**Министерство науки и высшего образования Российской Федерации** ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

# НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

**Факультет безопасности информационных технологий Дисциплина:**

«Компьютерные сети»

# ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

«Основы администрирования маршрутизируемых компьютерных сетей»

# Выполнили:

Ахраров Али, студент группы N3350



# Проверил:

Есипов Дмитрий Андреевич

(отметка о выполнении)

(подпись)

Санкт-Петербург

# СОДЕРЖАНИЕ

[Введение 4](#_bookmark0)

1. [Общая часть задания 5](#_bookmark1)

[Выбор варианта 5](#_bookmark2)

* 1. [Настройка IPv4 6](#_bookmark3)
  2. [Формирование таблиц маршрутизации 7](#_bookmark4)
  3. [Работа с утилитой nc 9](#_bookmark5)
  4. [Настройка iptables 10](#_bookmark6)
     1. [Запретить передачу TCP-пакетов на порт, использованный в nc 10](#_bookmark7)
     2. [Запретить прием UDP-пакетов с порта, использованного в nc 10](#_bookmark8)
     3. [Запретить передачу пакетов с IP-адреса машины А 10](#_bookmark9)
     4. [Запретить прием пакетов на IP-адрес машины Б 10](#_bookmark10)
     5. [Запретить ICMP-пакеты с размером больше 1000 байт и TTL меньше 10 11](#_bookmark11)
  5. [Проверка работоспособности правил iptables 12](#_bookmark12)

[Заключение 16](#_bookmark13)

# ВВЕДЕНИЕ

Цель работы – изучение основных методов настройки маршрутизируемых компьютерных сетей на примере сети, состоящей из компьютеров под управлением ОС Linux.

Для достижения поставленной цели необходимо решить следующие задачи:

− провести теоретический анализ сетевого уровня модели OSI, включая его основные функции и протоколы, применяемые в маршрутизируемых сетях;

− выполнить базовую настройку сетевых интерфейсов и связности между компьютерами в сети, чтобы обеспечить возможность обмена данными;

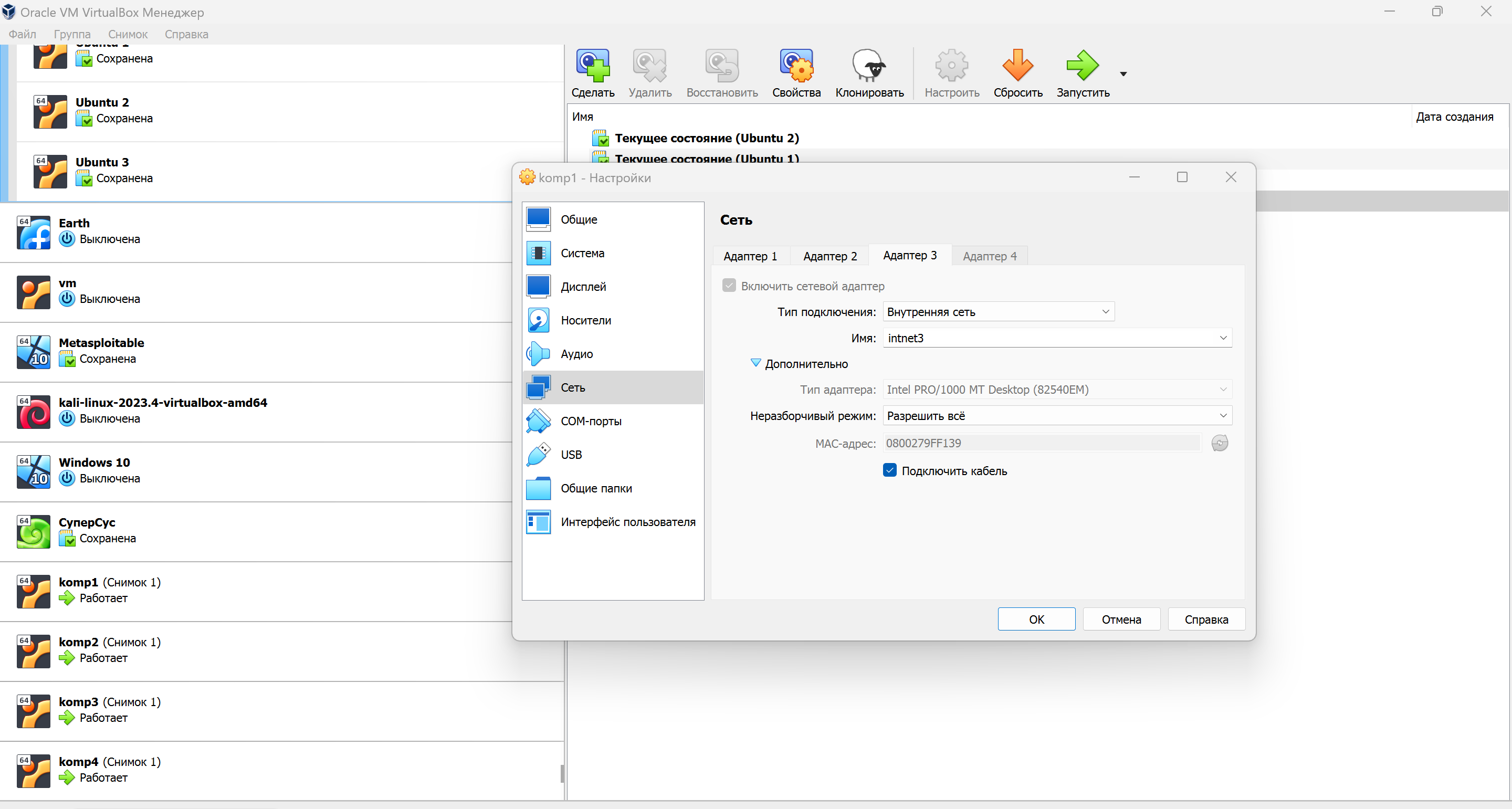
− исследовать и настроить таблицы маршрутизации для корректной передачи пакетов в сети, включая маршрутизацию для IPv4 и IPv6;

− использовать утилиту tcpdump для наблюдения за сетевым трафиком, анализируя проходящие пакеты и их внутреннюю структуру, а также изучить применение технологии NAT.

# ОБЩАЯ ЧАСТЬ ЗАДАНИЯ

Начнем с установки VirtualBox и образов нужных виртуальных машин: мы будем использовать Ubuntu 22.04.3. VirtualBox с установленными машинами и их сетевыми настройками будет выглядеть так:

Рисунок 1 – Установленные машины и их сетевые настройки



# Выбор варианта

Меня зовут Ахраров (7 букв) Али (3 буквы), так что мои варианты: N = 6 + 3 = 10, V1 = 1 + (10 mod 5) = 1, V2 = 6 + (10 mod 5) = 6.

# Настройка IPv4

Настроим IPv4-адреса на всех компьютерах сети. В качестве доказательства настройки приведем результаты выполнения команды ifconfig на всех машинах

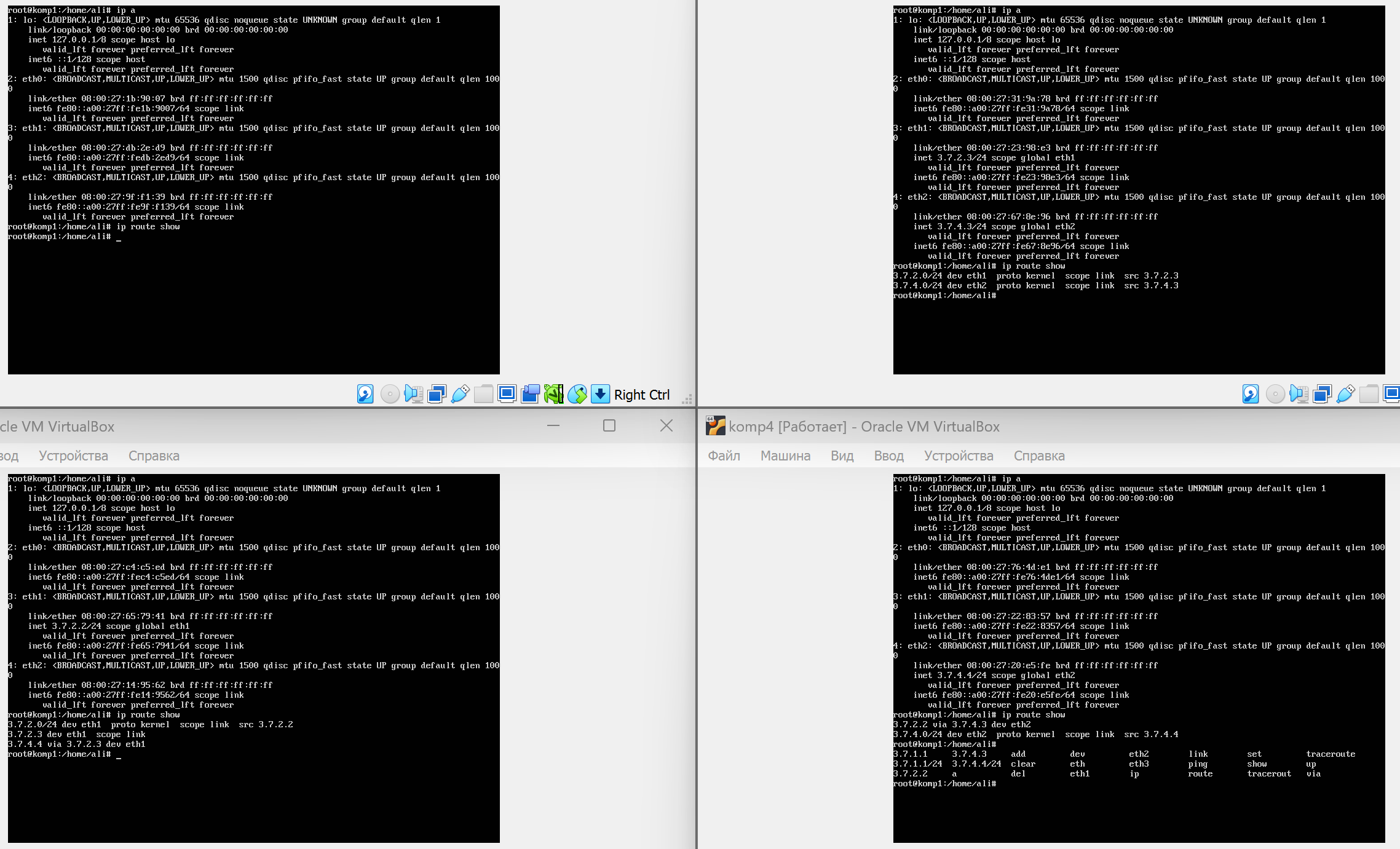


Рисунок 2 – Результат выполнения команды «ip a» и «ip route show» на всех машинах

Была получена следующая топология с поднятыми интерфейсами и IP-адресами:

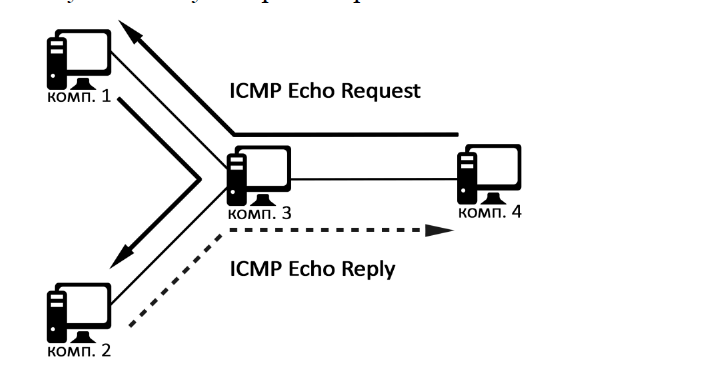
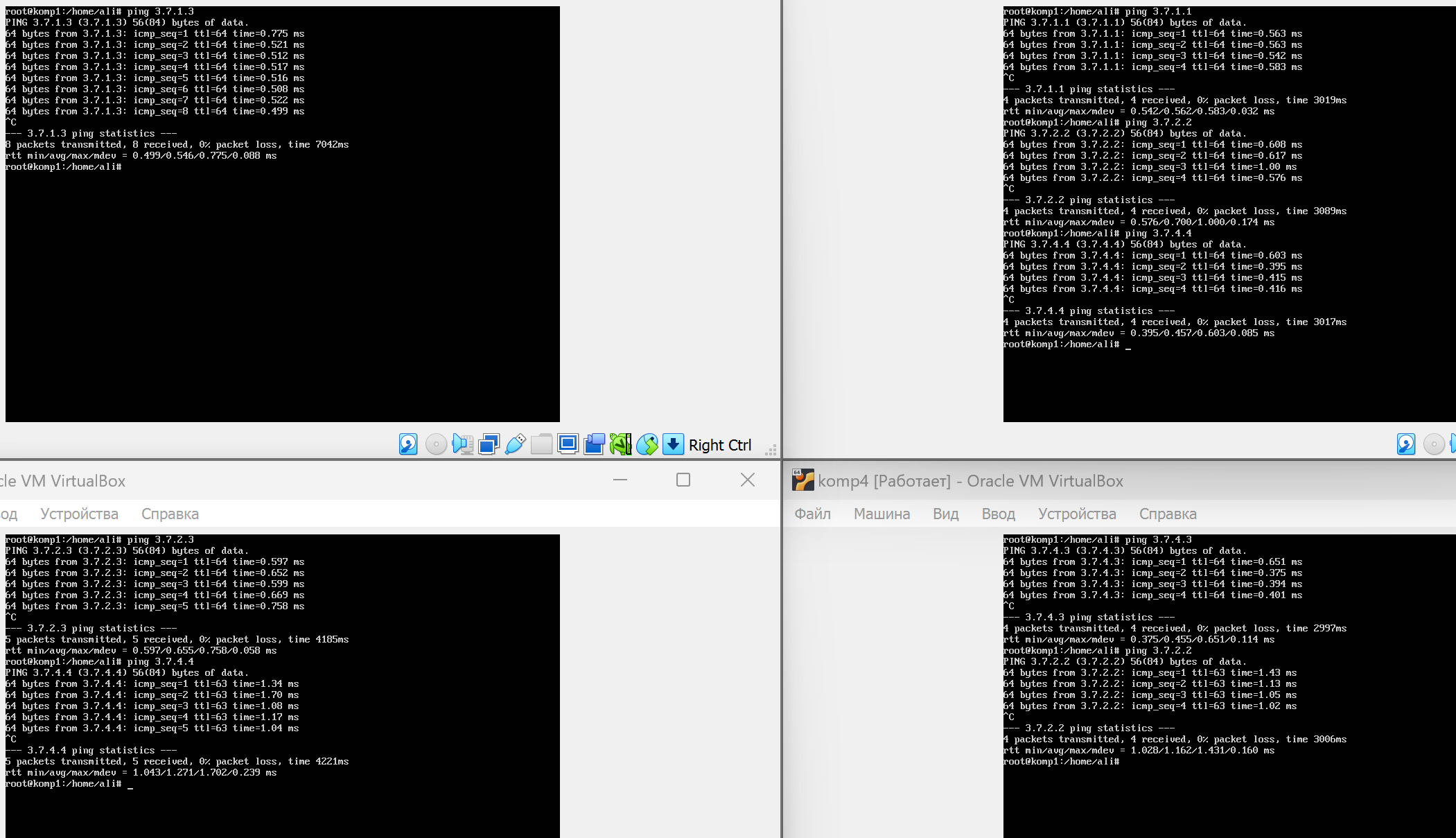


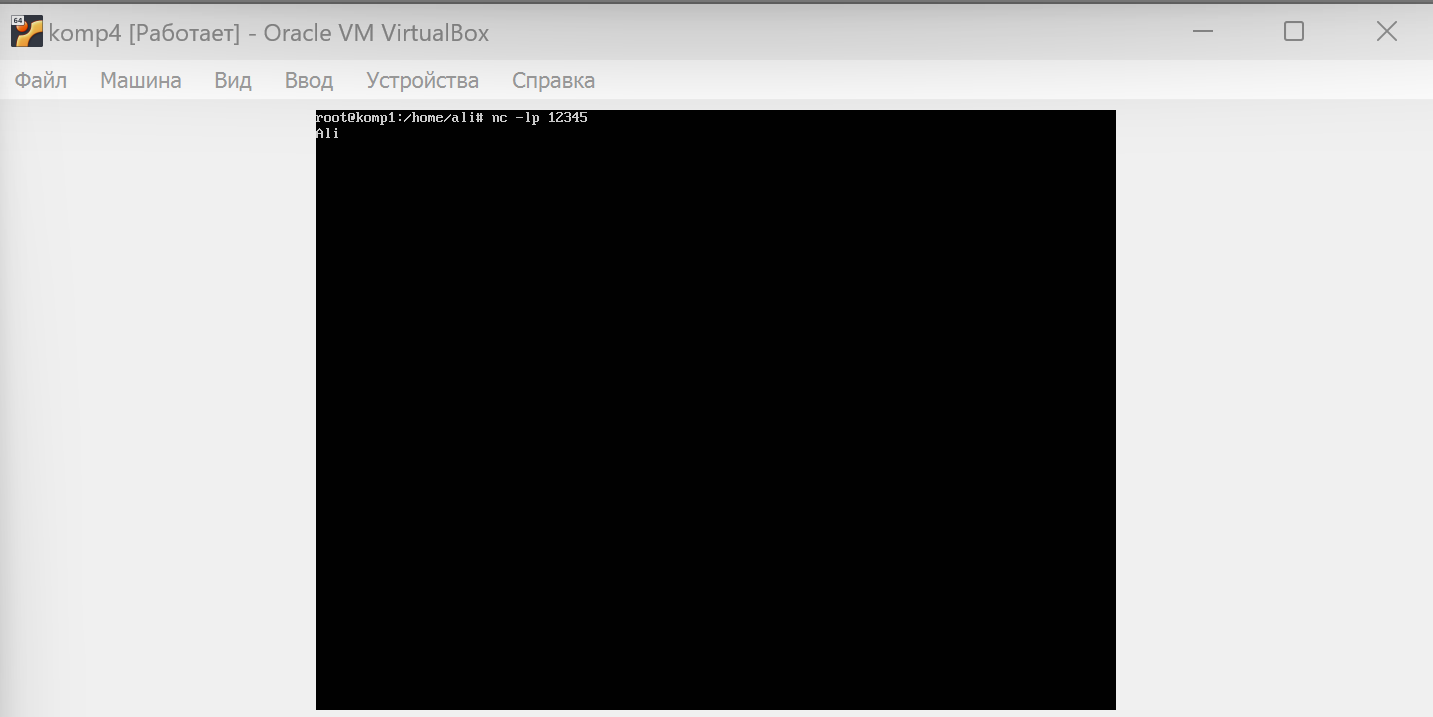
Рисунок 3 – Полученная топология

Теперь продемонстрируем, исходная машина может «пинговать» целевую машину:



# Работа с утилитой nc

Для тестирования работы утилиты nc выберем comp4 и comp2 (в нашей нотации) как самые удаленные. Итак, проверим ее работу:



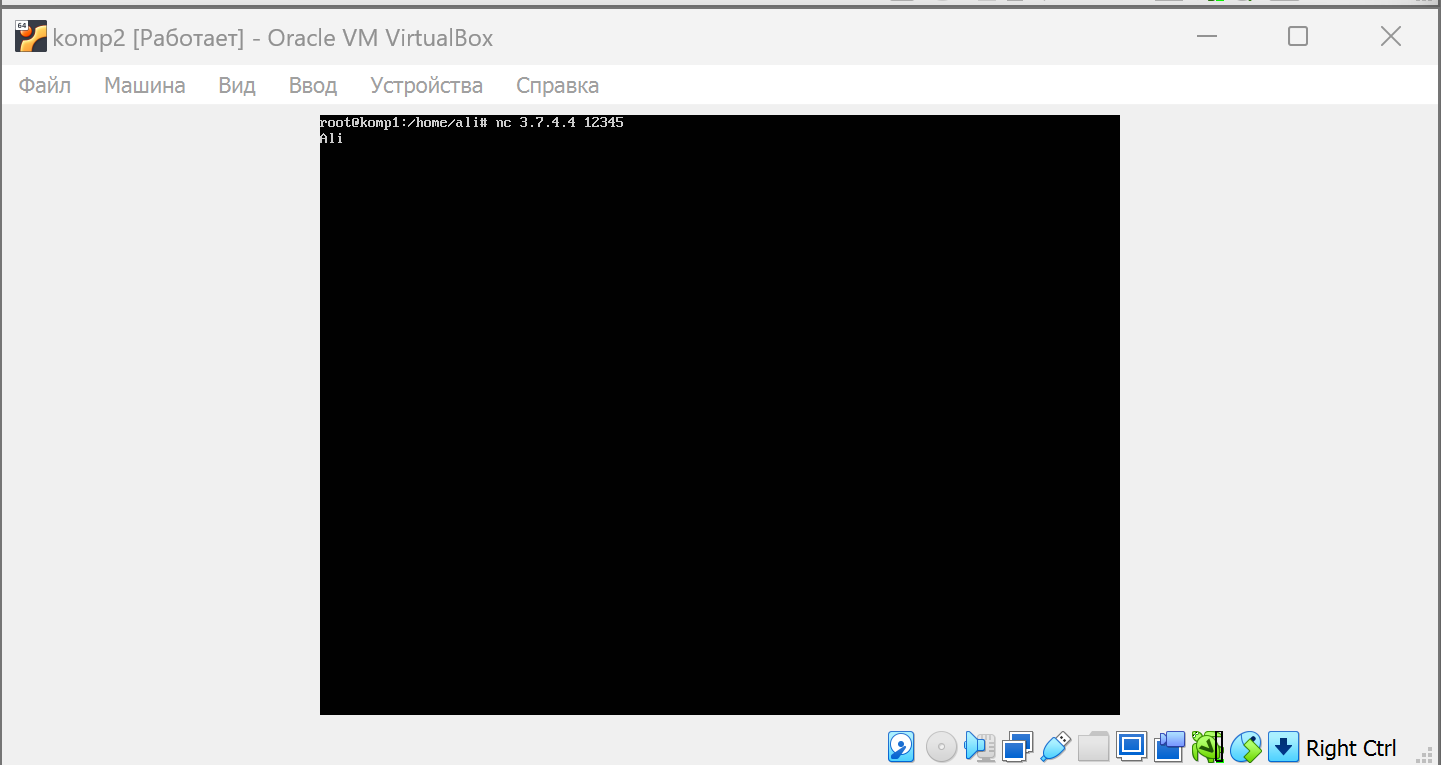


Рисунок 6 – Выполнили передачу сообщения с помощью утилиты nc

# Настройка iptables

# Запретить передачу TCP-пакетов на порт, использованный в nc

На обеих машинах, чтобы запретить передачу TCP-пакетов на указанный порт, выполним:

Листинг 2 – Запрет передачи TCP-пакетов

iptables -A OUTPUT -p tcp --dport 12345 -j DROP

# Запретить передачу TCP-пакетов, отправленных на порт 12345

# Запретить прием UDP-пакетов с порта, использованного в nc

Если nc использовал бы UDP-порт, для запрета приема UDP-пакетов с этого порта выполните:

Листинг 3 – Запрет приема UDP-пакетов

iptables -A INPUT -p udp --sport 12345 -j DROP

# Запретить прием UDP-пакетов, отправленных с порта 12345

# Запретить передачу пакетов с IP-адреса машины А

На машине Б выполним команду для запрета всех пакетов, приходящих с IP-адреса машины А (например, 192.7.1.1):

Листинг 4 – Запрет приема пакетов с конкретного адреса

iptables -A INPUT -s 6.7.2.1 -j DROP

# Запретить прием пакетов с IP-адреса 192.7.1.1

# Запретить прием пакетов на IP-адрес машины Б

На машине А выполним команду для запрета всех пакетов, отправляемых на IP- адрес машины Б (например, 192.7.1.2):

Листинг 5 – Запрет отправки пакетов на конкретный адрес

iptables -A OUTPUT -d 6.7.4.2 -j DROP

# Запретить отправку пакетов на IP-адрес 192.7.1.2

# Запретить ICMP-пакеты с размером больше 1000 байт и TTL меньше 10

На обеих машинах выполним команду для фильтрации таких ICMP-пакетов: Листинг 6 – Запрет передачи пакетов, удовлетворяющих некоторым требованиям

iptables -A INPUT -p icmp --icmp-type echo-request -m length --length 1001:65535 -m ttl --ttl-lt 10 -j DROP

# Запретить ICMP-запросы, превышающие 1000 байт и TTL меньше 10

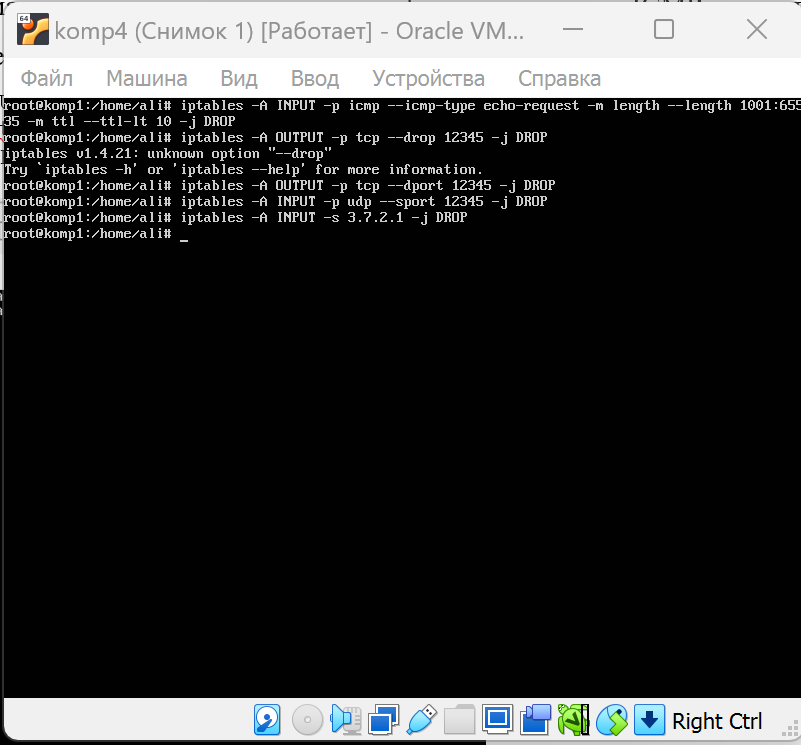
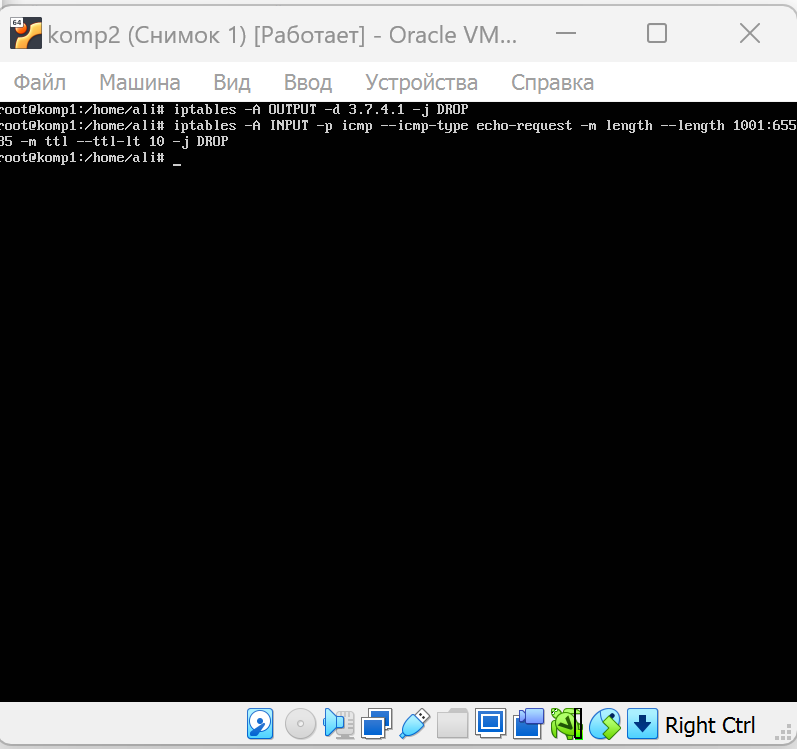


Рисунок 7 – Завершили настройку iptables

# Проверка работоспособности правил iptables

Теперь проверим, работают ли наши правила, так как доступность мы уже проверили.

Для начала видим, что между теми же машинами уже не удалось установить соединение с помощью nc:

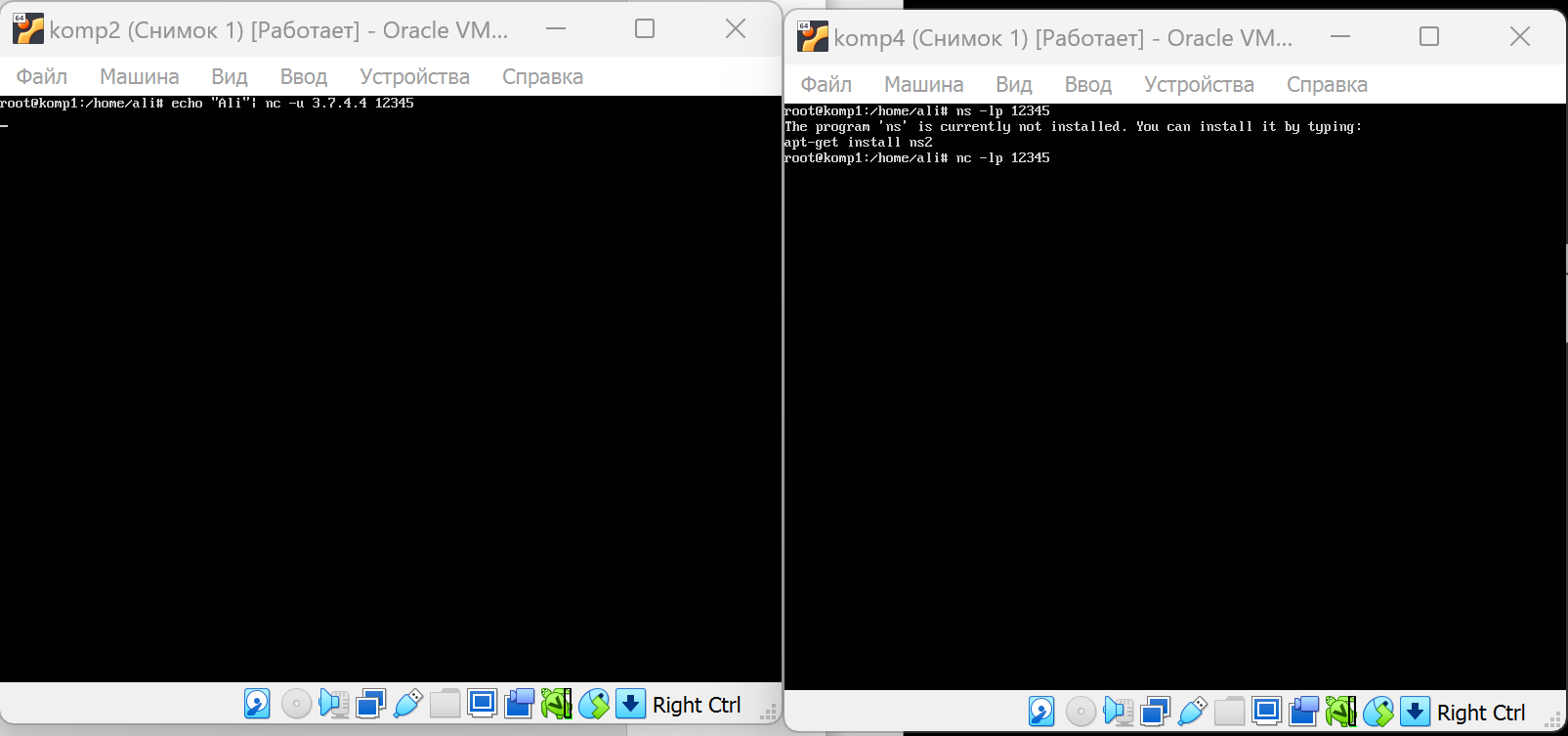
Видим неудачу в передаче сообщения с помощью nc с использованием UDP- пакетов: 

Рисунок 9 – Неудача в передаче сообщения через UDP-пакеты

Дальше пытаемся отправить пакеты с comp2 на comp4, не удовлетворяющие настройке iptables на comp4, и терпим неудачу:

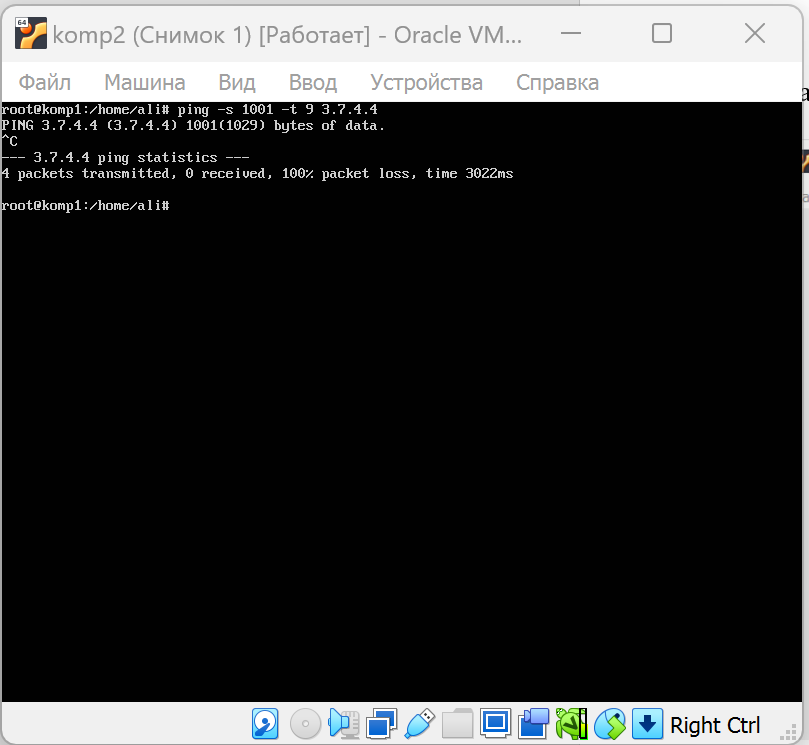


Рисунок 11 – Неудача из-за размера пакетов и малого TTL

А теперь продемонстрируем, что при другим параметрах пакета он принимается:

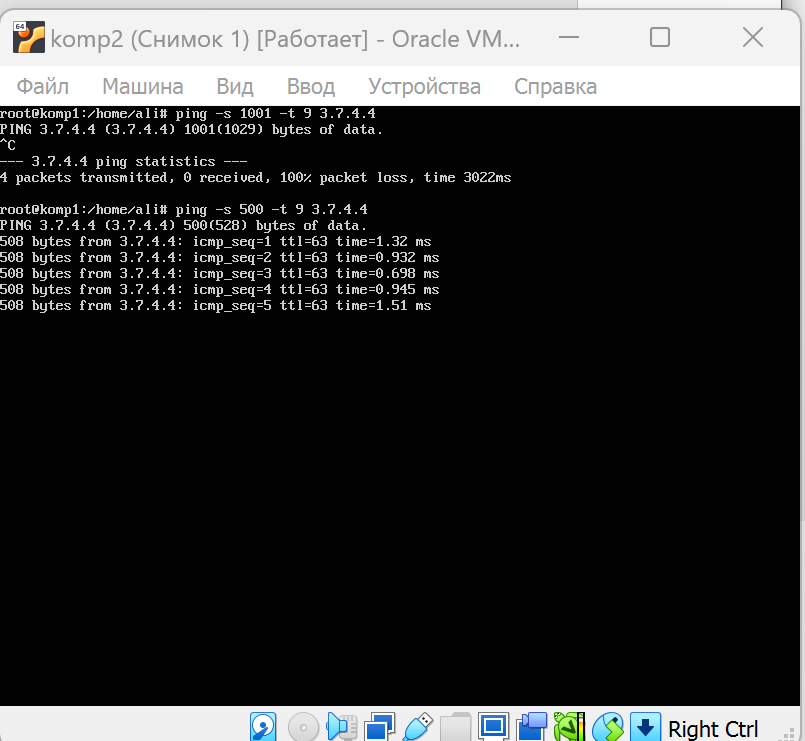


Рисунок 12 – Пакет, удовлетворяющий параметрам, принят

# ЗАКЛЮЧЕНИЕ

В ходе работы были изучены основные аспекты сетевого уровня модели OSI, включая его функции и протоколы, применяемые в маршрутизируемых сетях. Выполнена базовая настройка сетевых интерфейсов для обеспечения связности между компьютерами. Настроены таблицы маршрутизации для корректной передачи пакетов как в сетях IPv4, так и IPv6. Исследован и применен анализ сетевого трафика с помощью утилиты tcpdump, а также изучена технология NAT и её роль в маршрутизации пакетов.