**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. **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. **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).

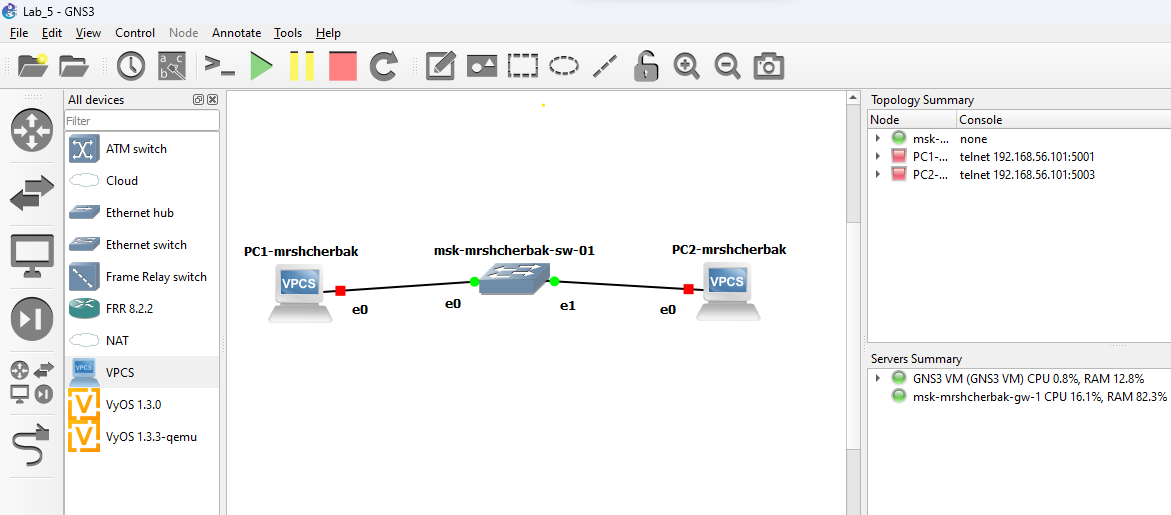


Рис.1.1. Топология простейшей сети в GNS3

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.

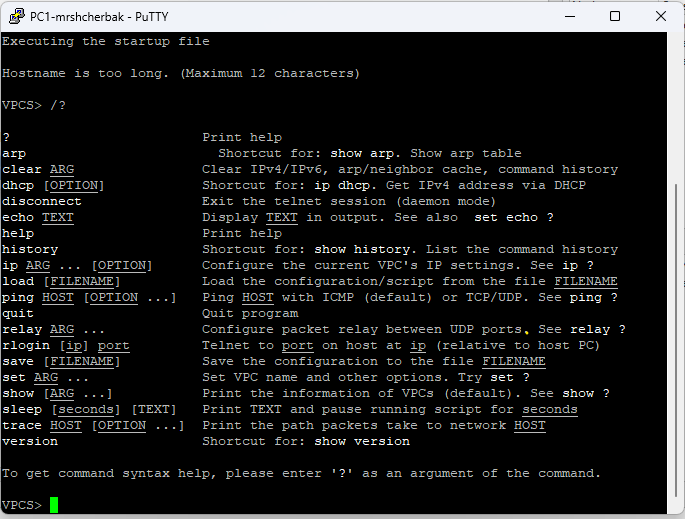


Рис.1.2. Просмотр синтаксиса возможных для ввода команд VPCS в GNS3

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.

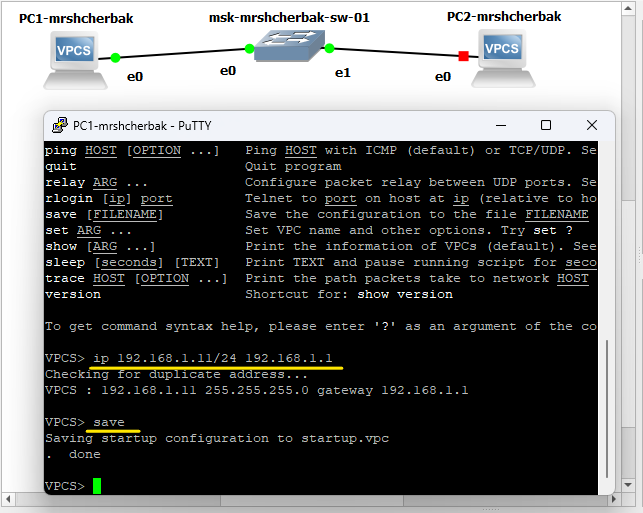


Рис.1.3. Задание IP-адреса и сохранение конфигурации VPCS в GNS3

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

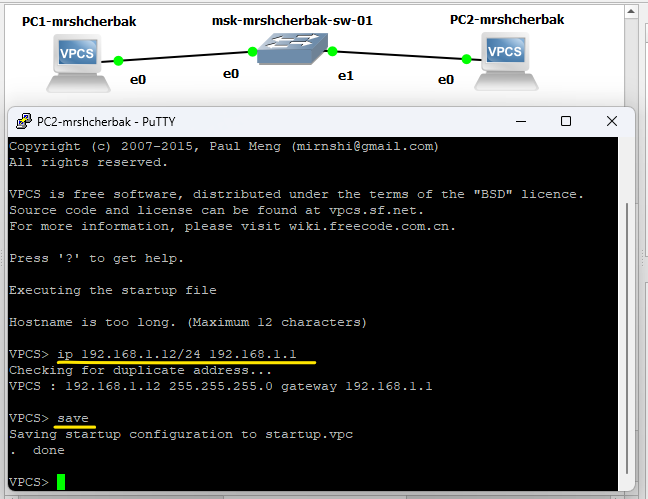
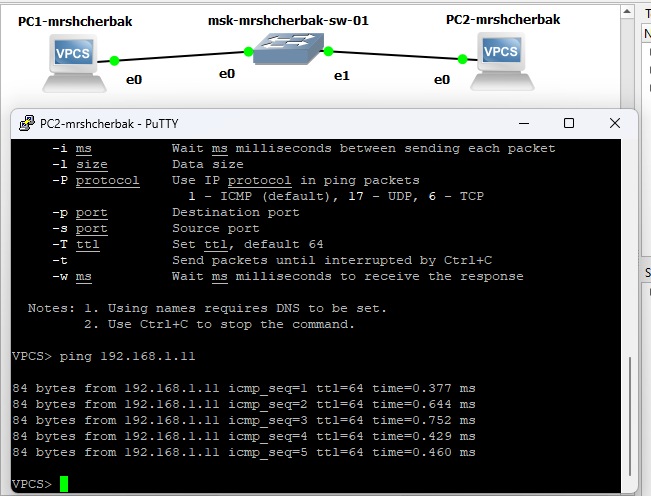


Рис.1.4. Задание IP-адреса и сохранение конфигурации VPCS в GNS3

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).

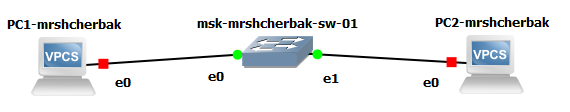


Рис.1.6. Остановка всех узлов

# 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).

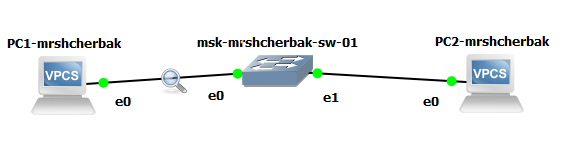


Рис.2.1. Запуск анализатора трафика на соединении между PC-1 и коммутатором

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 Adress индивидуальный и глобально администрируемый, а Destination Adress групповой и локально администрируемый.

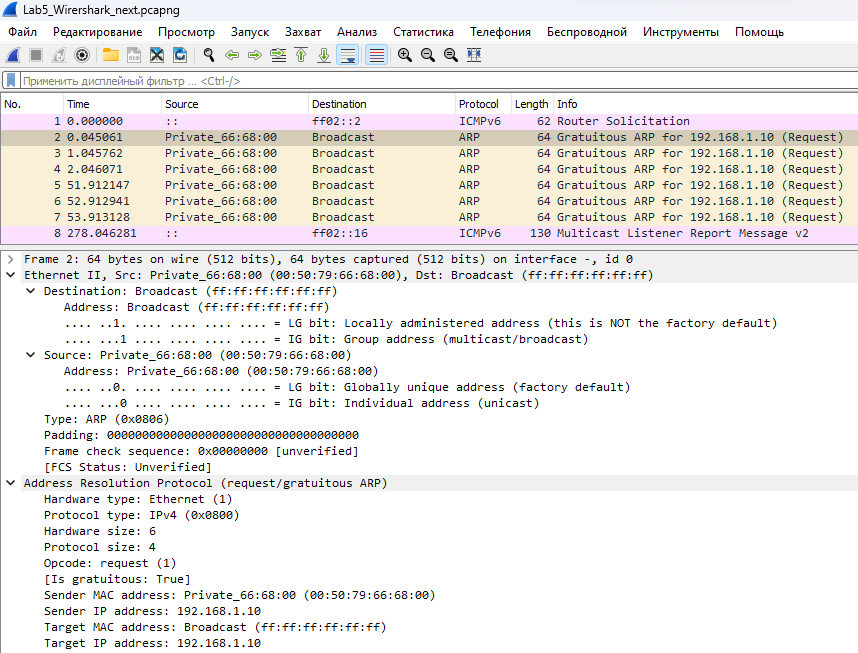


Рис.2.2. Информация по протоколу ARP

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

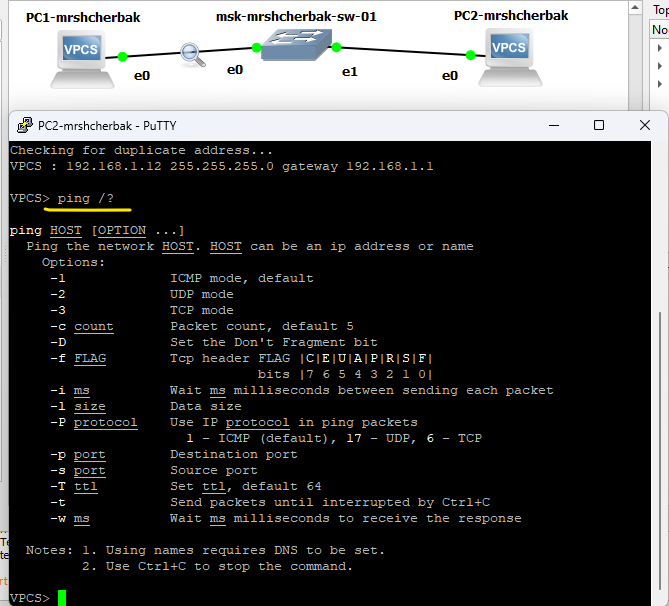


Рис.2.3. Просмотр информации по опциям команды ping

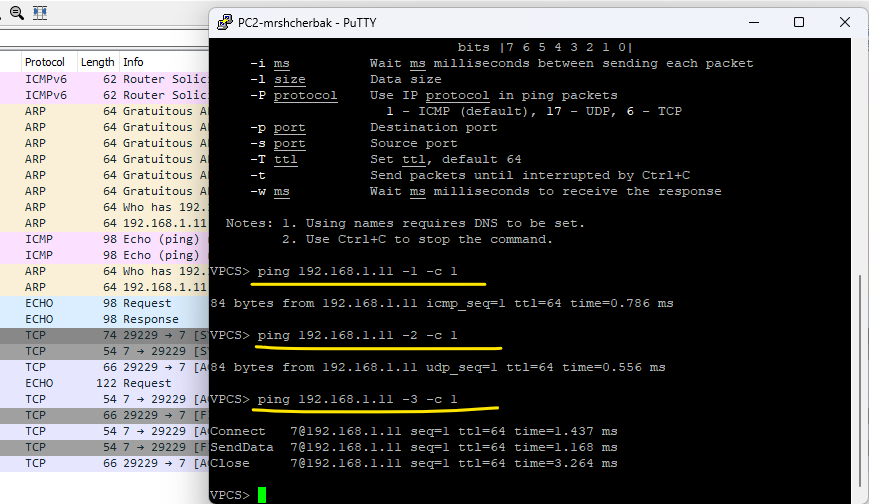


Рис.2.4. Выполнение команд

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.

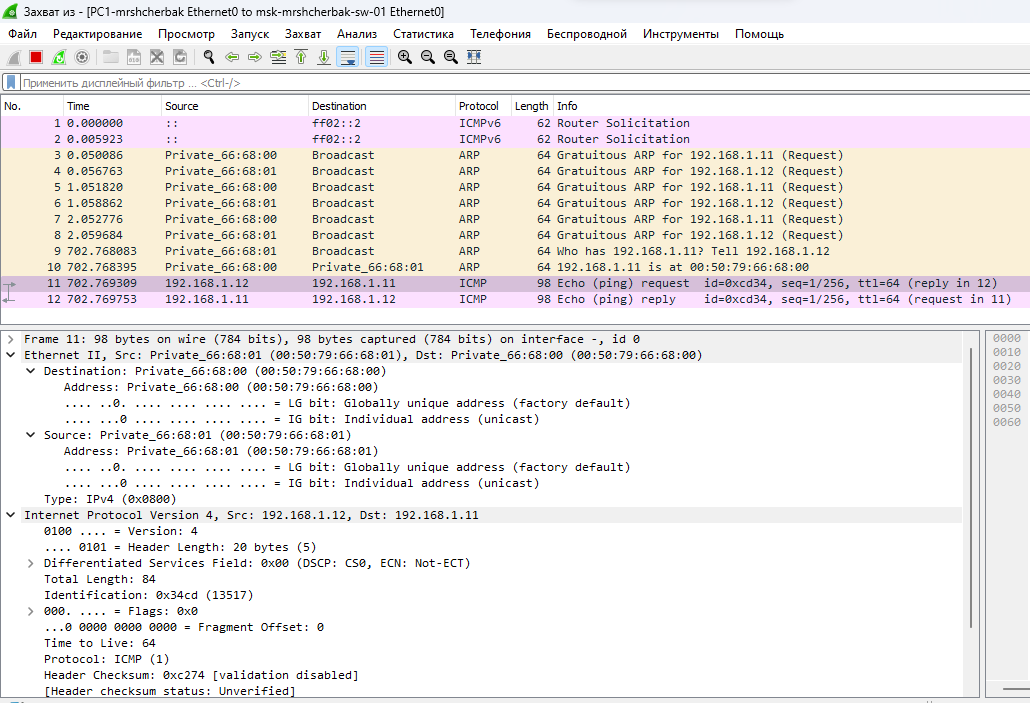


Рис.2.5. Сведения об эхо-запросе в ICMP-моде к узлу PC-1

Проанализировала полученную информацию от одного эхо-запроса в UDP-моде 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.

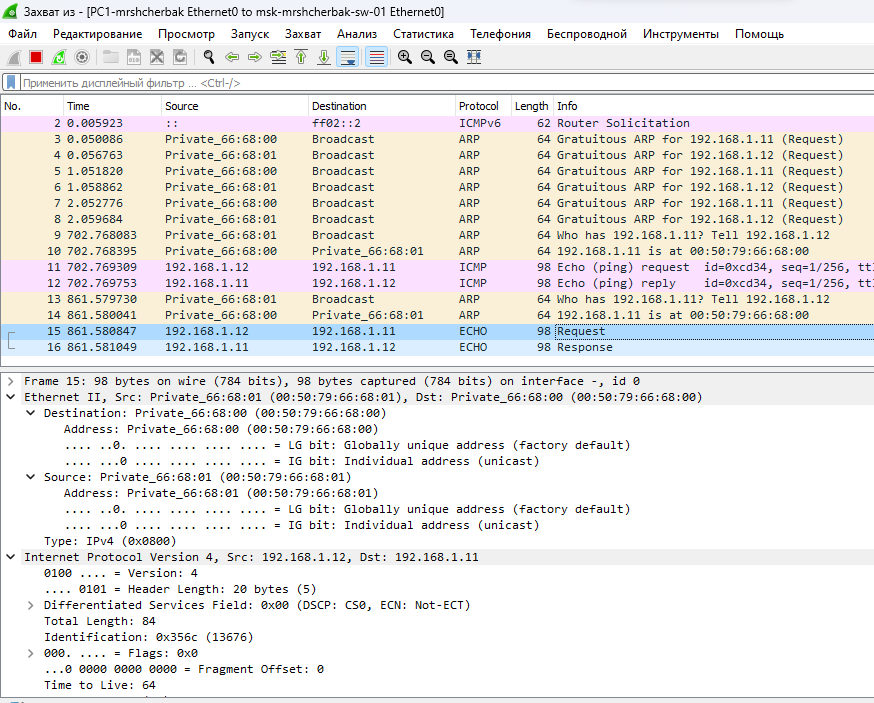


Рис.2.6. Сведения об эхо-запросе в UDP-моде к узлу PC-1

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.

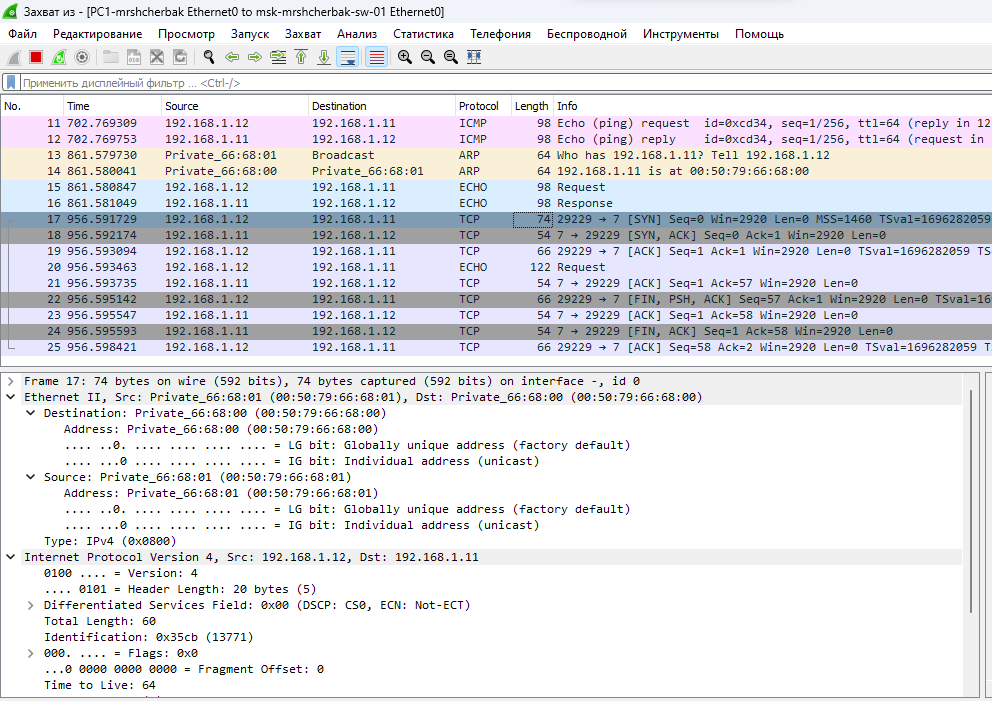


Рис.2.7. Сведения об эхо-запросе в TCP-моде к узлу PC-1

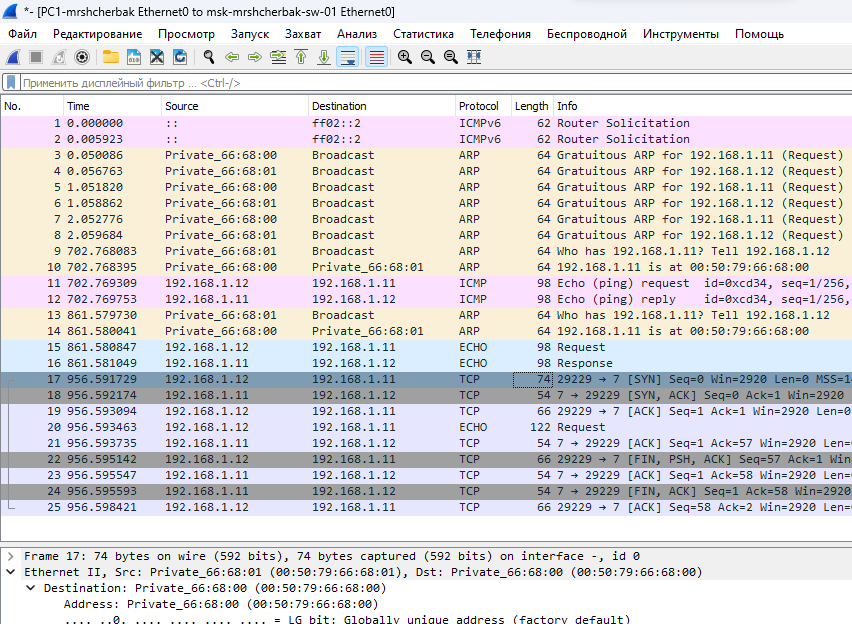


Рис.2.8. Полученная в Wireshark информация по ARP- и ICMP-сообщениям

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.

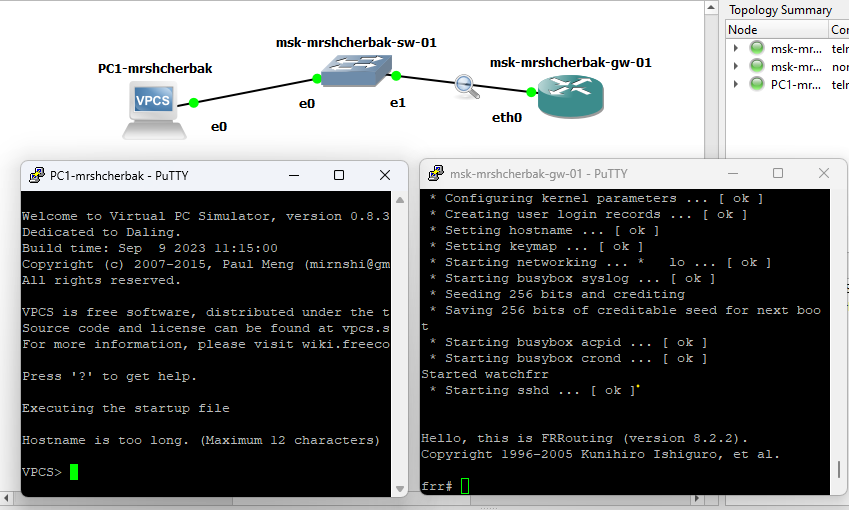


Рис.3.1. Топология простейшей сети с маршрутизатором в GNS3 и открытые консоли устройств

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

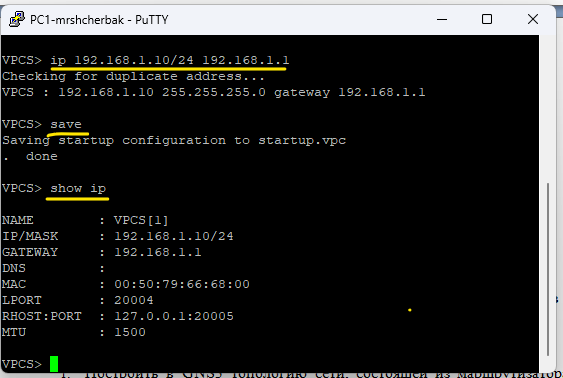


Рис.3.2. Настройка IP-адресации для интерфейса узла PC1

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

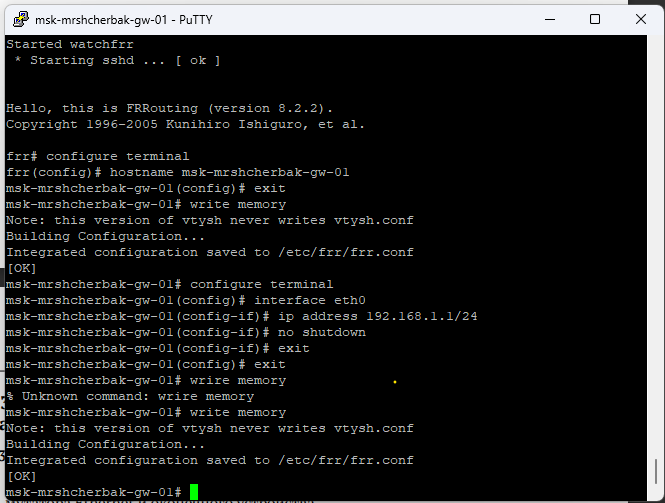


Рис.3.3. Настройка IP-адресации для интерфейса локальной сети маршрутизатора

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

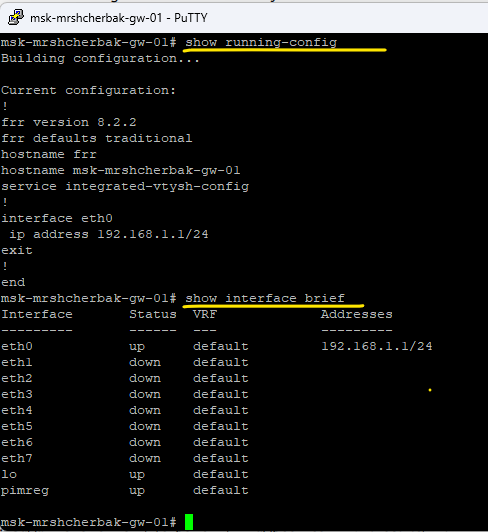


Рис.3.4. Проверка конфигурации маршрутизатора и настройки IP-адресации

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

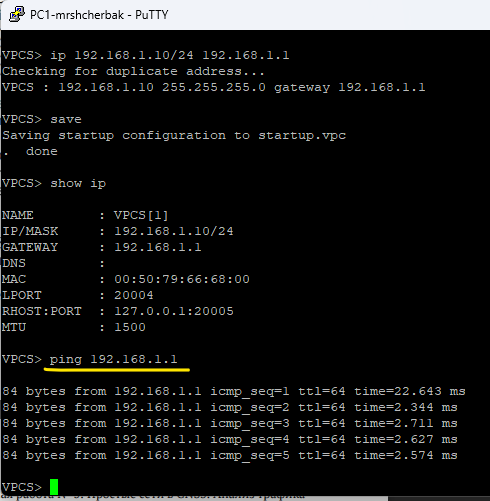


Рис.3.5. Проверка работоспособности соединения между PC-1 и маршрутизатором

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 (0с:56:а2:8а: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.

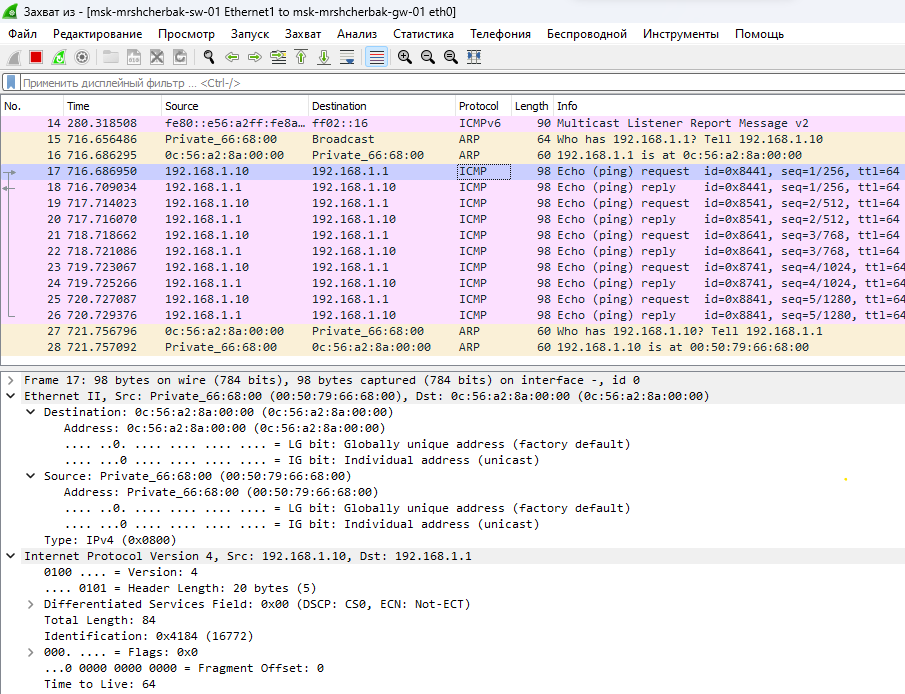


Рис.3.6. Сведения об эхо-запросе кадра ICMP

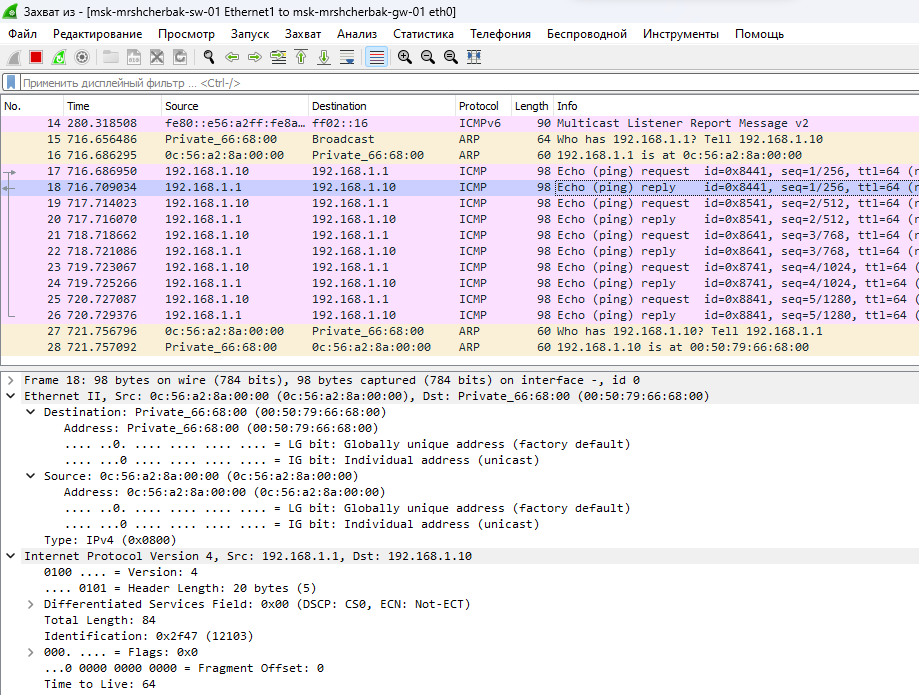


Рис.3.7. Сведения об эхо-ответе кадра ICMP

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 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.

# 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.

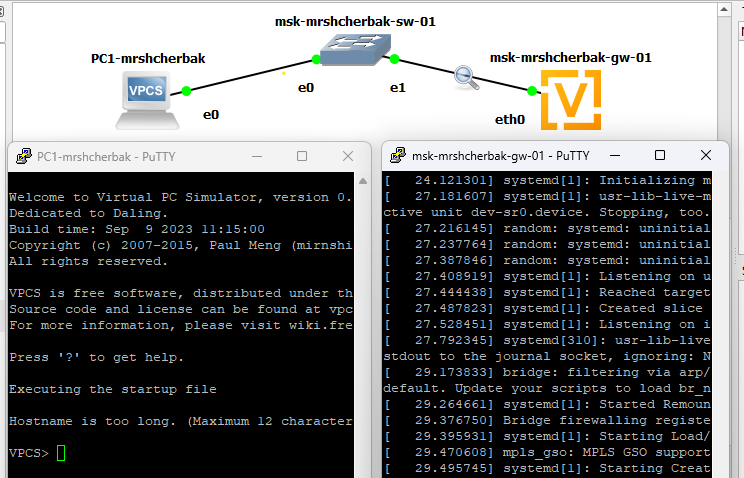


Рис.4.1. Топология простейшей сети с маршрутизатором в GNS3 и открытые консоли устройств

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

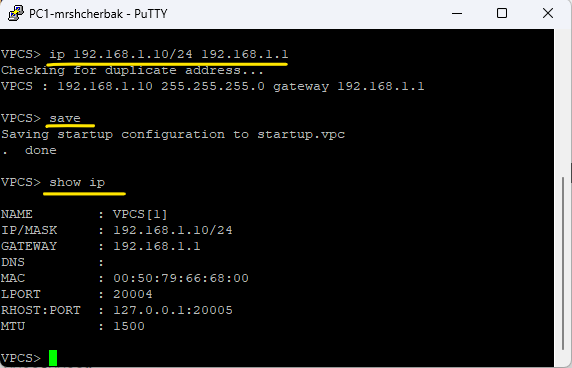


Рис.4.2. Настройка IP-адресации для интерфейса узла PC1

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).

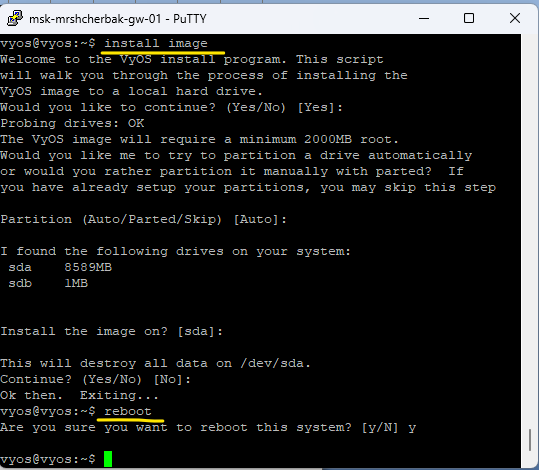


Рис.4.3. Установка системы на диск и перезапуск маршрутизатора

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.

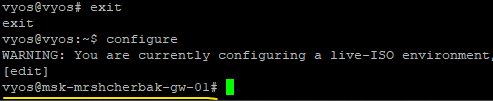


Рис.4.4. Изменено имя устройства

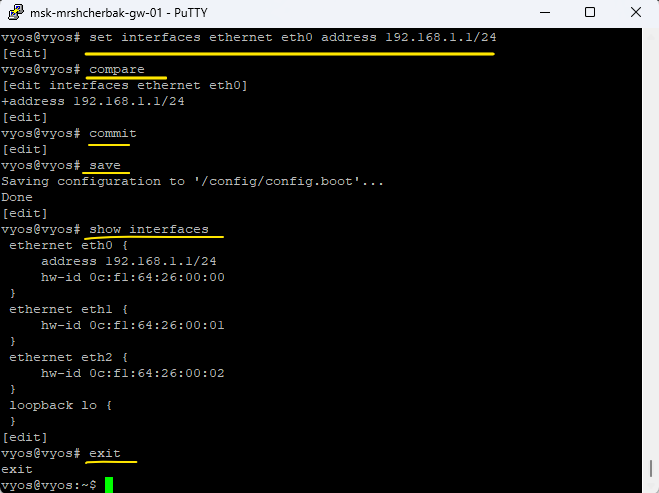


Рис.4.5. Выполнение команд

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

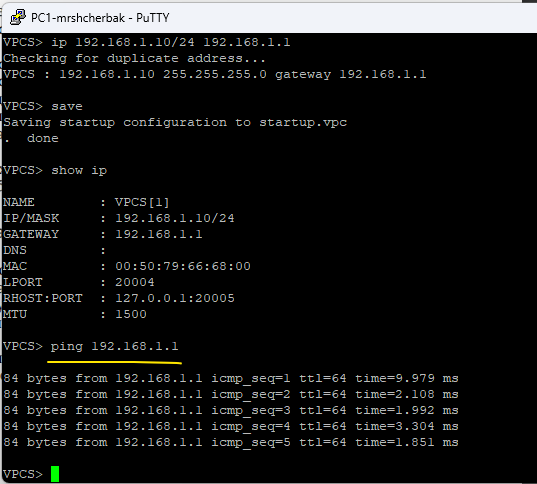


Рис.4.6. Проверка работоспособности соединения между PC-1 и маршрутизатором

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 (0с: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.

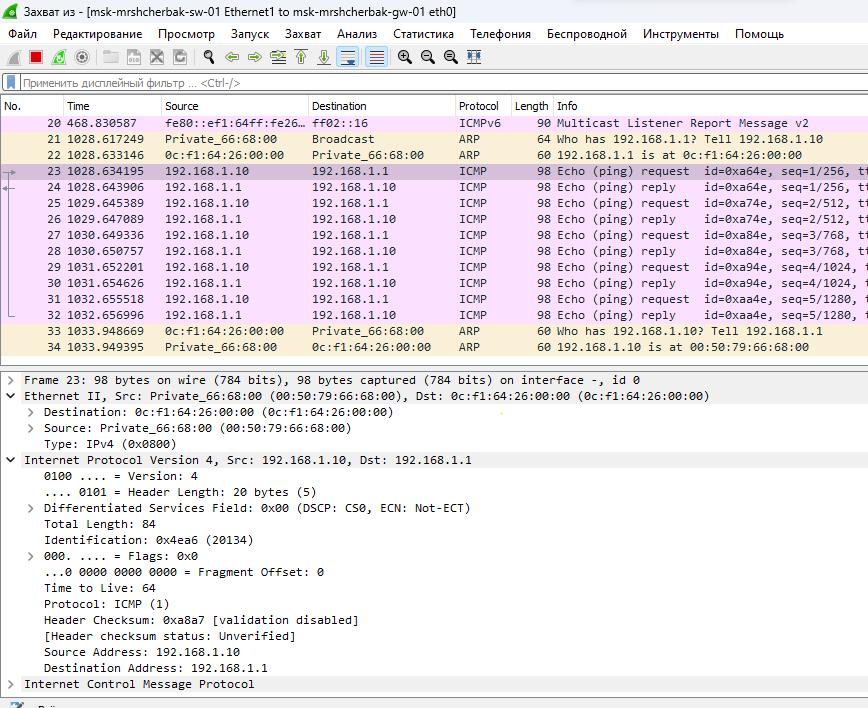


Рис.4.7. Сведения об эхо-запросе кадра ICMP

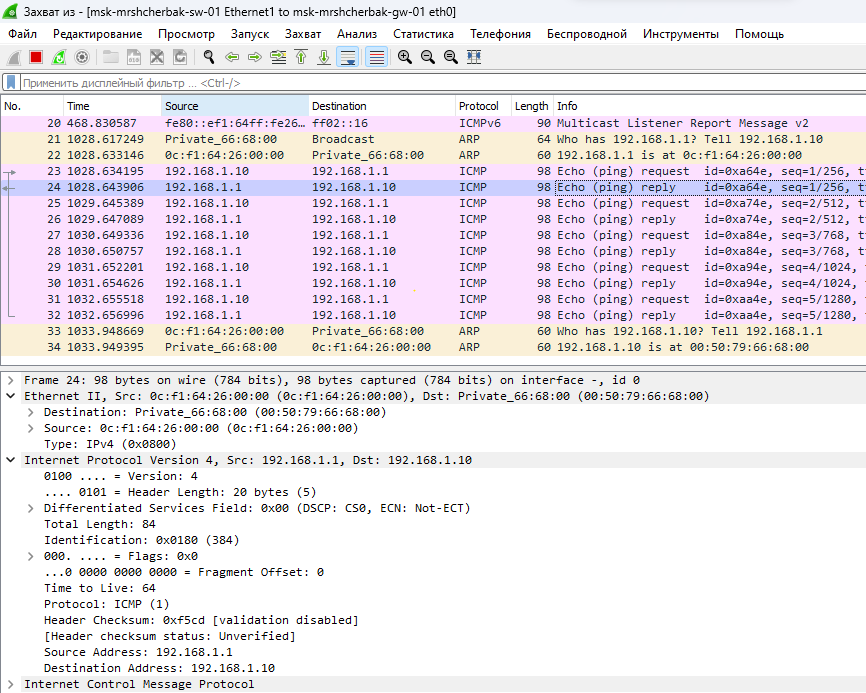


Рис.4.8. Сведения об эхо-ответе кадра ICMP

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.