Отчёт по лабораторной работе №5

Простые сети в GNS3. Анализ трафика

Авдадаев Джамал Геланиевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Выполнение задания

2.1 Построение простейшей сети и проверка связности

В ходе выполнения лабораторной работы в среде моделирования **GNS3** была построена простейшая локальная сеть, состоящая из одного Ethernet-коммутатора и двух оконечных устройств типа **VPCS**. Узлы были переименованы с включением имени учётной записи студента: **PC1-dgavdadaev**, **PC2-dgavdadaev**, коммутатор — **msk-dgavdadaev-sw-01**. После переименования оконечные устройства были соединены с коммутатором, в результате чего был сформирован единый широковещательный домен.

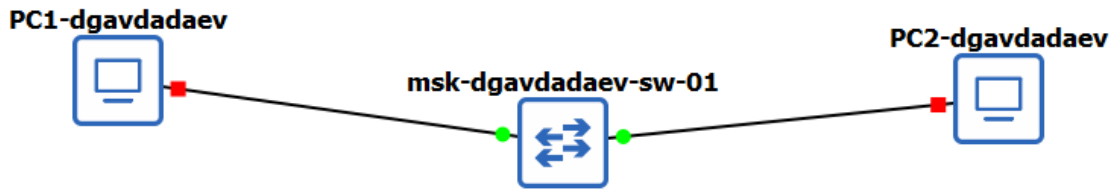

Рис. 2.1: Топология сети в GNS3

2.1.1 Просмотр синтаксиса команд VPCS

После запуска узлов был открыт терминал **PC1**. Для ознакомления с доступными командами VPCS была вызвана встроенная справка с помощью команды **?**. В

терминале отобразился перечень основных команд, предназначенных для настройки IP-параметров, диагностики соединений и управления конфигурацией.

При старте VPCS также выводится сообщение *“Hostname is too long (Maximum 12 characters)”*, связанное с ограничением длины имени хоста в VPCS. Данное сообщение носит информационный характер и не влияет на функционирование сети.

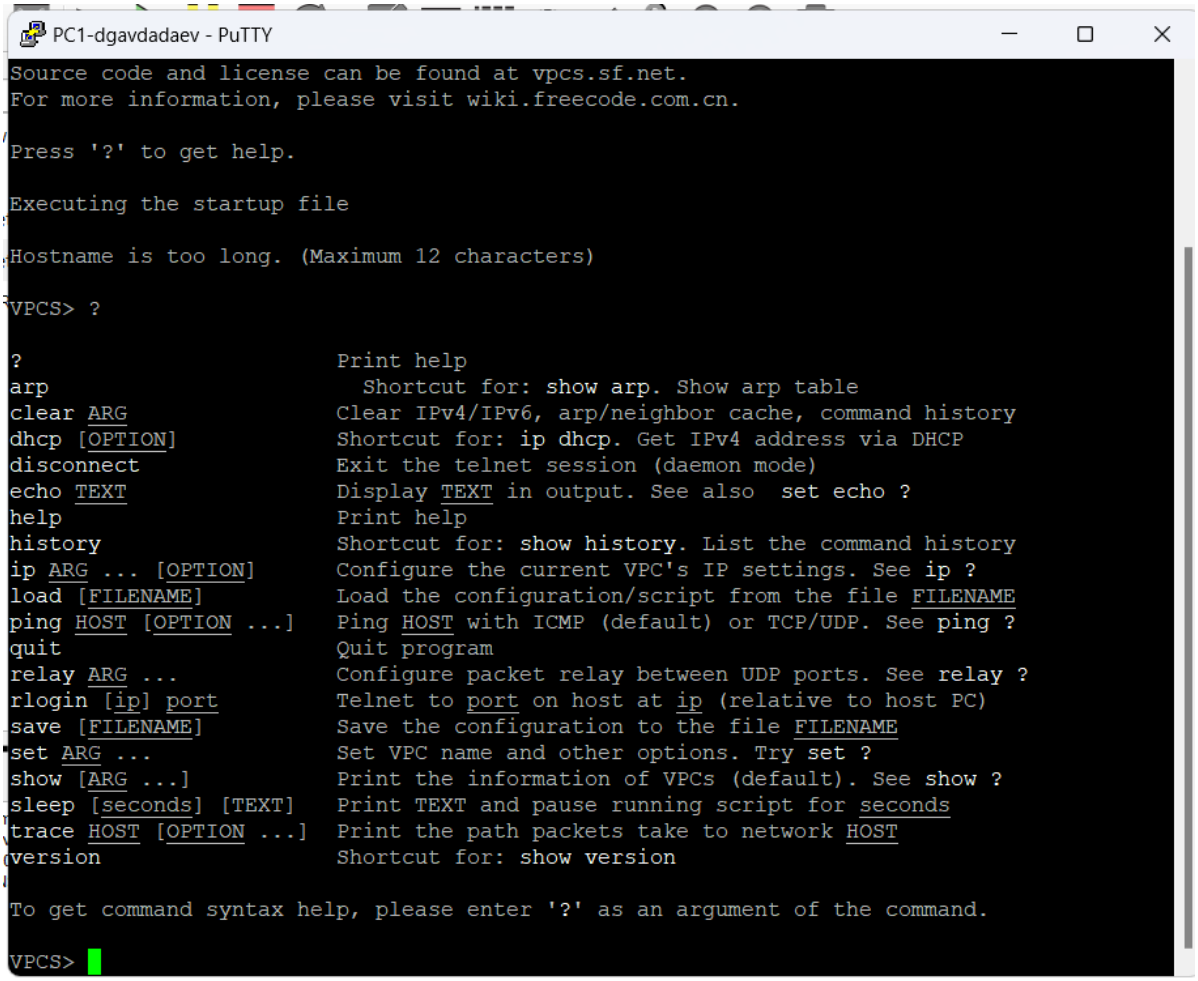

Рис. 2.2: Справка команд VPCS

2.1.2 Назначение IP-адресов оконечным устройствам

Для настройки сетевых параметров на **PC1** предварительно был просмотрен синтаксис команды настройки адресации с помощью `ip ?`. После этого устрой-

ству был назначен IP-адрес **192.168.1.11** с маской **/24**, а также указан шлюз по умолчанию **192.168.1.1**. После ввода параметров конфигурация была сохранена командой `save`.

Процесс задания IP-адреса и сохранения конфигурации на PC1 показан на рисунке ниже.

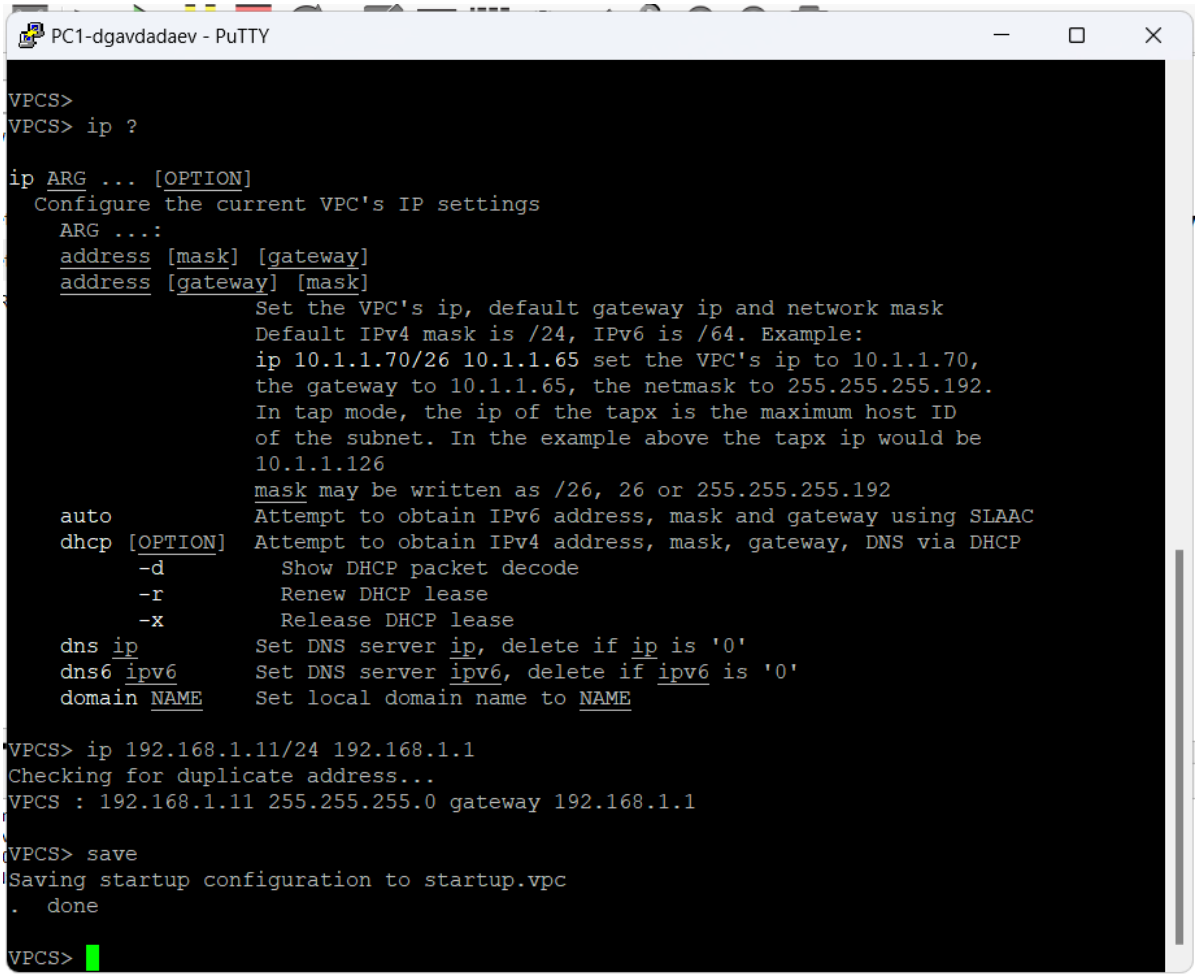

Рис. 2.3: Назначение IP-адреса PC1

Аналогичным образом на **PC2** был настроен IP-адрес **192.168.1.12/24** со шлюзом **192.168.1.1**, после чего конфигурация также была сохранена.

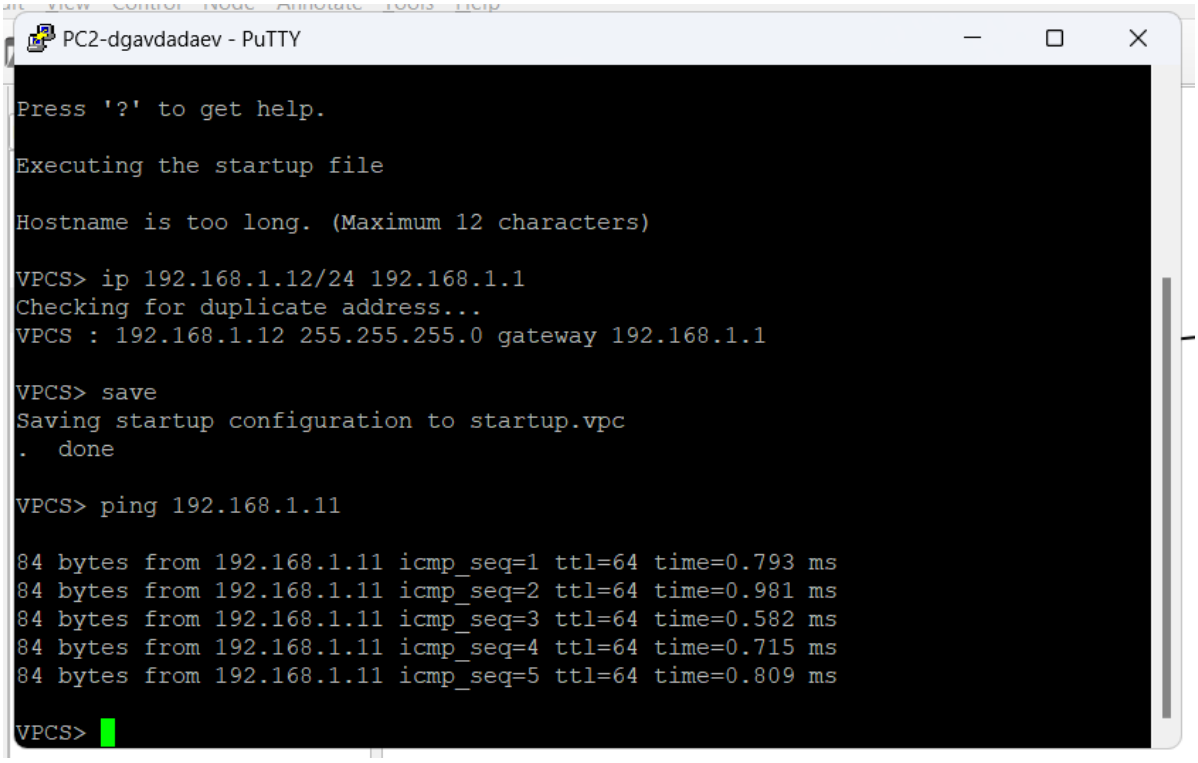

Рис. 2.4: Назначение IP-адреса PC2

2.1.3 Проверка связности между узлами

Для проверки работоспособности созданной сети и корректности настроенной адресации с **PC2** был выполнен эхо-запрос к **PC1**. В ответ были получены ICMP Echo Reply-пакеты без потерь, что свидетельствует о корректной работе коммутатора, правильной IP-адресации и наличии сетевой связности между узлами в одной подсети.

Результат выполнения проверки связности представлен на рисунке выше (см. Screenshot_4.png).

2.2 Анализ трафика в GNS3 с использованием Wireshark

На следующем этапе работы был выполнен захват и анализ сетевого трафика с помощью **Wireshark**. Захват был запущен на соединении между **PC1** и коммутатором. После запуска всех узлов в проекте в Wireshark начали отображаться кадры канального и сетевого уровней.

2.2.1 Анализ ARP-сообщений

В процессе захвата были зафиксированы ARP-кадры, в том числе **gratuitous ARP**. Данные сообщения отправляются узлом широковещательно и используются для проверки уникальности IP-адреса, а также для оповещения других устройств сети о соответствии IP- и MAC-адресов.

В разборе ARP-кадра видно, что IP-адрес отправителя совпадает с целевым IP-адресом, а MAC-адрес назначения является широковещательным. Это подтверждает, что кадр является gratuitous ARP-запросом.

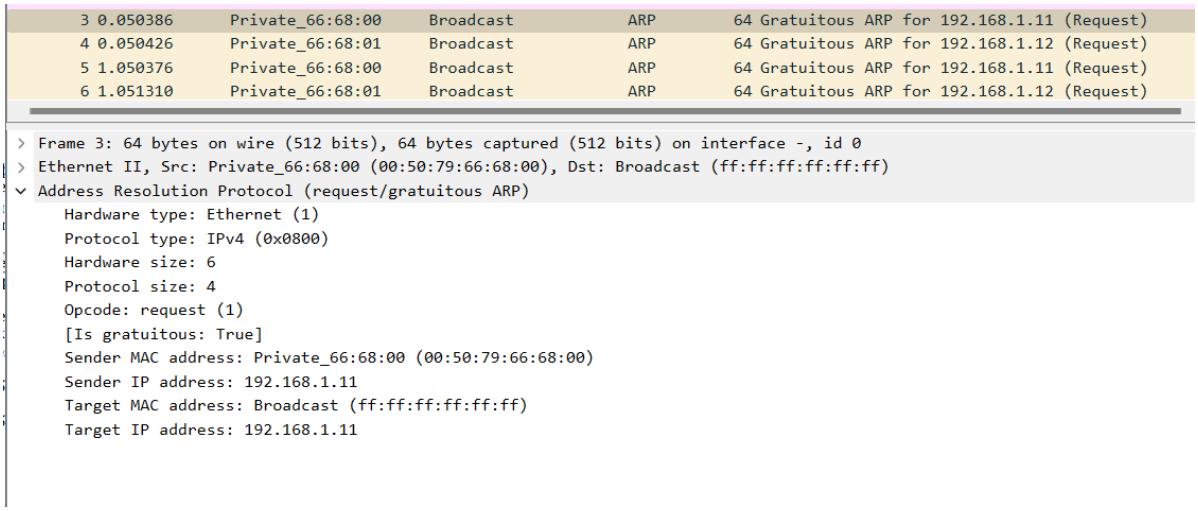

Рис. 2.5: ARP-трафик в Wireshark

2.2.2 Анализ ICMP-сообщений

В терминале **PC2** была вызвана справка по параметрам команды `ping`, после чего выполнен одиночный эхо-запрос в **ICMP-режиме** к узлу **PC1**. В Wireshark был зафиксирован ICMP Echo Request от адреса **192.168.1.12** к **192.168.1.11**, а также соответствующий ICMP Echo Reply в обратном направлении.

В деталях пакета отображаются поля протоколов Ethernet, IPv4 и ICMP, включая тип сообщения, идентификатор, номер последовательности и значение TTL.

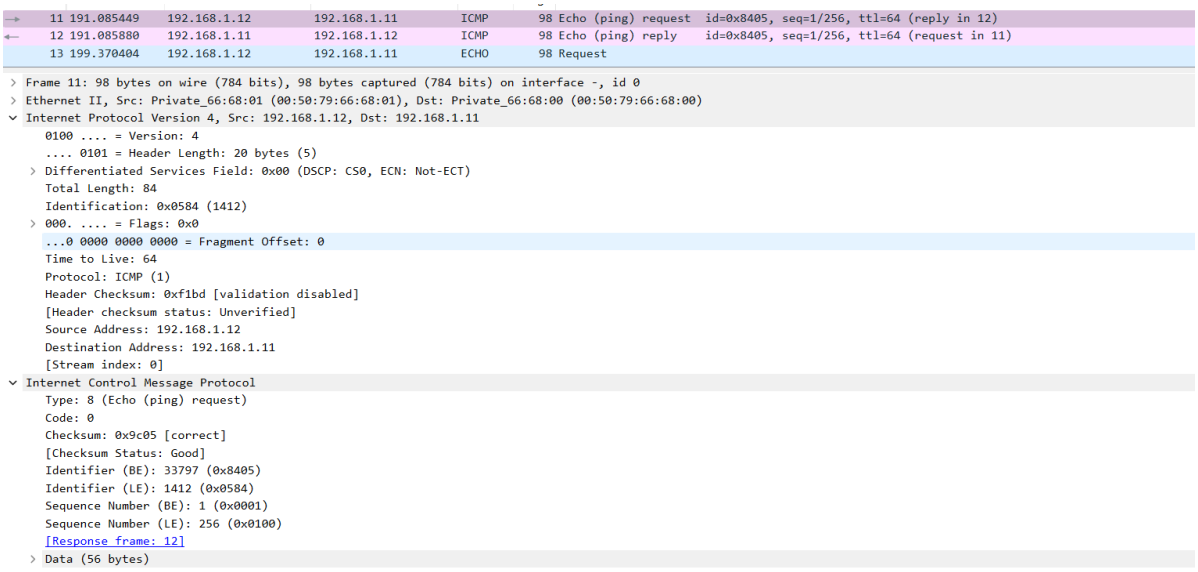

Рис. 2.6: ICMP Echo request и reply

2.2.3 Анализ UDP-сообщений

После этого был выполнен одиночный эхо-запрос в **UDP-режиме**. В Wireshark был зафиксирован UDP-пакет, инкапсулированный в IPv4, с целевым портом **7** (служба Echo). В пакете присутствует полезная нагрузка, возвращаемая получателем.

Анализ показывает, что при использовании UDP отсутствует установление соединения, а обмен данными осуществляется без подтверждения доставки на транспортном уровне.

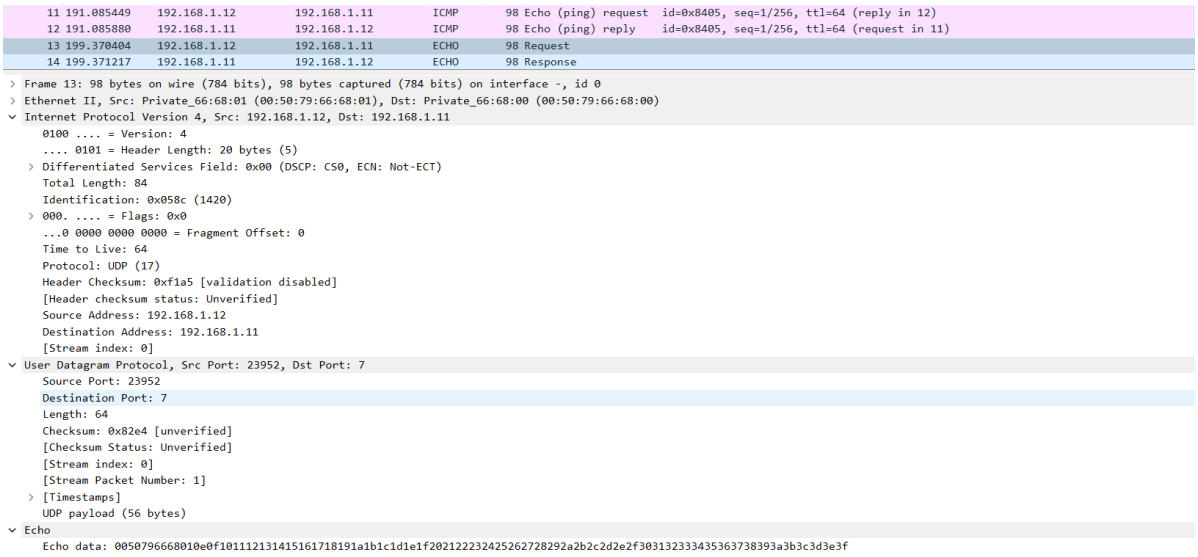

Рис. 2.7: UDP-пакет при ping в UDP-режиме

2.2.4 Анализ TCP-сообщений

При выполнении эхо-запроса в **TCP-режиме** в Wireshark наблюдается полноценная TCP-сессия. Сначала происходит установка соединения с использованием трёхстороннего рукопожатия (SYN, SYN/ACK, ACK), затем передача данных, после чего соединение корректно завершается с помощью сегментов FIN и ACK.

Данный анализ наглядно демонстрирует отличие TCP от ICMP и UDP, а также наличие механизмов установления соединения, подтверждения доставки и корректного завершения сеанса.

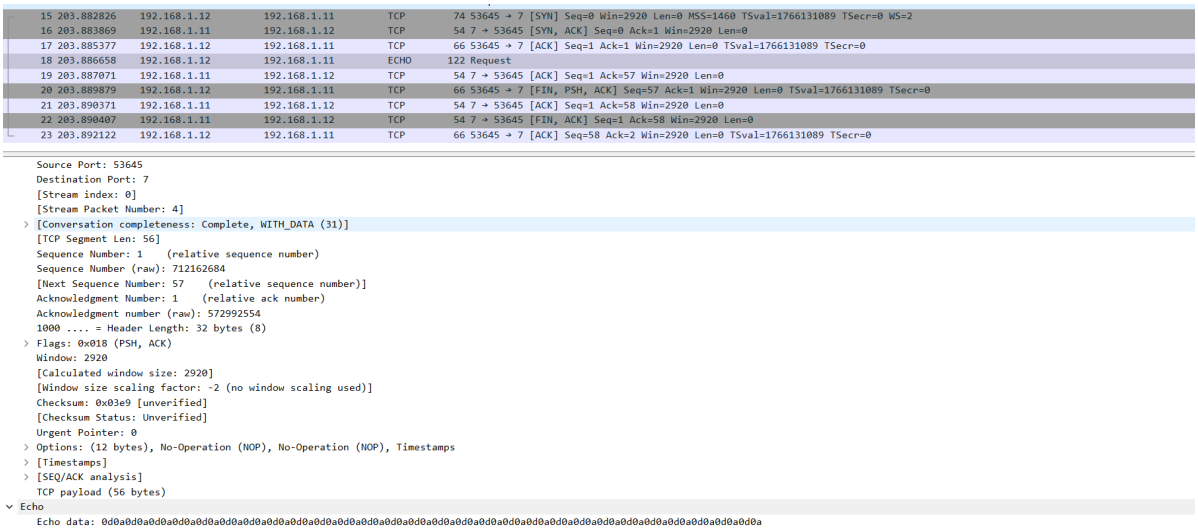

Рис. 2.8: TCP-сессия при ping в TCP-режиме

2.3 Моделирование простейшей сети на базе маршрутизатора FRR в GNS3

В рамках выполнения лабораторной работы в среде **GNS3** была смоделирована простейшая сеть с использованием маршрутизатора **FRR**, Ethernet-коммутатора и одного оконечного устройства **VPCS**. Целью работы являлась настройка базовой IP-адресации и анализ обмена ICMP- и ARP-сообщениями между узлом и маршрутизатором.

2.3.1 Построение топологии сети

В рабочей области GNS3 были размещены следующие устройства: - оконечное устройство **PC1-dgavdadaev**; - Ethernet-коммутатор **msk-dgavdadaev-sw-01**; - маршрутизатор **msk-dgavdadaev-gw-01**.

Устройства были соединены таким образом, что PC1 подключён к коммутатору, а коммутатор — к маршрутизатору. Таким образом, была сформирована локальная сеть с маршрутизатором в роли шлюза по умолчанию.

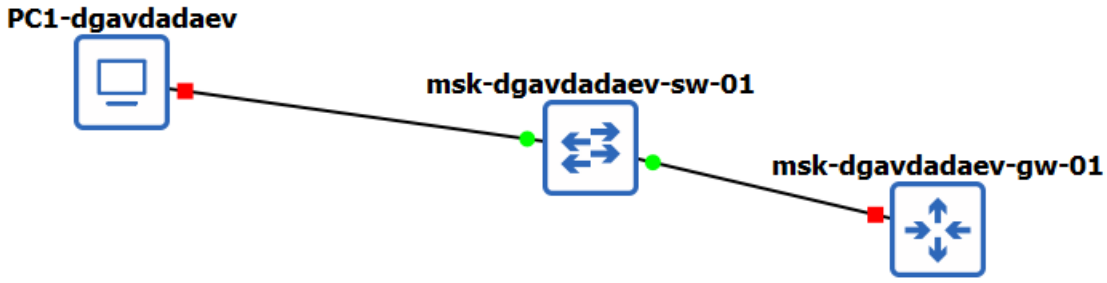

Рис. 2.9: Топология сети с маршрутизатором FRR

2.3.2 Настройка IP-адресации на оконечном устройстве

После запуска всех устройств был открыт терминал **PC1**. Оконечному устройству был назначен IP-адрес **192.168.1.10/24** с указанием шлюза по умолчанию **192.168.1.1**. После ввода параметров конфигурация была сохранена, а затем выполнен просмотр текущих IP-настроек для контроля корректности ввода.

В результате вывода команды отображаются: - IP-адрес узла — 192.168.1.10/24; - адрес шлюза — 192.168.1.1; - MAC-адрес сетевого интерфейса.

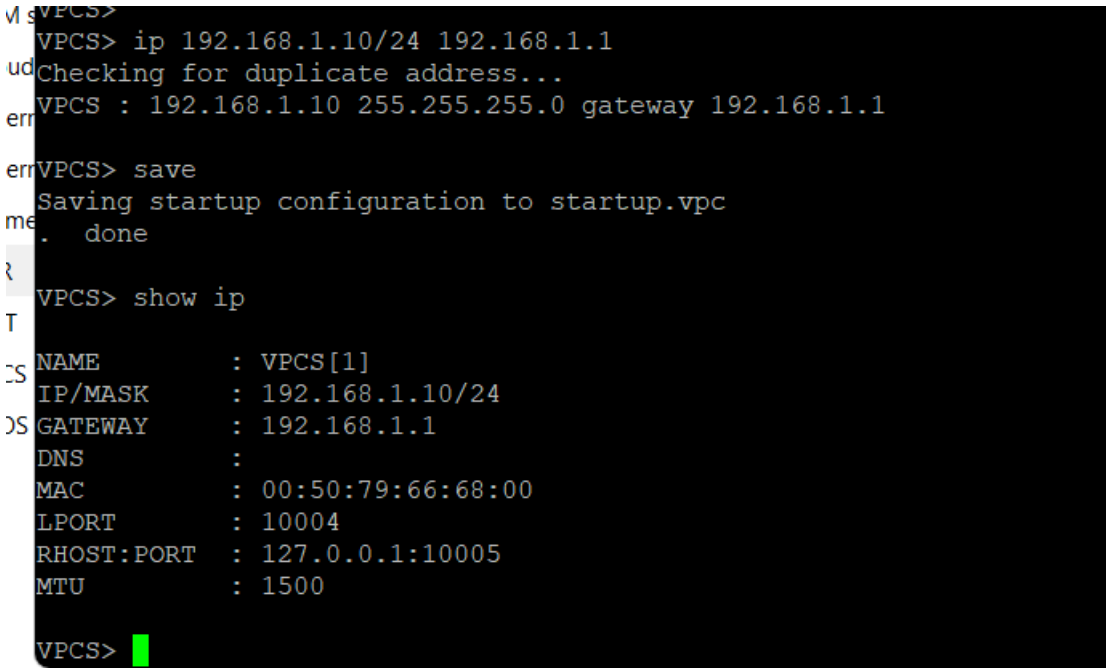

Рис. 2.10: Настройка IP-адресации на PC1

2.3.3 Настройка маршрутизатора FRR

Далее была выполнена настройка маршрутизатора **FRR**. Через консоль маршрутизатора был задан hostname **msk-dgavdadaev-gw-01**, после чего произведена настройка IP-адресации интерфейса локальной сети **eth0**. Интерфейсу был присвоен адрес **192.168.1.1/24**, после чего интерфейс был переведён в активное состояние.

После завершения конфигурации параметры были сохранены в постоянную память.

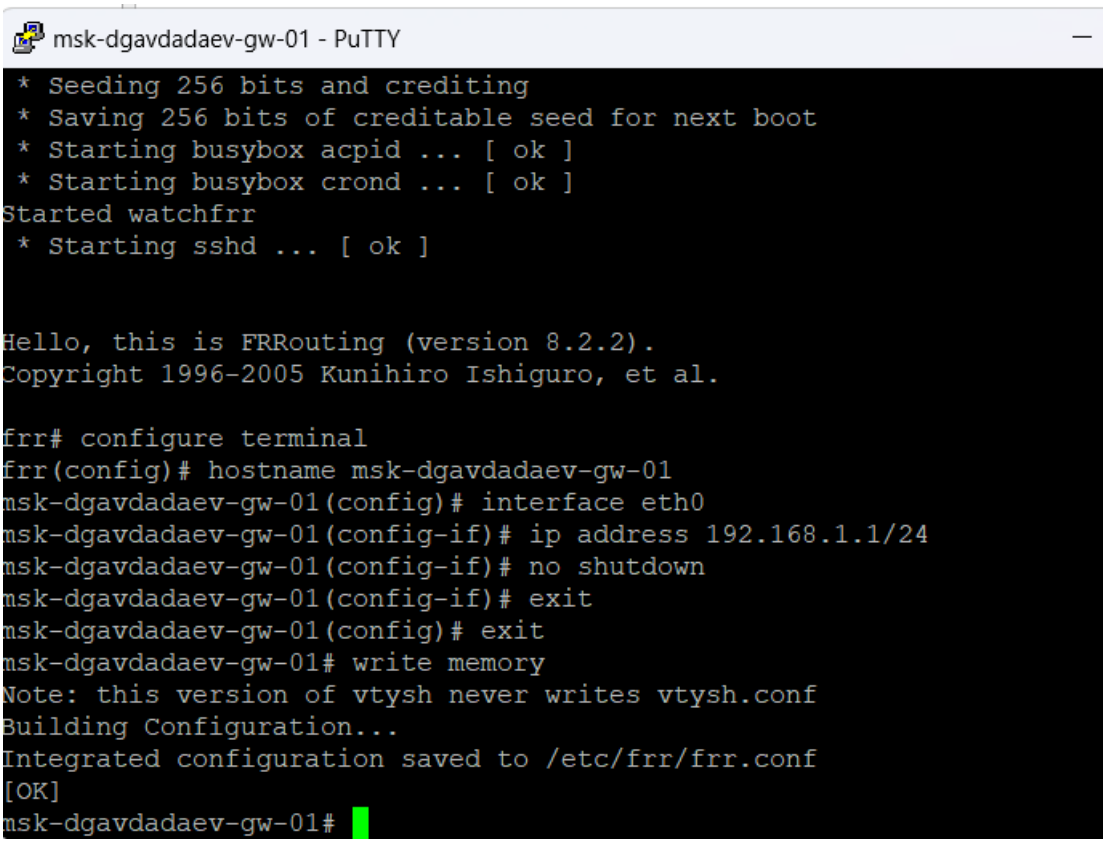

Рис. 2.11: Настройка интерфейса eth0 на маршрутизаторе FRR

2.3.4 Проверка конфигурации маршрутизатора

Для контроля корректности выполненной настройки были просмотрены текущая конфигурация маршрутизатора и краткая информация по интерфейсам. В выводе подтверждается: - наличие настроенного интерфейса **eth0**; - его состояние **up**; - назначенный IP-адрес **192.168.1.1/24**.

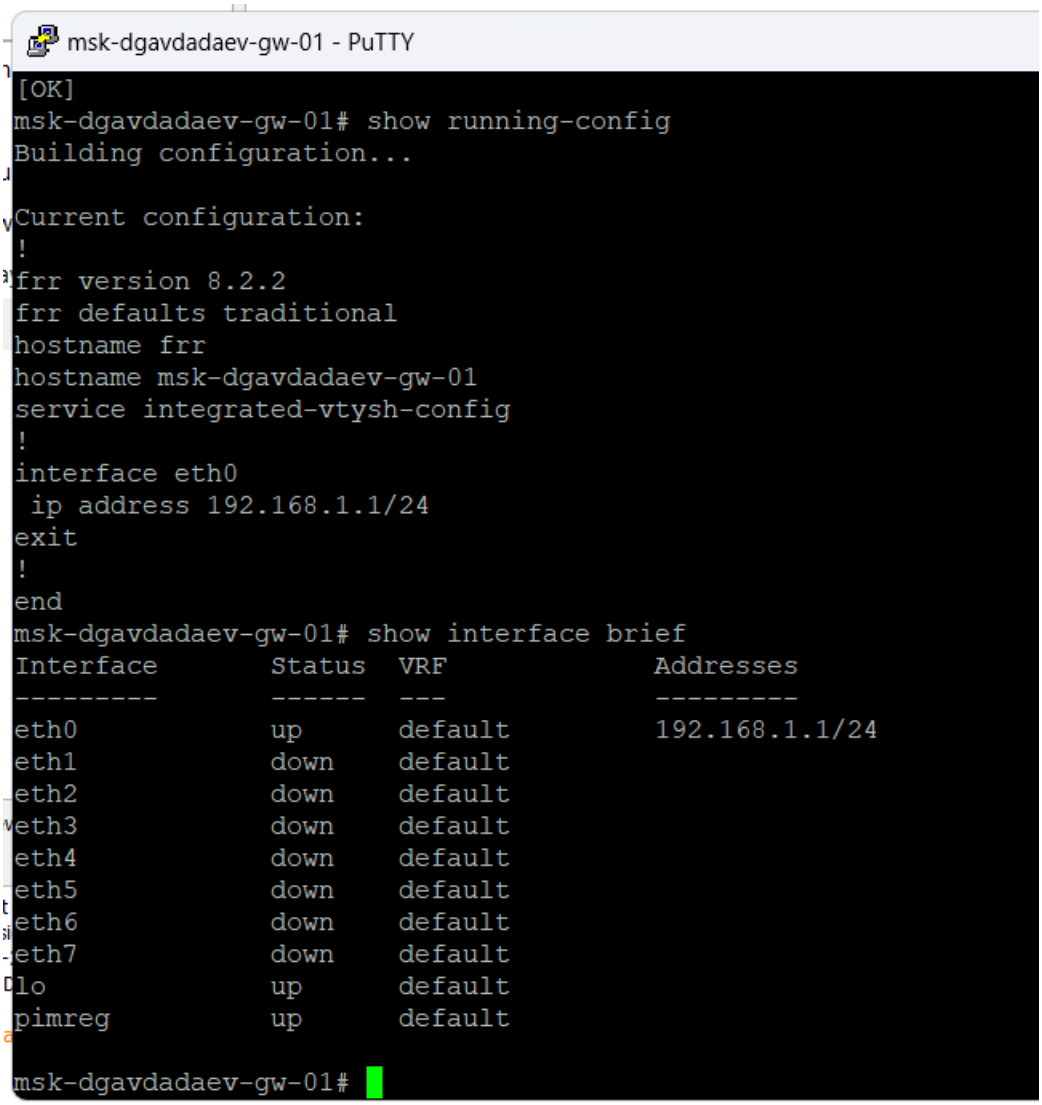

Рис. 2.12: Проверка конфигурации и интерфейсов FRR

2.3.5 Проверка сетевой связности

Для проверки работоспособности сети с оконечного устройства **PC1** был выполнен эхо-запрос к IP-адресу маршрутизатора **192.168.1.1**. В результате были получены ответы на все ICMP-запросы, что подтверждает: - корректную IP-адресацию узла и маршрутизатора; - исправную работу Ethernet-коммутатора; - наличие сетевой связности между PC1 и маршрутизатором.

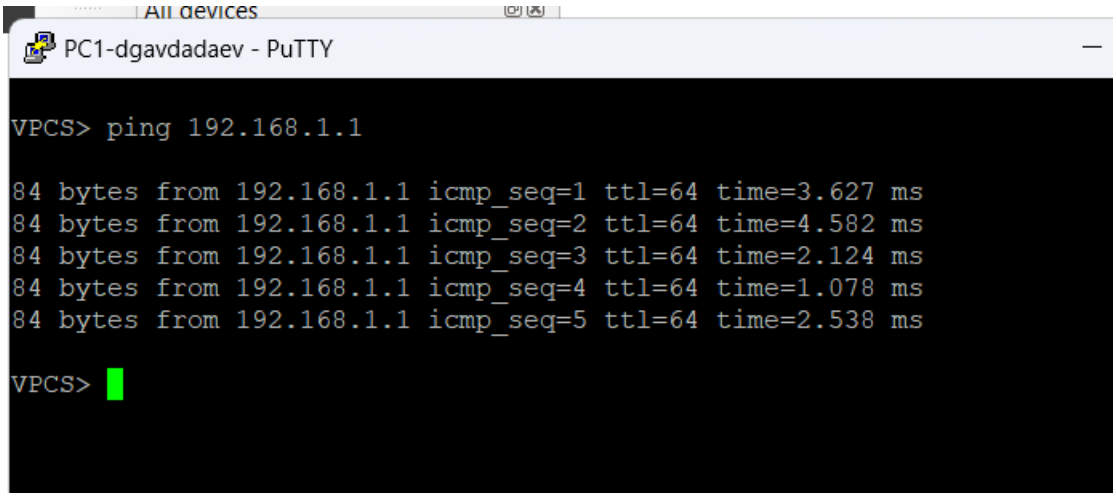

Рис. 2.13: Ping с PC1 на маршрутизатор

2.3.6 Анализ трафика в Wireshark

Во время проверки связности был включён захват трафика на соединении между коммутатором и маршрутизатором. В окне **Wireshark** зафиксированы ARP- и ICMP-сообщения.

В начале обмена наблюдается ARP-запрос от узла **192.168.1.10** с целью определения MAC-адреса узла **192.168.1.1**. В ответ маршрутизатор отправляет ARP-ответ, содержащий свой MAC-адрес. После разрешения ARP выполняется обмен ICMP Echo Request и Echo Reply между PC1 и маршрутизатором.

В деталях ICMP-пакета отображаются стандартные поля протоколов Ethernet, IPv4 и ICMP, включая тип сообщения, идентификатор, номер последовательности и время отклика.

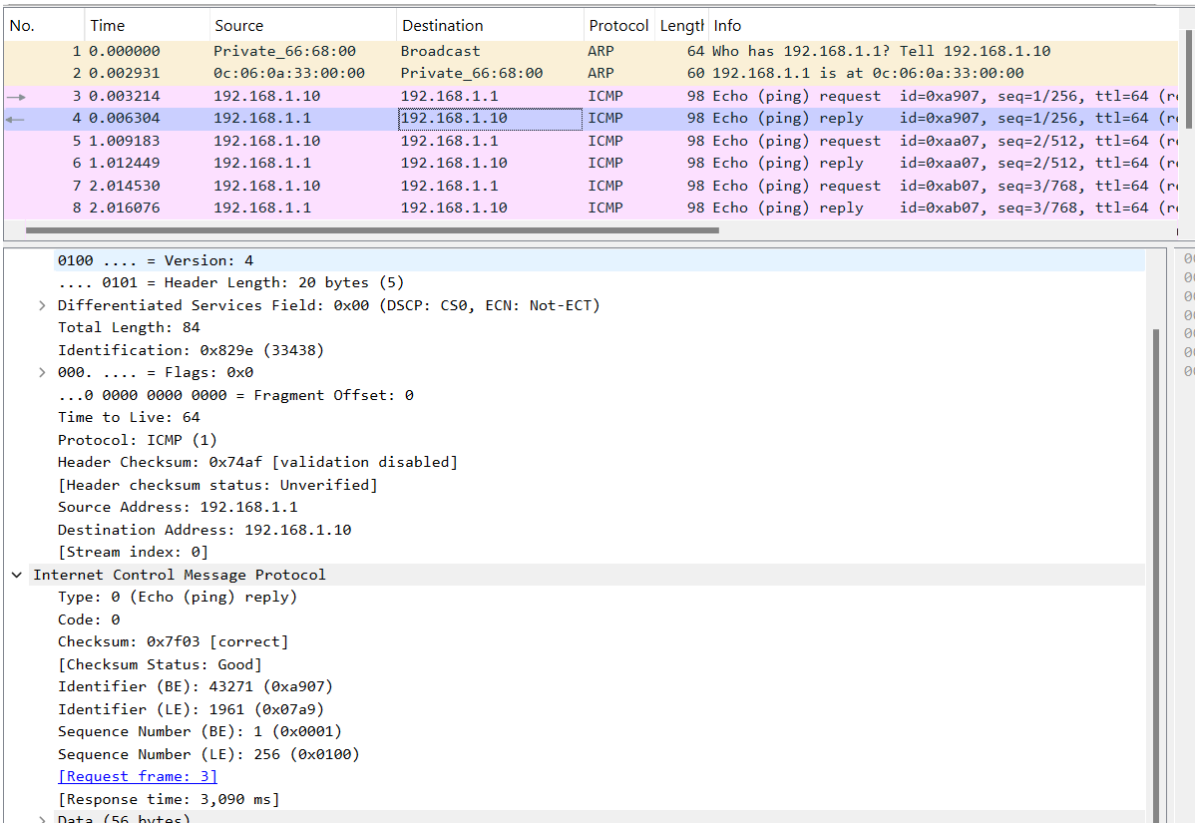

Рис. 2.14: Анализ ARP и ICMP-трафика в Wireshark

2.4 Моделирование простейшей сети на базе маршрутизатора VyOS в GNS3

В рамках выполнения лабораторной работы в среде **GNS3** была смоделирована простейшая сеть с использованием маршрутизатора **VyOS**, Ethernet-коммутатора и одного оконечного устройства **VPCS**. Целью работы являлась настройка базовой IP-адресации, проверка сетевой связности и анализ трафика с использованием анализатора **Wireshark**.

2.4.1 Построение топологии сети

В рабочей области GNS3 были размещены следующие устройства: - оконечное устройство **PC1-dgavdadaev**; - Ethernet-коммутатор **msk-dgavdadaev-sw-01**; - маршрутизатор **msk-dgavdadaev-gw-01** на базе VyOS.

Оконечное устройство было подключено к коммутатору, а коммутатор — к маршрутизатору. Таким образом, была сформирована локальная сеть с маршрутизатором VyOS в роли шлюза по умолчанию.

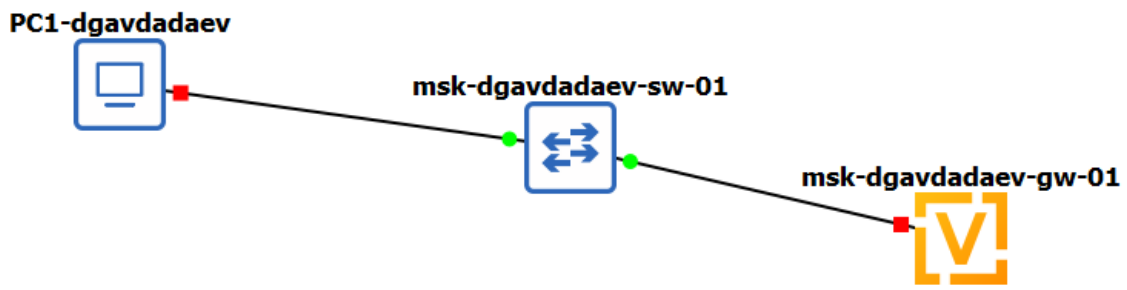

Рис. 2.15: Топология сети с маршрутизатором VyOS

2.4.2 Настройка IP-адресации на оконечном устройстве

После запуска всех устройств проекта была открыта консоль **PC1**. Оконечному устройству был назначен IP-адрес **192.168.1.10/24** с указанием шлюза по умолчанию **192.168.1.1**. После ввода параметров конфигурация была сохранена, а затем выполнен просмотр текущих IP-настроек для контроля корректности конфигурации.

В выводе отображаются назначенный IP-адрес, маска сети, адрес шлюза и MAC-адрес интерфейса.

2.4.3 Настройка маршрутизатора VyOS

После загрузки маршрутизатора VyOS был выполнен вход под стандартной учётной записью. Далее произведён переход в режим конфигурирования. В конфигурации маршрутизатора были выполнены следующие действия: - изменено имя устройства на **msk-dgavdadaev-gw-01**; - на интерфейсе **eth0** задан IP-адрес **192.168.1.1/24**; - удалена настройка получения адреса по DHCP; - просмотрены изменения в конфигурации; - применены и сохранены внесённые изменения.

После сохранения конфигурации был выполнен просмотр информации об интерфейсах маршрутизатора, что позволило убедиться в наличии назначенного IP-адреса и корректном состоянии интерфейса **eth0**.

Процесс настройки маршрутизатора VyOS и вывод информации об интерфейсах представлен на рисунке ниже.

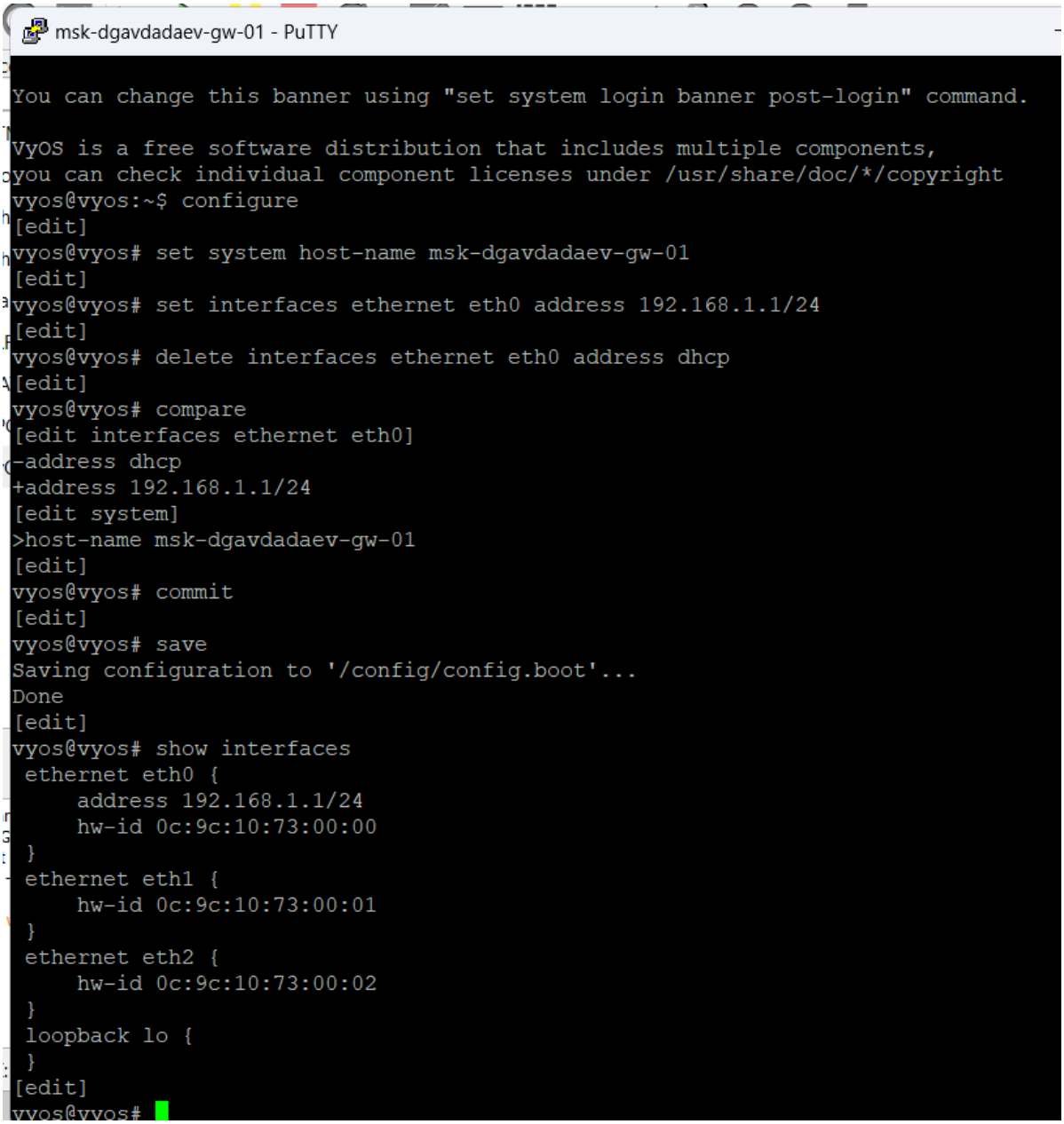

Рис. 2.16: Настройка и проверка интерфейсов маршрутизатора VyOS

2.4.4 Проверка сетевой связности

Для проверки работоспособности сети с оконечного устройства **PC1** был выполнен эхо-запрос к IP-адресу маршрутизатора **192.168.1.1**. В результате были получены ответы на все ICMP-запросы, что подтверждает корректную настрой-

ку IP-адресации и работоспособность сетевого взаимодействия между узлом и маршрутизатором.

Результат выполнения проверки связности представлен на рисунке ниже.

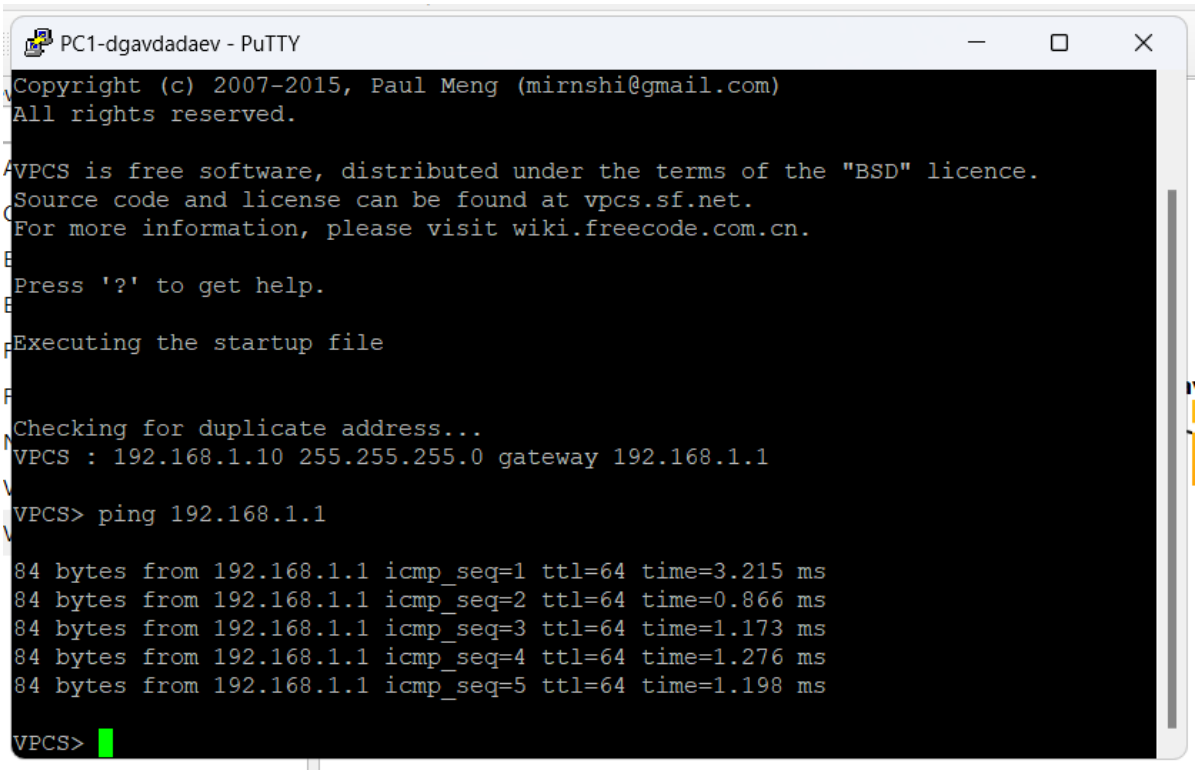

Рис. 2.17: Ping с PC1 на маршрутизатор VyOS

2.4.5 Анализ трафика в Wireshark

На соединении между коммутатором и маршрутизатором был включён захват трафика. В окне **Wireshark** были зафиксированы ARP- и ICMP-сообщения, возникающие в процессе проверки связности.

В начале обмена наблюдается ARP-запрос от узла **192.168.1.10**, направленный на определение MAC-адреса узла с IP **192.168.1.1**. В ответ маршрутизатор VyOS отправляет ARP-ответ, содержащий свой MAC-адрес. После завершения ARP-разрешения в трассировке фиксируются ICMP Echo Request и Echo Reply, подтверждающие успешный обмен данными.

В деталях ICMP-пакета отображаются основные поля протоколов Ethernet, IPv4

и ICMP, включая тип сообщения, идентификатор, номер последовательности и время отклика.

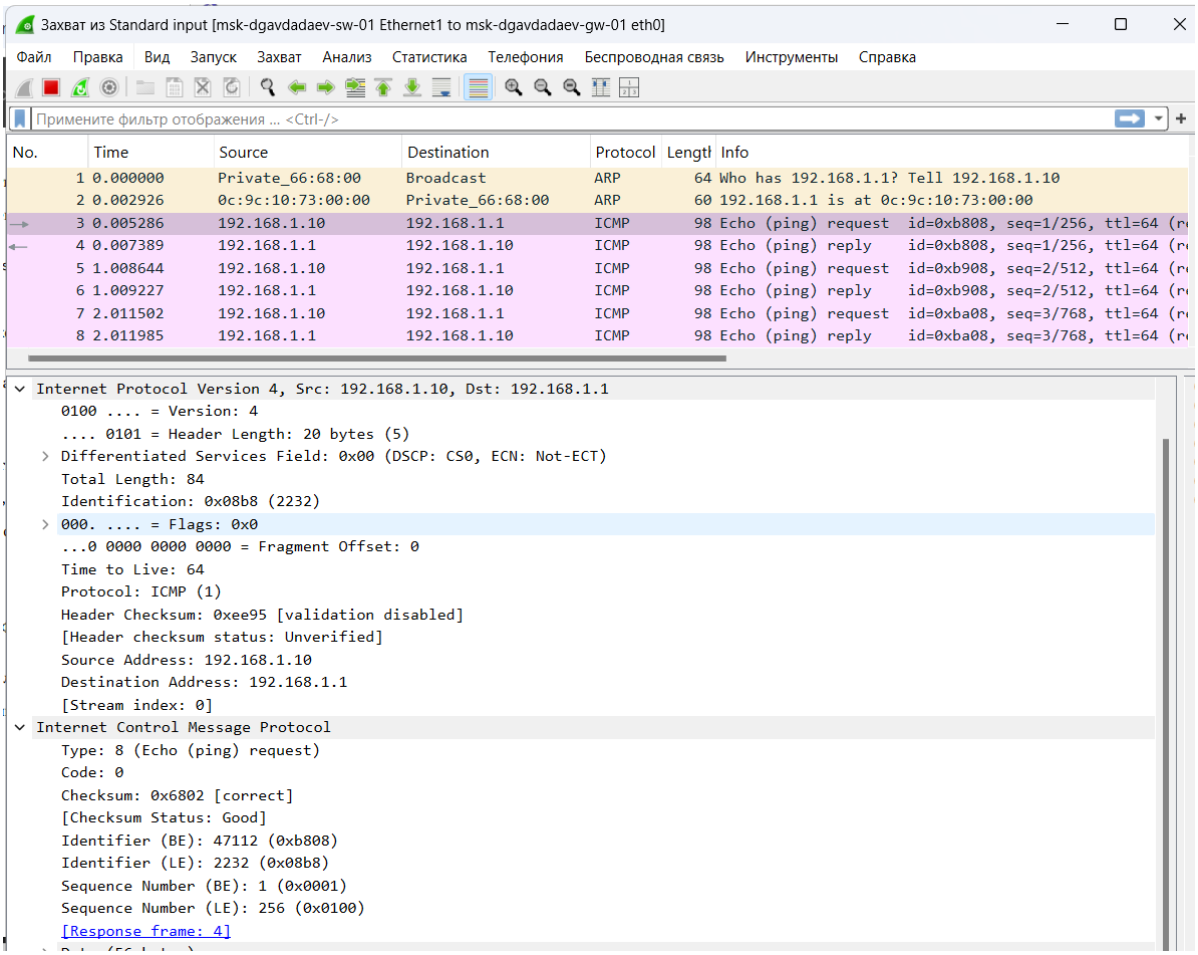

Рис. 2.18: Ping с PC1 на маршрутизатор VyOS

3 Заключение

В ходе выполнения лабораторной работы была освоена базовая настройка и моделирование простейших локальных сетей в среде GNS3 с использованием Ethernet-коммутаторов, оконечных устройств VPCS, а также маршрутизаторов на базе FRR и VyOS. Были построены сетевые топологии различной сложности, выполнена настройка IP-адресации и проверена корректность сетевого взаимодействия между узлами.

В процессе работы подтверждена работоспособность протоколов ARP и ICMP, а также на практике изучены особенности обмена данными при использовании различных режимов эхо-запросов. С помощью анализатора Wireshark был выполнен захват и разбор сетевого трафика, что позволило наглядно проследить процесс разрешения MAC-адресов и передачи ICMP-сообщений.