**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

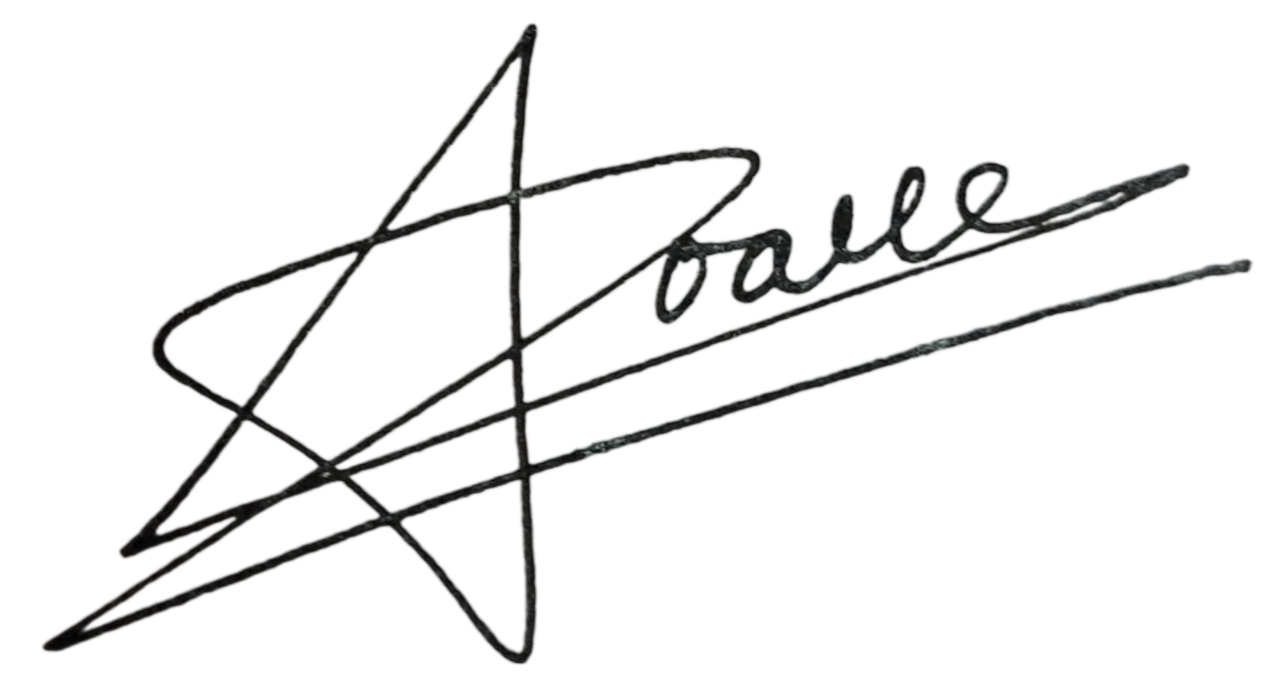
**Дисциплина:**

«Компьютерные сети»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3**

«Основы администрирования маршрутизируемых компьютерных сетей»

**Выполнили:**

Чу Ван Доан, студент группы N3347

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Есипов Дмитрий Андреевич

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

# Содержание

[1 ХОД РАБОТЫ 4](#_heading=h.30j0zll)

[1.1 Настройка IPv4 4](#_heading=h.7n6fsycnmhke)

[1.2 Работа с утилитой nc 6](#_heading=h.kn9m3665lt2f)

[1.3 Настройка iptables 7](#_heading=h.dhhfcoqs4y6h)

[1.4 Проверка работоспособности правил iptables](#_heading=h.s0ur16u1mnbt) 8

# 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:**

1. Провести теоретический анализ сетевого уровня модели OSI, включая его основные функции и протоколы, применяемые в маршрутизируемых сетях.
2. Выполнить базовую настройку сетевых интерфейсов и связности между компьютерами в сети, чтобы обеспечить возможность обмена данными.
3. Исследовать и настроить таблицы маршрутизации для корректной передачи пакетов в сети, включая маршрутизацию для IPv4 и IPv6.
4. Использовать утилиту **tcpdump** для наблюдения за сетевым трафиком, анализируя проходящие пакеты и их внутреннюю структуру, а также изучить применение технологии NAT.

## ХОД РАБОТЫ

Выбор варианта:

Меня зовут Чу Ван (5 букв)

V1 = 1 + (N mod 5) = 1 + (5 mod 5) = 1

V2 = 6 + (N mod 5) = 6 + (5 mod 5) = 6

Я выбираю операционную систему Ubuntu версии 14.04.6 Server.

VirtualBox с установленными машинами и их сетевыми настройками будет выглядеть так:

|  |  |
| --- | --- |
|  |  |

Рисунок 1 – Установленные машины и их сетевые настройки

### 1.1 Настройка IPv4

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

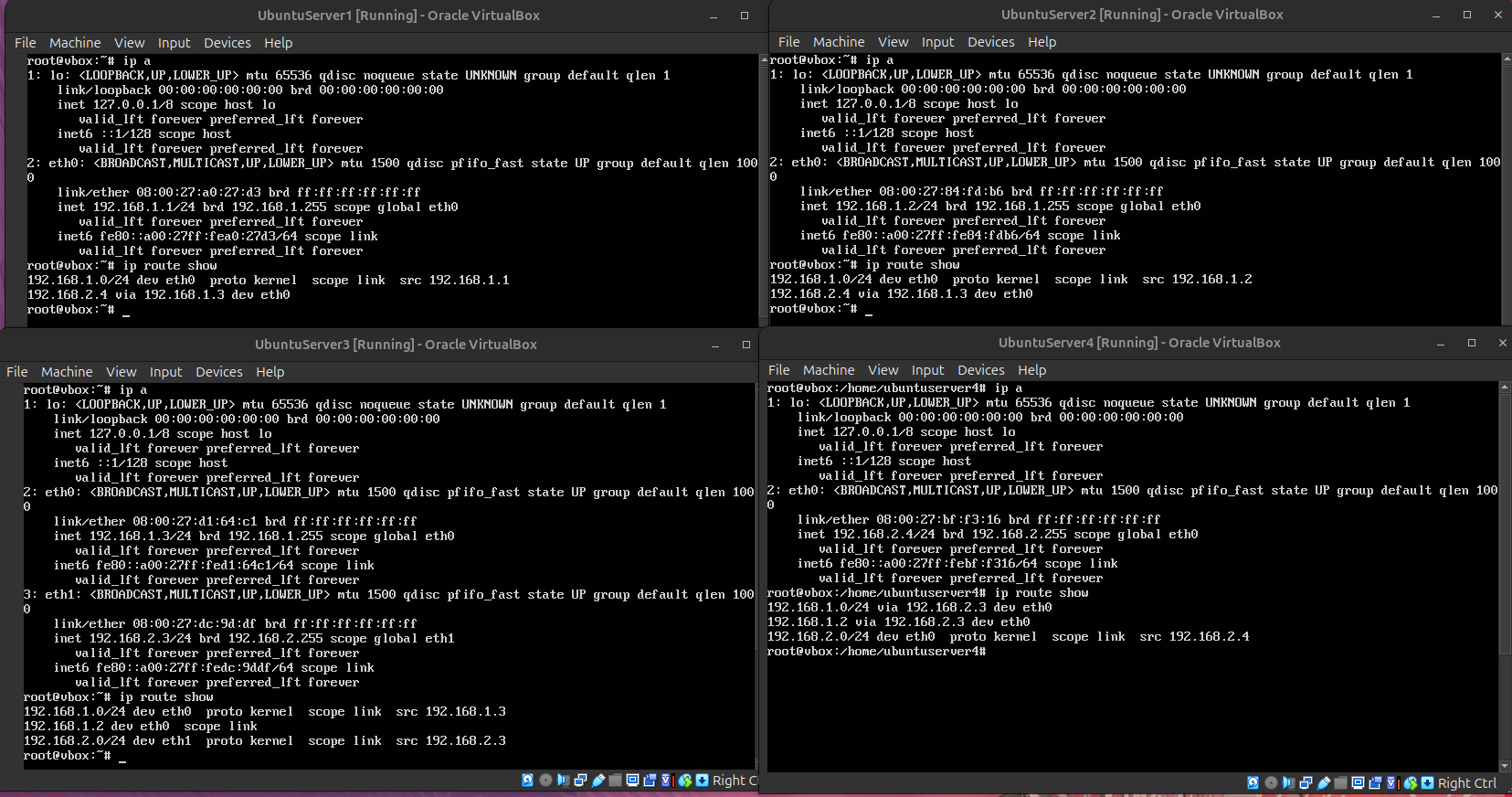


Рисунок 2 – Результат выполнения команды «ip a» и «ip route show» на всех машинах

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

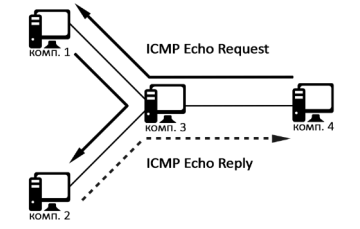


Рисунок 3 – Полученная топология

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

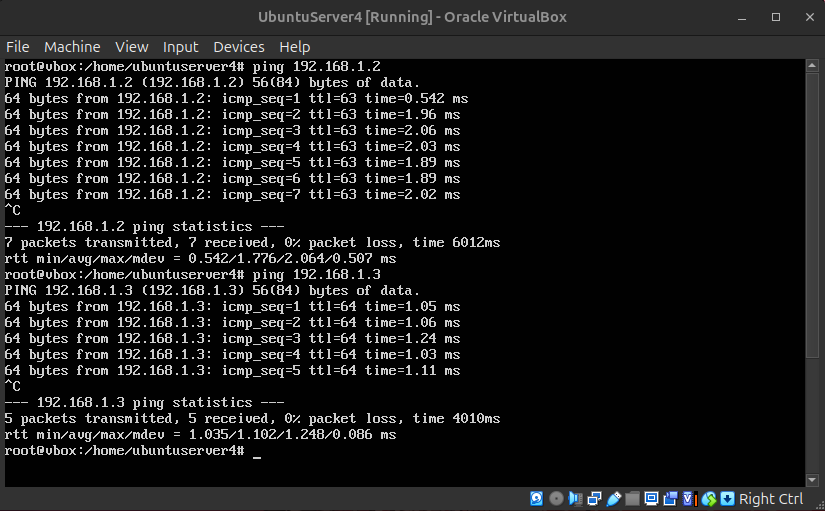


Рисунок 4 – С машины 4 выполните команду **ping** на машину 2

### 1.2 Работа с утилитой nc

Для тестирования работы утилиты nc выберем comp4 и comp2 (в нашей нотации) как

самые удаленные. Итак, проверим ее работу:

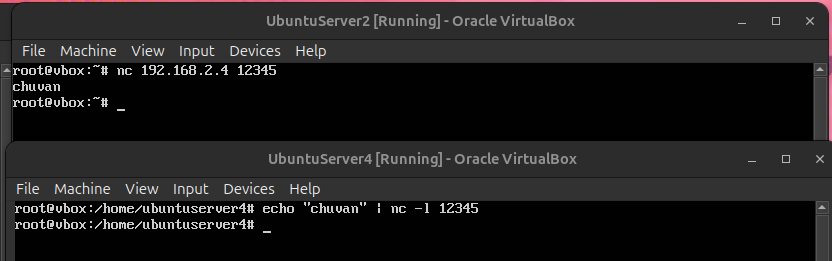


Рисунок 5 - Выполнили передачу сообщения с помощью утилиты nc

### 1.3 Настройка iptables

#### 1.3.1 Запрет передачи TCP на порт Netcat

Предполагаемый порт Netcat — 12345.

Команда на машине A или B:

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

#### 1.3.2 Запрет приема UDP с порта Netcat

Команда на машине A или B:

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

#### 1.3.3 Запрет передачи пакетов с IP машины A

Предположим, IP машины A — 192.168.1.2

Команда на машине B:

sudo iptables -A OUTPUT -s 192.168.1.2 -j DROP

#### 1.3.4 Запрет приема пакетов на IP машины B

Предположим, IP машины B — 192.168.2.4.

Команда на машине B:

sudo iptables -A INPUT -d 192.168.2.4 -j DROP

#### 1.3.5 Запрет ICMP-пакетов с размером >1000 байт и TTL <10

Команда на машине A или B:

sudo iptables -A INPUT -p icmp -m length --length 1001: -m ttl --ttl-lt 10 -j DROP

sudo iptables -A OUTPUT -p icmp -m length --length 1001: -m ttl --ttl-lt 10 -j DROP

### 1.4 Проверка работоспособности правил iptables

#### 1.4.1 Запрет передачи TCP на порт 12345

Машина 2 работает как сервер Netcat на порту 12345. Машина 4 пытается установить TCP-соединение с машиной 2, но iptables на машине 4 блокирует это соединение

На машине 2 (Server): Запустите Netcat для прослушивания на порту 12345:

nc -l 12345

На машине 4 (Client): Добавьте правило для блокировки TCP на порт 12345:

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

На машине 4 (Client): Попробуйте отправить сообщение на машину 2:

echo "hello" | nc 192.168.1.2 12345

Машина 2 не получит сообщение, так как TCP-пакет будет заблокирован

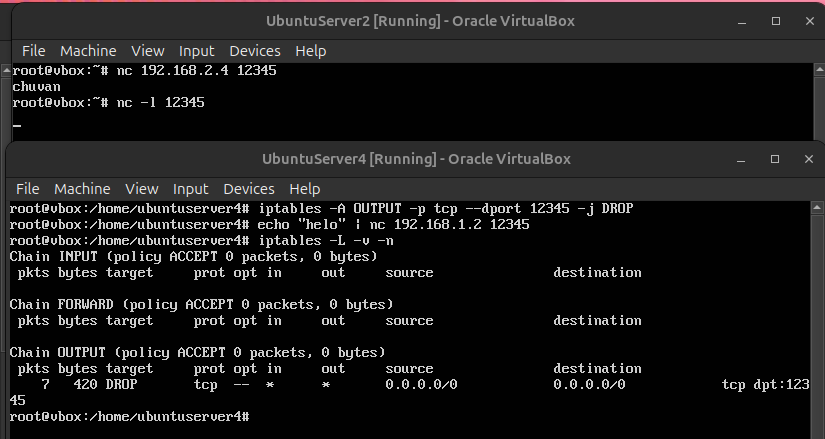


Рисунок 6 - Пример запрета передачи TCP на порт 12345

#### 1.4.2 Запрет приема UDP с порта 12345

Машина 4 работает как сервер Netcat и принимает данные UDP от машины 2, но iptables на машине 4 блокирует входящие UDP-пакеты с порта 12345.

На машине 4 (Server): Запустите Netcat для прослушивания UDP на порту 12345:

nc -u -l 12345

На машине 4 (Server): Добавьте правило для блокировки UDP-пакетов с порта 12345:

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

На машине 2 (Client): Отправьте сообщение UDP на машину 4:

echo "hi" | nc -u 192.168.2.4 12345

Машина 4 не получит сообщение от машины 2, так как UDP-пакет будет заблокирован.

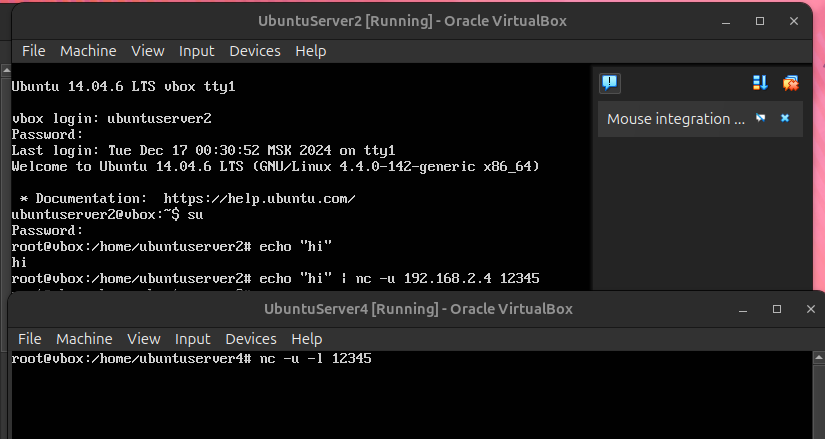


Рисунок 7 - Пример запрета передачи UDP на порт 12345

#### 1.4.3 Запрет передачи пакетов от IP машины A (192.168.1.2)

Машине **2 (192.168.1.2)** запрещается отправлять любые пакеты на машину **4**.

**На машине 4:** Добавьте правило для блокировки пакетов от машины 2:

sudo iptables -A INPUT -s 192.168.1.2 -j DROP

**На машине 2:** Отправьте пинг на машину 4:

ping 192.168.2.4

Машина 4 не ответит на пинг от машины 2.

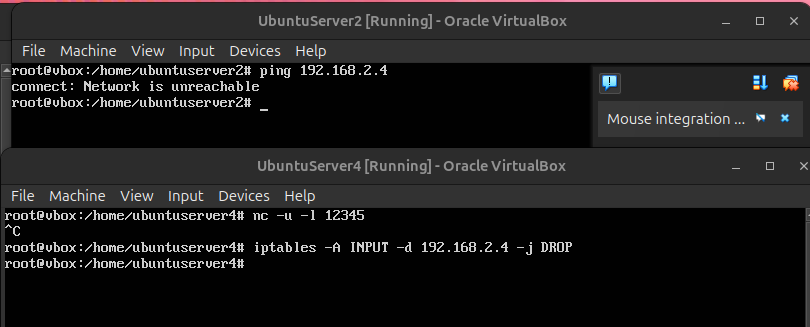


Рисунок 8 - Пример запрета передачи пакетов от IP машины A (192.168.1.2)

#### 1.4.4 Запрет приема пакетов на IP машины B (192.168.2.4)

Запрещаются все входящие пакеты на IP машины 4.

**На машине 4:** Добавьте правило:

sudo iptables -A INPUT -d 192.168.2.4 -j DROP

**На машине 2:** Отправьте пинг на машину 4:

ping 192.168.2.4

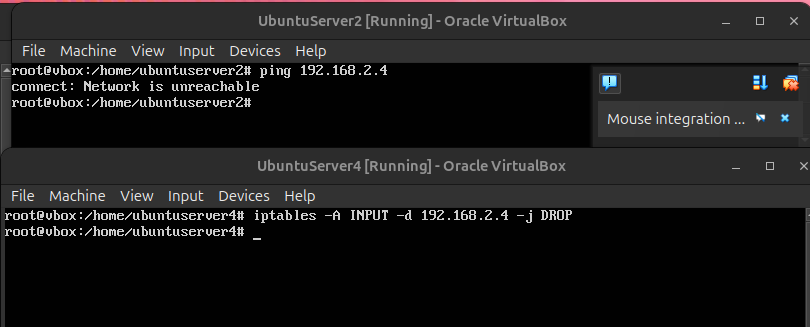


Рисунок 9 -Запрет приема пакетов на IP машины B (192.168.2.4)

#### 1.4.5 Запрет ICMP-пакетов больше 1000 байт и TTL меньше 10

Запрещаются ICMP-пакеты размером >1000 байт и TTL <10.

**На машине 4:** Добавьте правило:

sudo iptables -A INPUT -p icmp -m length --length 1001: -m ttl --ttl-lt 10 -j DROP

sudo iptables -A OUTPUT -p icmp -m length --length 1001: -m ttl --ttl-lt 10 -j DROP

**На машине 2:** Отправьте большой ICMP-пакет:

ping 192.168.2.4 -s 1200 -t 9

Машина 4 проигнорирует этот ICMP-пакет.

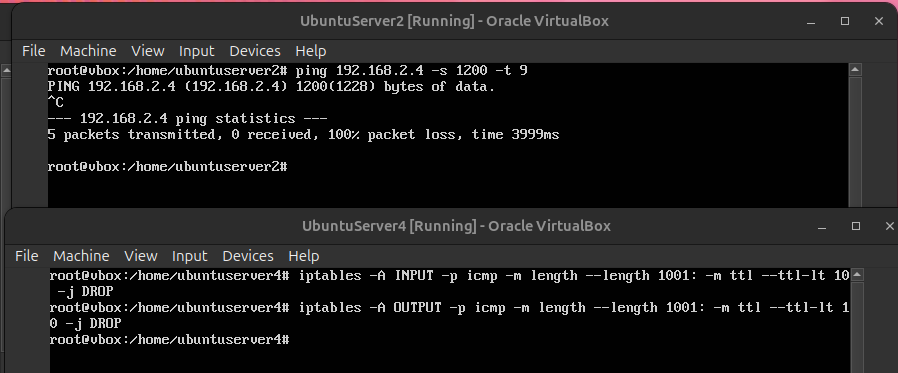


Рисунок 10 - Запрет ICMP-пакетов больше 1000 байт и TTL меньше 10

# 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.