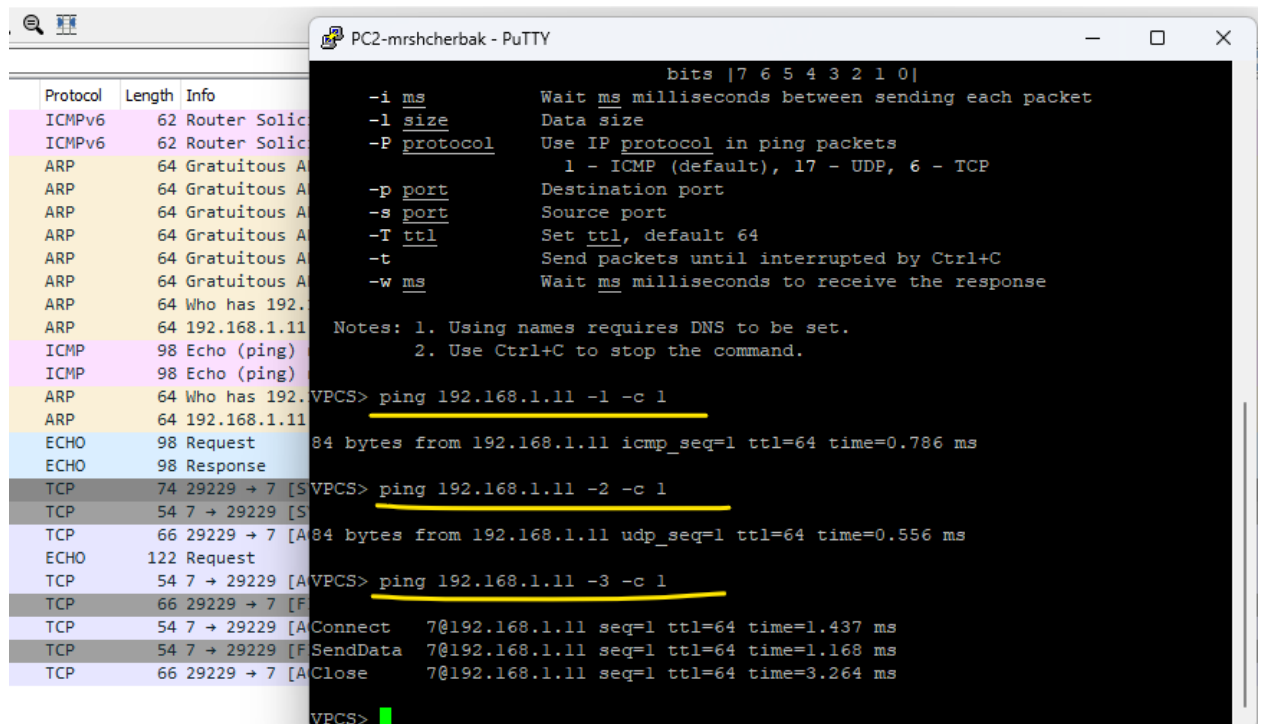


Рис.2.4. Выполнение команд

На панели списка пакетов выбрала указанный кадр ICMP — эхо-запрос (request) (рис.2.5). Изучила информацию на панели сведений о пакете. Длина кадра = 98 байт. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (00:50:79:66:68:01) и назначения Destination (00:50:79:66:68:00). MAC-адреса источника и назначения являются индивидуальными и глобально администрируемыми. Показан заголовок протокола сетевого уровня IPv4. Средний раздел содержит информацию о поле данных кадра. Данные содержат IPv4-адреса источника (192.168.1.12) и назначения (192.168.1.11). В заголовке ICMP основные поля — это type и code. Type говорит о том, что произошло в сети (Echo (ping) request). Во втором указанном кадре ICMP — эхо-ответе (reply) указаны IPv4-адреса источника (192.168.1.11) и назначения (192.168.1.12) наоборот по сравнению с эхо-запросом.

The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows several ICMP Router Solicitation and Gratuitous ARP packets, followed by an ICMP Echo (ping) request (packet 11) and its reply (packet 12). The packet details pane for packet 11 shows the Ethernet II header, the IPv4 header, and the ICMP Echo (ping) request structure.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::2	ICMPv6	62	Router Solicitation
2	0.005923	::	ff02::2	ICMPv6	62	Router Solicitation
3	0.050086	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
4	0.056763	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
5	1.051820	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
6	1.058862	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
7	2.052776	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
8	2.059684	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
9	702.768083	Private_66:68:01	Broadcast	ARP	64	Who has 192.168.1.11? Tell 192.168.1.12
10	702.768395	Private_66:68:00	Private_66:68:01	ARP	64	192.168.1.11 is at 00:50:79:66:68:00
11	702.769309	192.168.1.12	192.168.1.11	ICMP	98	Echo (ping) request id=0xcd34, seq=1/256, ttl=64 (reply in 12)
12	702.769753	192.168.1.11	192.168.1.12	ICMP	98	Echo (ping) reply id=0xcd34, seq=1/256, ttl=64 (request in 11)

Packet 11 details:

- Frame 11: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
- Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)
 - Destination: Private_66:68:00 (00:50:79:66:68:00)
 - Address: Private_66:68:00 (00:50:79:66:68:00)
 - = LG bit: Globally unique address (factory default)
 - = IG bit: Individual address (unicast)
 - Source: Private_66:68:01 (00:50:79:66:68:01)
 - Address: Private_66:68:01 (00:50:79:66:68:01)
 - = LG bit: Globally unique address (factory default)
 - = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.11
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84
 - Identification: 0x34cd (13517)
 - > 0000 = Flags: 0x0
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 64
 - Protocol: ICMP (1)
 - Header Checksum: 0xc274 [validation disabled]
 - [Header checksum status: Unverified]

Рис.2.5. Сведения об эхо-запросе в ICMP-моду к узлу PC-1

Проанализировала полученную информацию от одного эхо-запроса в UDP-моду к узлу PC-1. Длина кадра Request = 98 байт. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (00:50:79:66:68:01) и назначения Destination (00:50:79:66:68:00). MAC-адреса

источника и назначения являются индивидуальными и глобально администрируемыми. Показан заголовок протокола сетевого уровня IPv4. Средний раздел содержит информацию о поле данных кадра. Данные содержат IPv4-адреса источника (192.168.1.12) и назначения (193.232.1.11).

Во втором указанном кадре Response указаны IPv4-адреса источника (192.168.1.11) и назначения (192.168.1.12) наоборот по сравнению с Request.

Захват из - [PC1-mrshcherbak Ethernet0 to msk-mrshcherbak-sw-01 Ethernet0]

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2	0.005923	::	ff02::2	ICMPv6	62	Router Solicitation
3	0.050086	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
4	0.056763	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
5	1.051820	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
6	1.058862	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
7	2.052776	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
8	2.059684	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
9	702.768083	Private_66:68:01	Broadcast	ARP	64	Who has 192.168.1.11? Tell 192.168.1.12
10	702.768395	Private_66:68:00	Private_66:68:01	ARP	64	192.168.1.11 is at 00:50:79:66:68:00
11	702.769309	192.168.1.12	192.168.1.11	ICMP	98	Echo (ping) request id=0xcd34, seq=1/256, tt
12	702.769753	192.168.1.11	192.168.1.12	ICMP	98	Echo (ping) reply id=0xcd34, seq=1/256, tt
13	861.579730	Private_66:68:01	Broadcast	ARP	64	Who has 192.168.1.11? Tell 192.168.1.12
14	861.580041	Private_66:68:00	Private_66:68:01	ARP	64	192.168.1.11 is at 00:50:79:66:68:00
15	861.580847	192.168.1.12	192.168.1.11	ECHO	98	Request
16	861.581049	192.168.1.11	192.168.1.12	ECHO	98	Response

> Frame 15: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0

▼ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)

▼ Destination: Private_66:68:00 (00:50:79:66:68:00)

Address: Private_66:68:00 (00:50:79:66:68:00)
... .. = LG bit: Globally unique address (factory default)
... .. = IG bit: Individual address (unicast)

▼ Source: Private_66:68:01 (00:50:79:66:68:01)

Address: Private_66:68:01 (00:50:79:66:68:01)
... .. = LG bit: Globally unique address (factory default)
... .. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.11

0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x356c (13676)
> 000. = Flags: 0x0
... 0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64

Рис.2.6. Сведения об эхо-запросе в UDP-моду к узлу PC-1

В Wireshark проанализировала handshake протокола TCP. Установление связи клиент-сервер в TCP осуществляется в три этапа (трёхступенчатый handshake). Сначала клиент отправляет SYN, т.е. в передаваемом сообщении установлен бит SYN (Synchronize Sequence Number — установить соединение), затем сервер отвечает ACK (подтверждение) + SYN, т.е. установлены биты SYN и ACK, и наконец, клиент отправляет ACK — подтверждение получения SYN сегмента от сервера. Это происходит после пассивного открытия сервера, где он начинает

прослушивать порт. Теперь клиент может посылать пакеты с данными на сервер по только что созданному виртуальному TCP-каналу. На рис.2.7 изображён первый этап рукопожатия — где в заголовке ICMP указан Sequence Number, а Acknowledgment Number равен 0.

Единственными идентификаторами TCP-абонентов и TCP-соединения являются два параметра — Порядковый номер (Sequence Number) и Номер подтверждения (Acknowledgment Number).

На рис.2.8 представлена полученная в Wireshark информация по ARP- и ICMP-сообщениям.

No.	Time	Source	Destination	Protocol	Length	Info
11	702.769309	192.168.1.12	192.168.1.11	ICMP	98	Echo (ping) request id=0xcd34, seq=1/256, ttl=64 (reply in 12
12	702.769753	192.168.1.11	192.168.1.12	ICMP	98	Echo (ping) reply id=0xcd34, seq=1/256, ttl=64 (request in
13	861.579730	Private_66:68:01	Broadcast	ARP	64	Who has 192.168.1.11? Tell 192.168.1.12
14	861.580041	Private_66:68:00	Private_66:68:01	ARP	64	192.168.1.11 is at 00:50:79:66:68:00
15	861.580847	192.168.1.12	192.168.1.11	ECHO	98	Request
16	861.581049	192.168.1.11	192.168.1.12	ECHO	98	Response
17	956.591729	192.168.1.12	192.168.1.11	TCP	74	29229 → 7 [SYN] Seq=0 Win=2920 Len=0 MSS=1460 TSval=1696282059
18	956.592174	192.168.1.11	192.168.1.12	TCP	54	7 → 29229 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0
19	956.593094	192.168.1.12	192.168.1.11	TCP	66	29229 → 7 [ACK] Seq=1 Ack=1 Win=2920 Len=0 TSval=1696282059 TS
20	956.593463	192.168.1.12	192.168.1.11	ECHO	122	Request
21	956.593735	192.168.1.11	192.168.1.12	TCP	54	7 → 29229 [ACK] Seq=1 Ack=57 Win=2920 Len=0
22	956.595142	192.168.1.12	192.168.1.11	TCP	66	29229 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=16
23	956.595547	192.168.1.11	192.168.1.12	TCP	54	7 → 29229 [ACK] Seq=1 Ack=58 Win=2920 Len=0
24	956.595593	192.168.1.11	192.168.1.12	TCP	54	7 → 29229 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
25	956.598421	192.168.1.12	192.168.1.11	TCP	66	29229 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1696282059 T


```

> Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface -, id 0
▼ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)
  ▼ Destination: Private_66:68:00 (00:50:79:66:68:00)
    Address: Private_66:68:00 (00:50:79:66:68:00)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: Private_66:68:01 (00:50:79:66:68:01)
    Address: Private_66:68:01 (00:50:79:66:68:01)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.11
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x35cb (13771)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  
```

Рис.2.7. Сведения об эхо-запросе в TCP-моду к узлу PC-1

*- [PC1-mrshcherbak Ethernet0 to msk-mrshcherbak-sw-01 Ethernet0]

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::2	ICMPv6	62	Router Solicitation
2	0.005923	::	ff02::2	ICMPv6	62	Router Solicitation
3	0.050086	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
4	0.056763	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
5	1.051820	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
6	1.058862	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
7	2.052776	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
8	2.059684	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
9	702.768083	Private_66:68:01	Broadcast	ARP	64	Who has 192.168.1.11? Tell 192.168.1.12
10	702.768395	Private_66:68:00	Private_66:68:01	ARP	64	192.168.1.11 is at 00:50:79:66:68:00
11	702.769309	192.168.1.12	192.168.1.11	ICMP	98	Echo (ping) request id=0xcd34, seq=1/256,
12	702.769753	192.168.1.11	192.168.1.12	ICMP	98	Echo (ping) reply id=0xcd34, seq=1/256,
13	861.579730	Private_66:68:01	Broadcast	ARP	64	Who has 192.168.1.11? Tell 192.168.1.12
14	861.580041	Private_66:68:00	Private_66:68:01	ARP	64	192.168.1.11 is at 00:50:79:66:68:00
15	861.580847	192.168.1.12	192.168.1.11	ECHO	98	Request
16	861.581049	192.168.1.11	192.168.1.12	ECHO	98	Response
17	956.591729	192.168.1.12	192.168.1.11	TCP	74	29229 → 7 [SYN] Seq=0 Win=2920 Len=0 MSS=1
18	956.592174	192.168.1.11	192.168.1.12	TCP	54	7 → 29229 [SYN, ACK] Seq=0 Ack=1 Win=2920
19	956.593094	192.168.1.12	192.168.1.11	TCP	66	29229 → 7 [ACK] Seq=1 Ack=1 Win=2920 Len=0
20	956.593463	192.168.1.12	192.168.1.11	ECHO	122	Request
21	956.593735	192.168.1.11	192.168.1.12	TCP	54	7 → 29229 [ACK] Seq=1 Ack=57 Win=2920 Len=
22	956.595142	192.168.1.12	192.168.1.11	TCP	66	29229 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=
23	956.595547	192.168.1.11	192.168.1.12	TCP	54	7 → 29229 [ACK] Seq=1 Ack=58 Win=2920 Len=
24	956.595593	192.168.1.11	192.168.1.12	TCP	54	7 → 29229 [FIN, ACK] Seq=1 Ack=58 Win=2920
25	956.598421	192.168.1.12	192.168.1.11	TCP	66	29229 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=

> Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface -, id 0

▼ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)

▼ Destination: Private_66:68:00 (00:50:79:66:68:00)

Address: Private_66:68:00 (00:50:79:66:68:00)

.... .. = LG bit: Globally unique address (factory default)

Рис.2.8. Полученная в Wireshark информация по ARP- и ICMP-сообщениям

6. Остановила захват пакетов в Wireshark.

3. Моделирование простейшей сети на базе маршрутизатора FRR в GNS3

3.1. Постановка задачи

1. Построить в GNS3 топологию сети, состоящей из маршрутизатора FRR, коммутатора Ethernet и оконечного устройства.
2. Задать оконечному устройству IP-адрес в сети 192.168.1.0/24.
3. Присвоить интерфейсу маршрутизатора адрес 192.168.1.1/24.
4. Проверить связь.

3.2. Выполнение

1. Запустила GNS3 VM и GNS3. Создала новый проект под названием «Lab_5_next». В рабочей области GNS3 разместила VPCS, коммутатор Ethernet и маршрутизатор FRR. Изменила отображаемые названия устройств в соответствии с требованиями. Включила захват трафика на соединении между коммутатором и

маршрутизатором (рис.3.1). Запустила все устройства проекта. Открыла консоль всех устройств проекта.

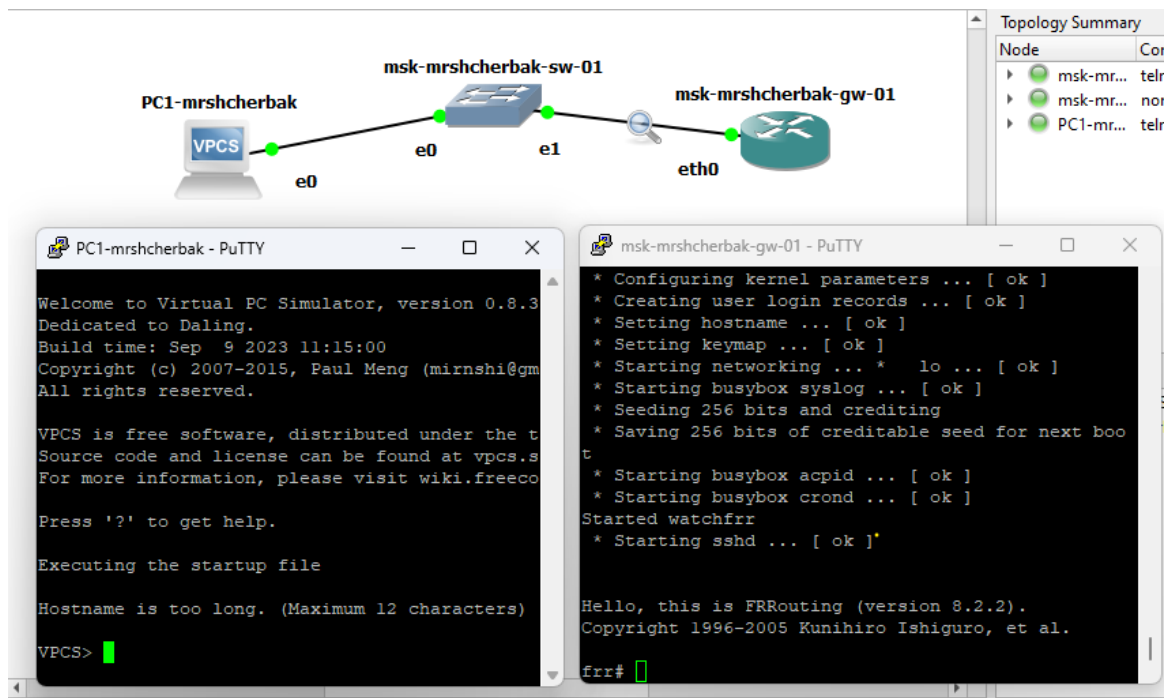


Рис.3.1. Топология простейшей сети с маршрутизатором в GNS3 и открытые консоли устройств

2. Настроила IP-адресацию для интерфейса узла PC1. Команды представлены на рис.3.2.

```
PC1-mrshcherbak - PuTTY

VPCS> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
VPCS : 192.168.1.10 255.255.255.0 gateway 192.168.1.1

VPCS> save
Saving startup configuration to startup.vpc
. done

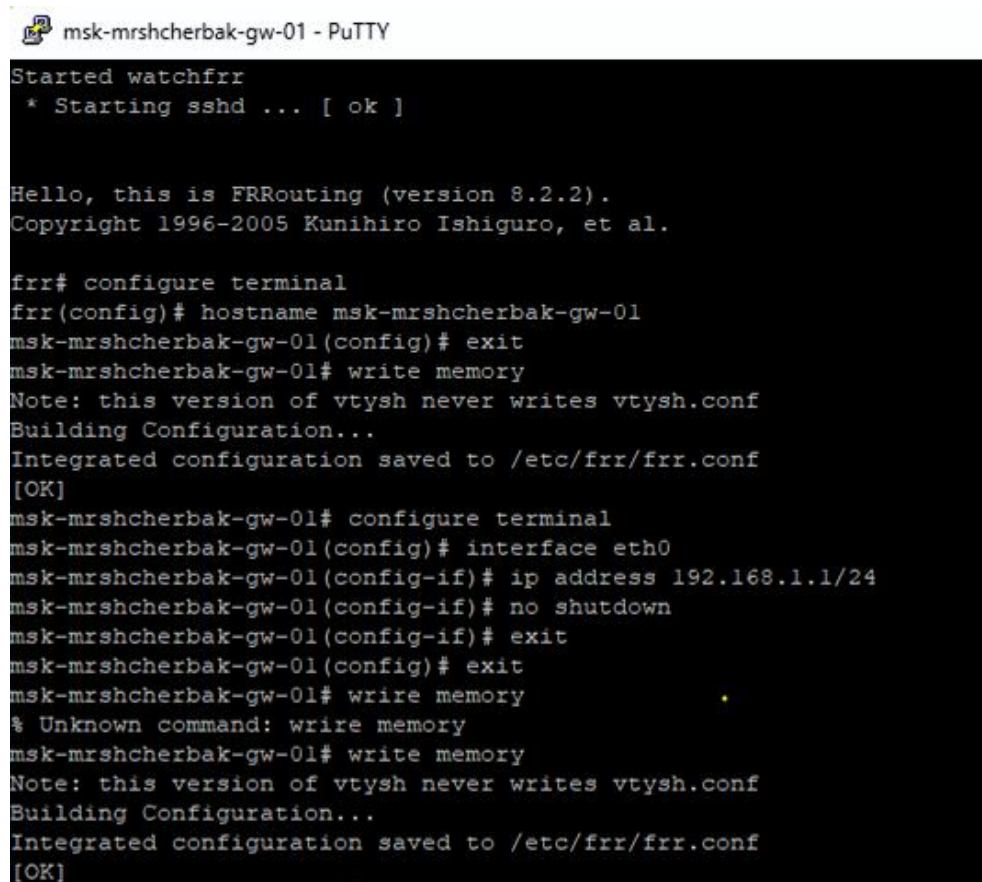
VPCS> show ip

NAME       : VPCS[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 20004
RHOST:PORT : 127.0.0.1:20005
MTU        : 1500

VPCS>
```

Рис.3.2. Настройка IP-адресации для интерфейса узла PC1

3. Настроила IP-адресацию для интерфейса локальной сети маршрутизатора (рис.3.3).



```
msk-mrshcherbak-gw-01 - PuTTY
Started watchfrr
* Starting sshd ... [ ok ]

Hello, this is FRROUTING (version 8.2.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

frr# configure terminal
frr(config)# hostname msk-mrshcherbak-gw-01
msk-mrshcherbak-gw-01(config)# exit
msk-mrshcherbak-gw-01# write memory
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
msk-mrshcherbak-gw-01# configure terminal
msk-mrshcherbak-gw-01(config)# interface eth0
msk-mrshcherbak-gw-01(config-if)# ip address 192.168.1.1/24
msk-mrshcherbak-gw-01(config-if)# no shutdown
msk-mrshcherbak-gw-01(config-if)# exit
msk-mrshcherbak-gw-01(config)# exit
msk-mrshcherbak-gw-01# write memory
% Unknown command: write memory
msk-mrshcherbak-gw-01# write memory
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
```

Рис.3.3. Настройка IP-адресации для интерфейса локальной сети маршрутизатора

4. Проверила конфигурацию маршрутизатора и настройки IP-адресации (рис.3.4).

```
msk-mrshcherbak-gw-01 - PuTTY
msk-mrshcherbak-gw-01# show running-config
Building configuration...

Current configuration:
!
frr version 8.2.2
frr defaults traditional
hostname frr
hostname msk-mrshcherbak-gw-01
service integrated-vtysh-config
!
interface eth0
 ip address 192.168.1.1/24
exit
!
end
msk-mrshcherbak-gw-01# show interface brief
Interface      Status VRF      Addresses
-----
eth0            up    default  192.168.1.1/24
eth1            down  default
eth2            down  default
eth3            down  default
eth4            down  default
eth5            down  default
eth6            down  default
eth7            down  default
lo              up    default
pimreg          up    default
msk-mrshcherbak-gw-01#
```

Рис.3.4. Проверка конфигурации маршрутизатора и настройки IP-адресации

5.Проверила подключение. Узел PC1 отправляет эхо-запросы на адрес маршрутизатора 192.168.1.1 (рис.3.5).

```
PC1-mrshcherbak - PuTTY
VPCS> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
VPCS : 192.168.1.10 255.255.255.0 gateway 192.168.1.1

VPCS> save
Saving startup configuration to startup.vpc
. done

VPCS> show ip

NAME       : VPCS[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 20004
RHOST:PORT : 127.0.0.1:20005
MTU        : 1500

VPCS> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=22.643 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.344 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=2.711 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=2.627 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=2.574 ms

VPCS>
```

Рис.3.5. Проверка работоспособности соединения между PC-1 и маршрутизатором

6. В окне Wireshark на панели списка пакетов отображено 5 эхо-запросов и эхо-ответов (дефолтное количество команды ping). Выбрала указанный кадр ICMP — эхо-запрос (request) (рис.3.6). Изучила информацию на панели сведений о пакете. Длина кадра = 98 байт. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (00:50:79:66:68:00) и назначения Destination (0c:56:a2:8a:00:00). MAC-адреса источника и назначения являются индивидуальными и глобально администрируемыми. Показан заголовок протокола сетевого уровня IPv4. Средний раздел содержит информацию о поле данных кадра. Данные содержат IPv4-адреса источника (192.168.1.10) и назначения (192.168.1.1). В заголовке ICMP основные поля — это type и code. Type говорит о том, что произошло в сети (Echo (ping) request).

Во втором указанном кадре ICMP (рис.3.7) — эхо-ответе (reply) указаны IPv4-адреса источника (192.168.1.1) и назначения (192.168.1.10) наоборот по сравнению с эхо-запросом.

Захват из - [msk-mrshcherbak-sw-01 Ethernet1 to msk-mrshcherbak-gw-01 eth0]

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
14	280.318508	fe80::e56:a2ff:fe8a...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
15	716.656486	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.1? Tell 192.168.1.10
16	716.686295	0c:56:a2:8a:00:00	Private_66:68:00	ARP	60	192.168.1.1 is at 0c:56:a2:8a:00:00
17	716.686950	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x8441, seq=1/256, ttl=64
18	716.709034	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x8441, seq=1/256, ttl=64
19	717.714023	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x8541, seq=2/512, ttl=64
20	717.716070	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x8541, seq=2/512, ttl=64
21	718.718662	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x8641, seq=3/768, ttl=64
22	718.721086	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x8641, seq=3/768, ttl=64
23	719.723067	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x8741, seq=4/1024, ttl=64
24	719.725266	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x8741, seq=4/1024, ttl=64
25	720.727087	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x8841, seq=5/1280, ttl=64
26	720.729376	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x8841, seq=5/1280, ttl=64
27	721.756796	0c:56:a2:8a:00:00	Private_66:68:00	ARP	60	Who has 192.168.1.10? Tell 192.168.1.1
28	721.757092	Private_66:68:00	0c:56:a2:8a:00:00	ARP	60	192.168.1.10 is at 00:50:79:66:68:00

> Frame 17: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0

▼ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: 0c:56:a2:8a:00:00 (0c:56:a2:8a:00:00)

▼ Destination: 0c:56:a2:8a:00:00 (0c:56:a2:8a:00:00)

Address: 0c:56:a2:8a:00:00 (0c:56:a2:8a:00:00)

.... 0. = LG bit: Globally unique address (factory default)

.... 0. = IG bit: Individual address (unicast)

▼ Source: Private_66:68:00 (00:50:79:66:68:00)

Address: Private_66:68:00 (00:50:79:66:68:00)

.... 0. = LG bit: Globally unique address (factory default)

.... 0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 84

Identification: 0x4184 (16772)

> 000. = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Рис.3.6. Сведения об эхо-запросе кадра ICMP

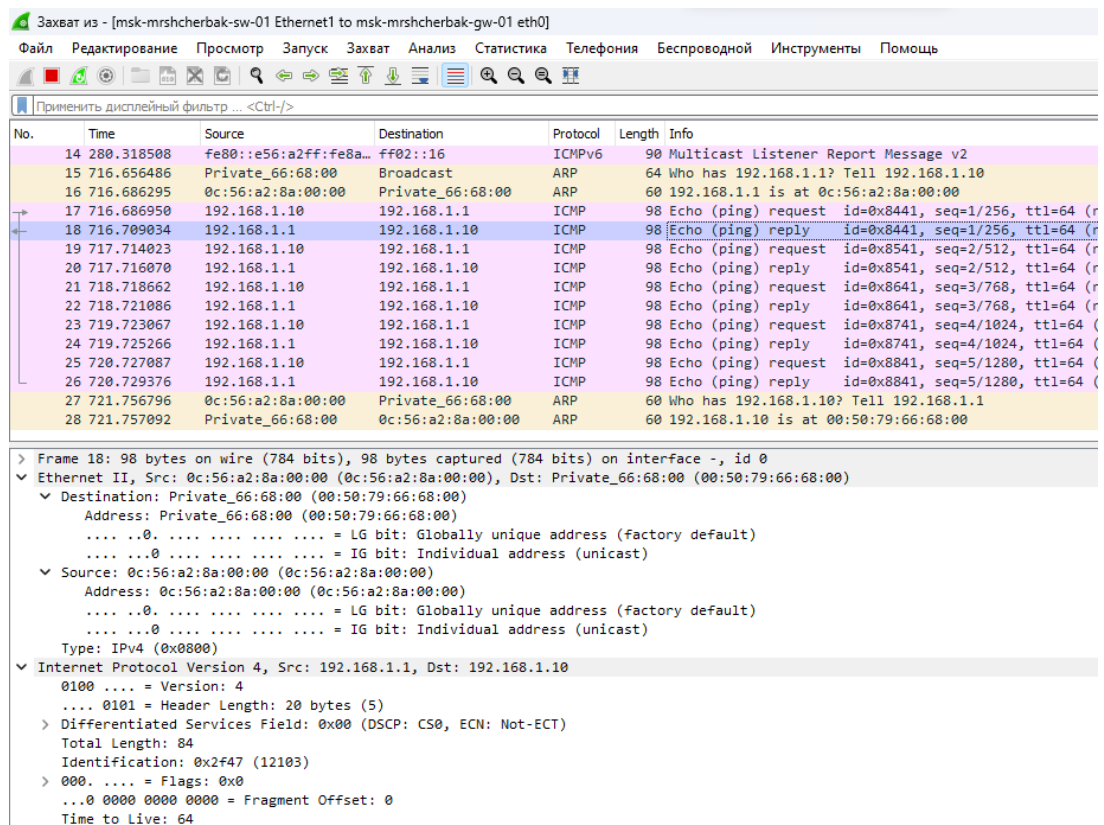


Рис.3.7. Сведения об эхо-ответе кадра ICMP

7. Остановила захват пакетов в Wireshark и все устройства в проекте.

4. Моделирование простейшей сети на базе маршрутизатора VyOS в GNS3

4.1. Постановка задачи

1. Построить в GNS3 топологию сети, состоящей из маршрутизатора VyOS, коммутатора Ethernet и конечного устройства.
2. Задать конечному устройству IP-адрес в сети 192.168.1.0/24.
3. Присвоить интерфейсу маршрутизатора адрес 192.168.1.1/24.
4. Проверить связь.

4.2. Выполнение

1. Запустила GNS3 VM и GNS3. Создала новый проект под названием «Lab_5_next_next». В рабочей области разместила VPCS, коммутатор Ethernet и маршрутизатор VyOS. Изменила названия устройств в соответствии с требованиями. Включила захват трафика на соединении между коммутатором и маршрутизатором (рис.4.1). Запустила все устройства проекта и открыла консоль всех устройств.

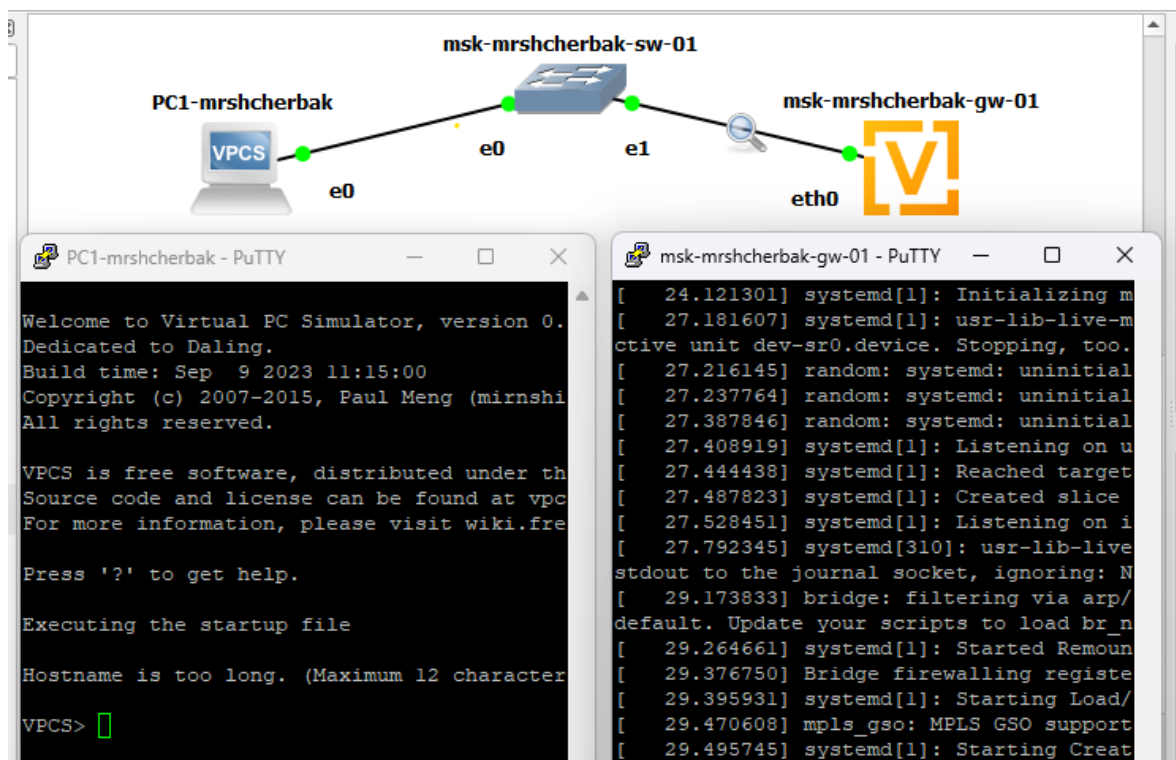


Рис.4.1. Топология простейшей сети с маршрутизатором в GNS3 и открытые консоли устройств

2. Настройте IP-адресацию для интерфейса узла PC1. Команды представлены на рис.4.2.

```

PC1-mrshcherbak - PuTTY

VPCS> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
VPCS : 192.168.1.10 255.255.255.0 gateway 192.168.1.1

VPCS> save
Saving startup configuration to startup.vpc
. done

VPCS> show ip

NAME       : VPCS[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 20004
RHOST:PORT : 127.0.0.1:20005
MTU        : 1500

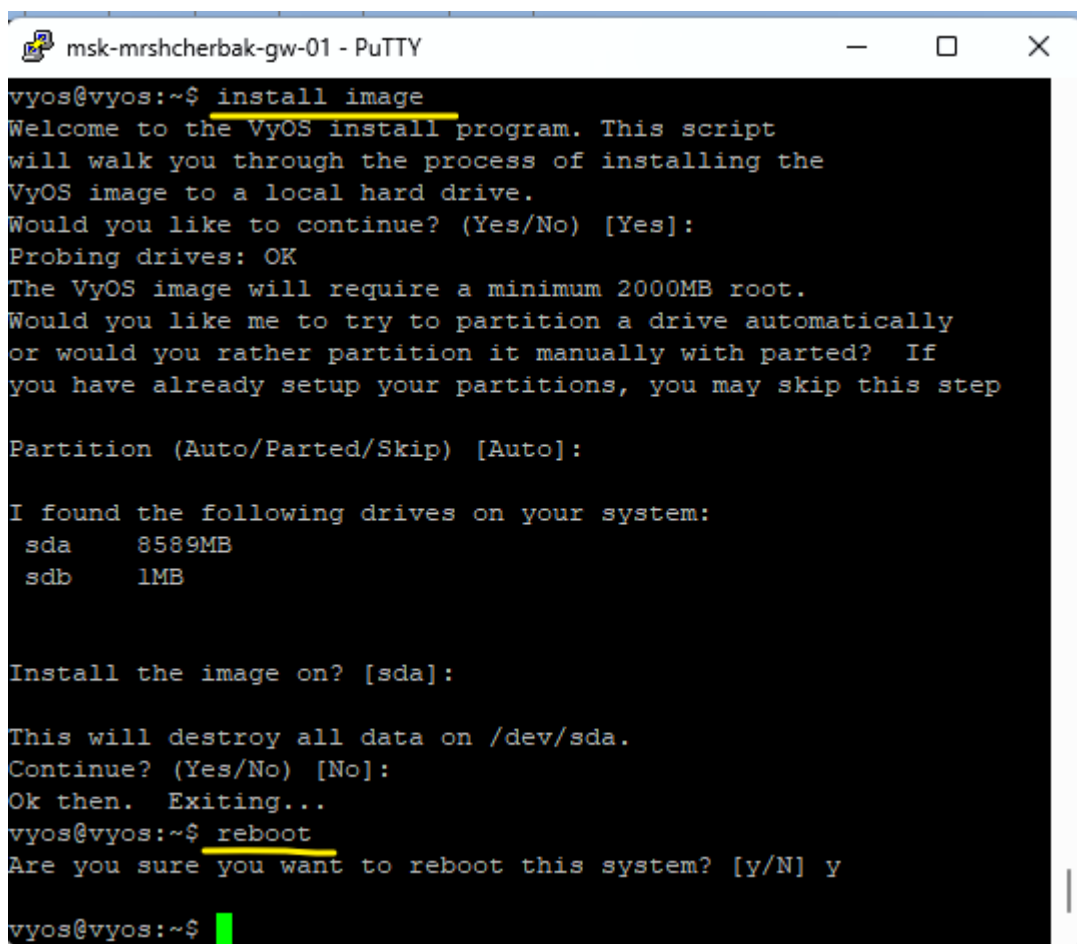
VPCS>

```

Рис.4.2. Настройка IP-адресации для интерфейса узла PC1

3. Настроила маршрутизатор VyOS. После загрузки ввела логин vyos и пароль vyos.

Установила систему на диск: `vyos@vyos:~$ install image`. Далее ответила на вопросы диалога установки, нажимая Enter. По завершении диалога перезапустила маршрутизатор, введя команду `reboot` (рис.4.3).



```
msk-mrshcherbak-gw-01 - PuTTY
vyos@vyos:~$ install image
Welcome to the VyOS install program. This script
will walk you through the process of installing the
VyOS image to a local hard drive.
Would you like to continue? (Yes/No) [Yes]:
Probing drives: OK
The VyOS image will require a minimum 2000MB root.
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted? If
you have already setup your partitions, you may skip this step

Partition (Auto/Parted/Skip) [Auto]:

I found the following drives on your system:
sda      8589MB
sdb      1MB

Install the image on? [sda]:

This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]:
Ok then.  Exiting...
vyos@vyos:~$ reboot
Are you sure you want to reboot this system? [y/N] y
vyos@vyos:~$
```

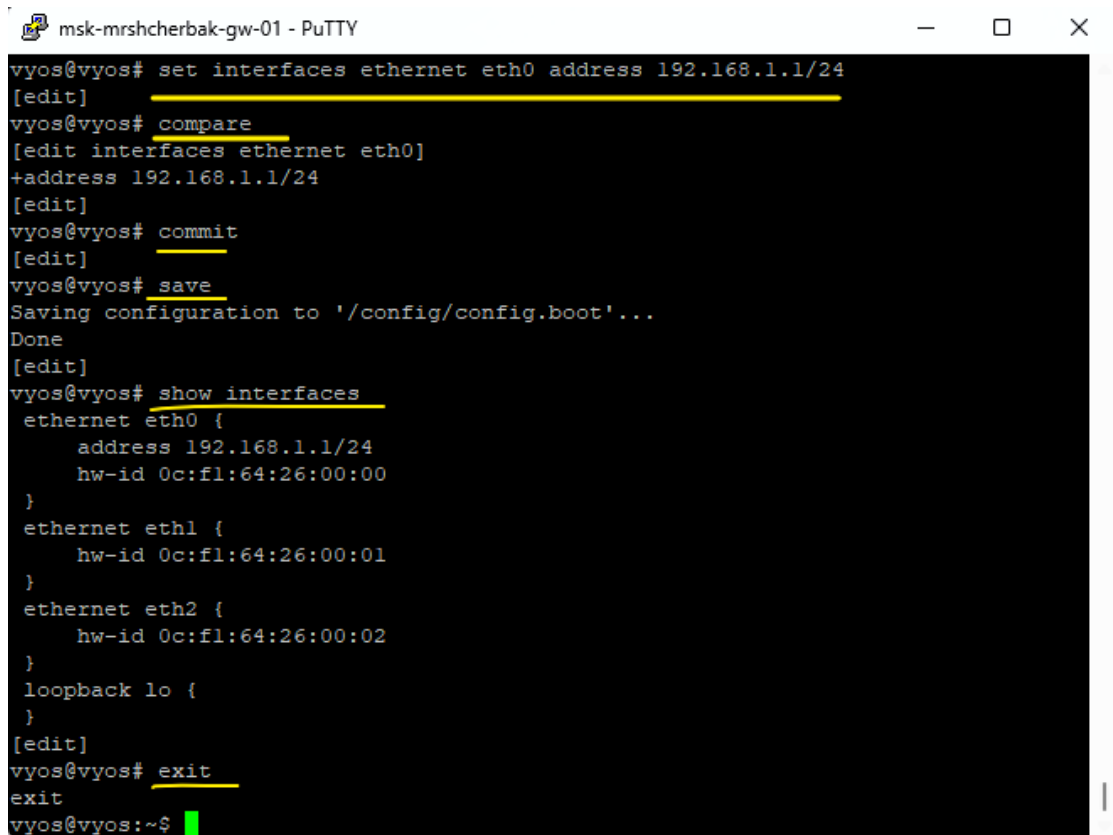
Рис.4.3. Установка системы на диск и перезапуск маршрутизатора

Перешла в режим конфигурирования с помощью команды «`configure`» и изменила имя устройства с помощью команды «`set system host-name msk-user-gw-01`» на `msk-mrshcherbak-gw-01` (рис.4.4).

Задала IP-адрес на интерфейсе `eth0` с помощью команды «`set interfaces ethernet eth0 address 192.168.1.1/24`» и посмотрела внесённые в конфигурацию изменения, введя «`compare`», после чего применила изменения в конфигурации и сохранила саму конфигурацию с помощью команд «`commit`» и «`save`» соответственно. Посмотрела информацию об интерфейсах маршрутизатора, введя «`show interfaces`» и вышла из режима конфигурирования. Выше описанные действия представлены на рис.4.5.

```
vyos@vyos# exit
exit
vyos@vyos:~$ configure
WARNING: You are currently configuring a live-ISO environment.
[edit]
vyos@msk-mrshcherbak-gw-01#
```

Рис.4.4. Изменено имя устройства



```
msk-mrshcherbak-gw-01 - PuTTY
vyos@vyos# set interfaces ethernet eth0 address 192.168.1.1/24
[edit]
vyos@vyos# compare
[edit interfaces ethernet eth0]
+address 192.168.1.1/24
[edit]
vyos@vyos# commit
[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos# show interfaces
  ethernet eth0 {
    address 192.168.1.1/24
    hw-id 0c:fl:64:26:00:00
  }
  ethernet eth1 {
    hw-id 0c:fl:64:26:00:01
  }
  ethernet eth2 {
    hw-id 0c:fl:64:26:00:02
  }
  loopback lo {
  }
[edit]
vyos@vyos# exit
exit
vyos@vyos:~$
```

Рис.4.5. Выполнение команд

4.Проверила подключение. Узел PC1 отправляет эхо-запросы на адрес маршрутизатора 192.168.1.1 (рис.4.6).

```
PC1-mrshcherbak - PuTTY
VPCS> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
VPCS : 192.168.1.10 255.255.255.0 gateway 192.168.1.1

VPCS> save
Saving startup configuration to startup.vpc
. done

VPCS> show ip
NAME       : VPCS[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 20004
RHOST:PORT : 127.0.0.1:20005
MTU        : 1500

VPCS> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=9.979 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.108 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=1.992 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=3.304 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=1.851 ms

VPCS>
```

Рис.4.6. Проверка работоспособности соединения между PC-1 и маршрутизатором

В окне Wireshark на панели списка пакетов отображено 5 эхо-запросов и эхо-ответов (дефолтное количество команды ping). Выбрала указанный кадр ICMP — эхо-запрос (request) (рис.4.7). Изучила информацию на панели сведений о пакете. Длина кадра = 98 байт. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (00:50:79:66:68:00) и назначения Destination (0c:f1:64:26:00:00). Показан заголовок протокола сетевого уровня IPv4. Средний раздел содержит информацию о поле данных кадра. Данные содержат IPv4-адреса источника (192.168.1.10) и назначения (192.168.1.1). В заголовке ICMP основные поля — это type и code. Type говорит о том, что произошло в сети (Echo (ping) request).

Во втором указанном кадре ICMP (рис.4.8) — эхо-ответе (reply) указаны IPv4-адреса источника (192.168.1.1) и назначения (192.168.1.10) наоборот по сравнению с эхо-запросом.

Захват из - [msk-mrshcherbak-sw-01 Ethernet1 to msk-mrshcherbak-gw-01 eth0]						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
Применить дисплейный фильтр ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
20	468.830587	fe80::ef1:64ff:fe26...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
21	1028.617249	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.1? Tell 192.168.1.10
22	1028.633146	0c:f1:64:26:00:00	Private_66:68:00	ARP	60	192.168.1.1 is at 0c:f1:64:26:00:00
23	1028.634195	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xa64e, seq=1/256, ti
24	1028.643906	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xa64e, seq=1/256, ti
25	1029.645389	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xa74e, seq=2/512, ti
26	1029.647089	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xa74e, seq=2/512, ti
27	1030.649336	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xa84e, seq=3/768, ti
28	1030.650757	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xa84e, seq=3/768, ti
29	1031.652201	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xa94e, seq=4/1024, ti
30	1031.654626	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xa94e, seq=4/1024, ti
31	1032.655518	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xaa4e, seq=5/1280, ti
32	1032.656996	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xaa4e, seq=5/1280, ti
33	1033.948669	0c:f1:64:26:00:00	Private_66:68:00	ARP	60	Who has 192.168.1.10? Tell 192.168.1.1
34	1033.949395	Private_66:68:00	0c:f1:64:26:00:00	ARP	60	192.168.1.10 is at 00:50:79:66:68:00

>	Frame 23: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
▼	Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: 0c:f1:64:26:00:00 (0c:f1:64:26:00:00)
>	Destination: 0c:f1:64:26:00:00 (0c:f1:64:26:00:00)
>	Source: Private_66:68:00 (00:50:79:66:68:00)
>	Type: IPv4 (0x0800)
▼	Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1
>	0100 = Version: 4
> 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
>	Total Length: 84
>	Identification: 0x4ea6 (20134)
>	000. = Flags: 0x0
>	...0 0000 0000 0000 = Fragment Offset: 0
>	Time to Live: 64
>	Protocol: ICMP (1)
>	Header Checksum: 0xa8a7 [validation disabled]
>	[Header checksum status: Unverified]
>	Source Address: 192.168.1.10
>	Destination Address: 192.168.1.1
>	Internet Control Message Protocol

Рис.4.7. Сведения об эхо-запросе кадра ICMP

Захват из - [msk-mrshcherbak-sw-01 Ethernet1 to msk-mrshcherbak-gw-01 eth0]

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
20	468.830587	fe80::ef1:64ff:fe26...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
21	1028.617249	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.1? Tell 192.168.1.10
22	1028.633146	0c:f1:64:26:00:00	Private_66:68:00	ARP	60	192.168.1.1 is at 0c:f1:64:26:00:00
23	1028.634195	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xa64e, seq=1/256, t
24	1028.643906	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xa64e, seq=1/256, t
25	1029.645389	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xa74e, seq=2/512, t
26	1029.647089	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xa74e, seq=2/512, t
27	1030.649336	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xa84e, seq=3/768, t
28	1030.650757	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xa84e, seq=3/768, t
29	1031.652201	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xa94e, seq=4/1024, t
30	1031.654626	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xa94e, seq=4/1024, t
31	1032.655518	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xaa4e, seq=5/1280, t
32	1032.656996	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xaa4e, seq=5/1280, t
33	1033.948669	0c:f1:64:26:00:00	Private_66:68:00	ARP	60	Who has 192.168.1.10? Tell 192.168.1.1
34	1033.949395	Private_66:68:00	0c:f1:64:26:00:00	ARP	60	192.168.1.10 is at 00:50:79:66:68:00

> Frame 24: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0

▼ Ethernet II, Src: 0c:f1:64:26:00:00 (0c:f1:64:26:00:00), Dst: Private_66:68:00 (00:50:79:66:68:00)

> Destination: Private_66:68:00 (00:50:79:66:68:00)

> Source: 0c:f1:64:26:00:00 (0c:f1:64:26:00:00)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 84

Identification: 0x0180 (384)

> 000. = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: ICMP (1)

Header Checksum: 0xf5cd [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.1

Destination Address: 192.168.1.10

> Internet Control Message Protocol

Рис.4.8. Сведения об эхо-ответе кадра ICMP

5. Остановила захват пакетов в Wireshark и все устройства в проекте. Завершила работу с GNS3.

Вывод: таким образом, в ходе выполнения л/р №5, я построила модели сетей на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, проанализировала трафик посредством Wireshark.