**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:**

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

(подпись)

**Проверил:**

Есипов Дмитрий Андреевич

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

(отметка о выполнении)

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

(подпись)

**Содержание**

[1.1 Настройка IPv4 5](#_heading=h.7n6fsycnmhke)

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

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

[1.3.1 Запрет передачи TCP на порт Netcat 7](#_heading=h.iyea27a23sap)

[1.3.2 Запрет приёма UDP с порта Netcat 7](#_heading=h.ximn6cwe1z5m)

[1.3.3 Запрет передачи пакетов с IP машины A 7](#_heading=h.pi8hiunx12l9)

[1.3.4 Запрет приёма пакетов на IP машины Б 8](#_heading=h.47q4amh0j637)

[1.3.5 Запрет ICMP-пакетов с размером >1000 байт и TTL <10 8](#_heading=h.kmilhuojqal)

[1.4 Проверка работоспособности правил iptables 9](#_heading=h.s0ur16u1mnbt)

[1.4.1 Запрет передачи TCP на порт 12345 9](#_heading=h.n085cods0jl7)

[1.4.2 Запрет приема UDP с порта 12345 9](#_heading=h.y7vd27964ldf)

[1.4.3 Запрет передачи пакетов с IP-адреса компьютера A 10](#_heading=h.6dx5ydxo74p6)

[1.4.4 Запрет приёма пакетов на IP-адрес компьютера Б 10](#_heading=h.q8fzc7u6i4dk)

[1.4.5 Запрет ICMP-пакетов больше 1000 байт и TTL меньше 10 11](#_heading=h.tbtcakh6s5by)

**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.
5. **ХОД РАБОТЫ**

Выбор варианта:

Меня зовут Юдина Маргарита (14 букв)

V1 = 1 + (N mod 5) = 1 + (14 mod 5) = 5

V2 = 6 + (N mod 5) = 6 + (14 mod 5) = 10

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

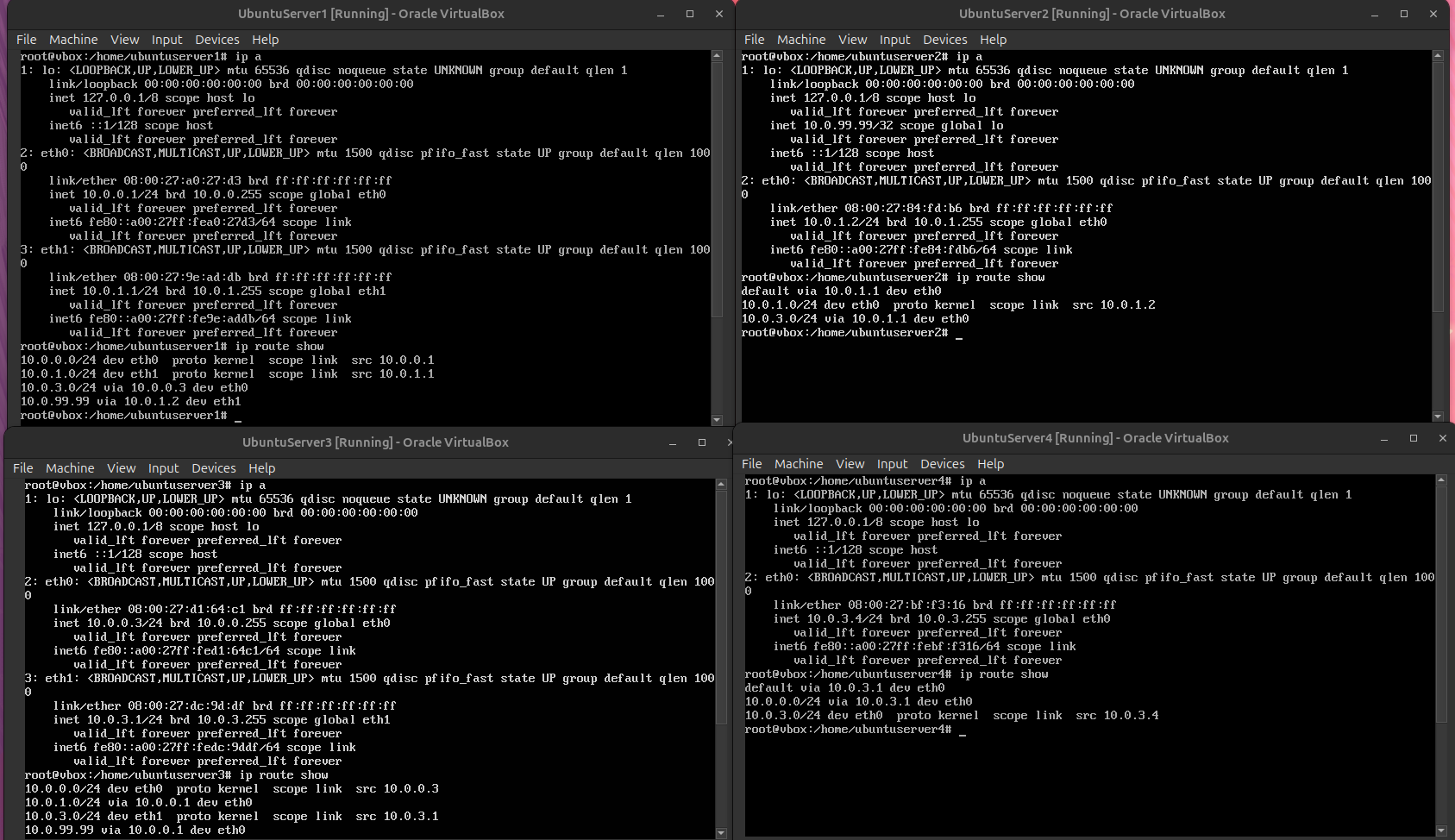


Рисунок 2 – Результат выполнения команды «ip a» и «ip route show» на всех машинах

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

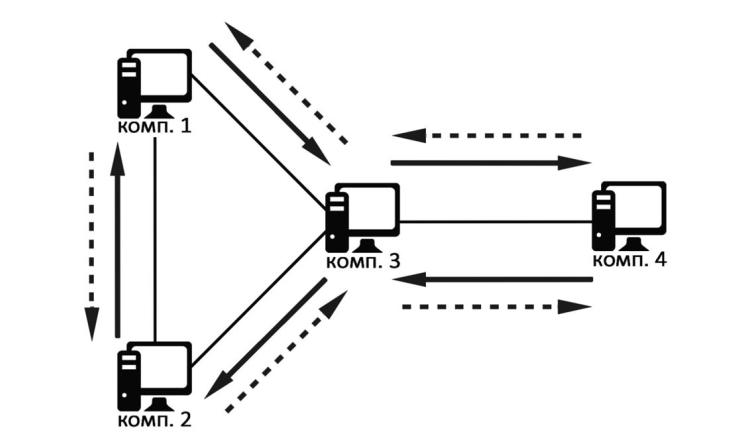


Рисунок 3 – Полученная топология

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

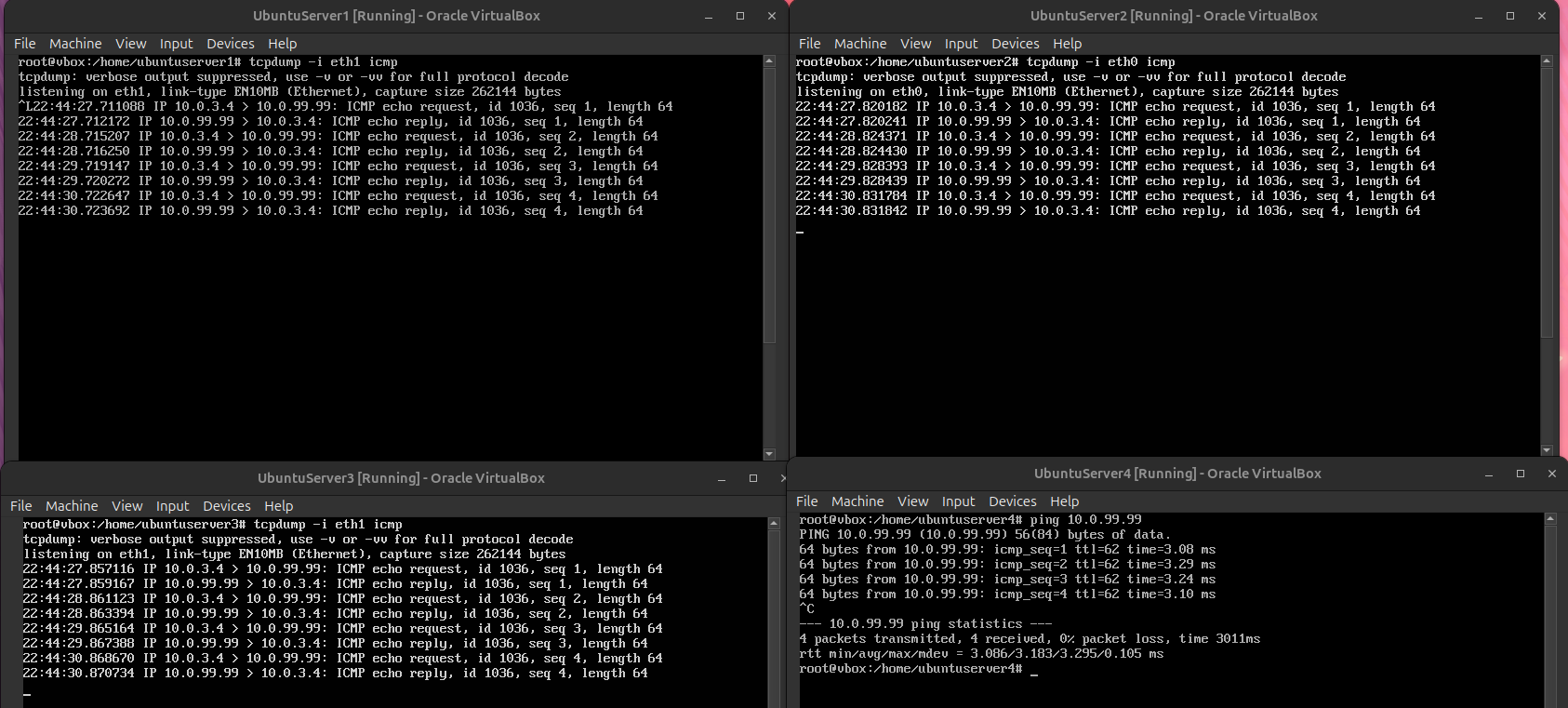


Рисунок 4 – С машины 4 выполните команду **ping** 10.0.99.99

**1.2 Работа с утилитой nc**

Для тестирования работы утилиты nc выберем comp3 и comp1 (в нашей нотации) как

самые удаленные. Итак, проверим ее работу:

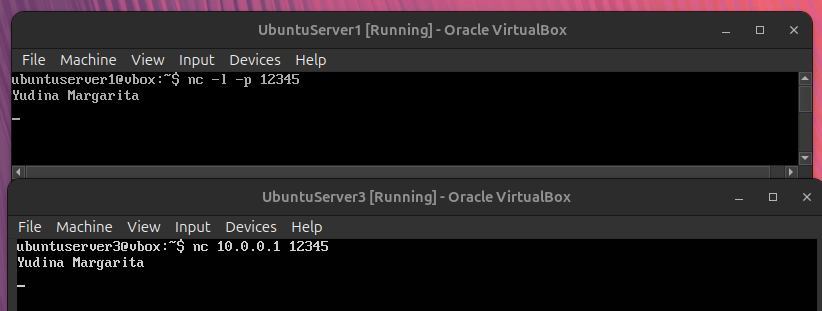


Рисунок 5 - Выполнили передачу сообщения с помощью утилиты nc

**1.3 Настройка iptables**

**1.3.1 Запрет передачи TCP на порт Netcat**

**Требование**: Заблокировать TCP-пакеты, отправляемые на порт **12345**.

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

Запустите Netcat сервер на Компьютере Б (порт 12345): nc -l -p 12345

Подключитесь с Компьютера A (Netcat клиент):

nc <IP\_КОМПЬЮТЕРА\_Б> 12345

Результат: Соединение будет отклонено.

**1.3.2 Запрет приёма UDP с порта Netcat**

**Требование**: Заблокировать UDP-пакеты, получаемые с порта **12345**.

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

Запустите Netcat UDP сервер на Компьютере A (порт 12345):

nc -u -l -p 12345

С Компьютера Б отправьте сообщение через UDP:

echo "Test message" | nc -u <IP\_КОМПЬЮТЕРА\_A> 12345

**Результат**: Компьютер A не получит сообщение.

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

**Требование**: Заблокировать **OUTPUT** пакеты с IP-адреса Компьютера A (например, 10.0.1.2).

sudo iptables -A OUTPUT -s 10.0.1.2 -j DROP

С Компьютера A выполните ping Компьютера Б:

ping <IP\_КОМПЬЮТЕРА\_Б>

**Результат**: Пакеты будут заблокированы на Компьютере A.

**1.3.4 Запрет приёма пакетов на IP машины Б**

**Требование**: Заблокировать **INPUT** пакеты, отправляемые на IP-адрес Компьютера Б (например, 10.0.3.4).

sudo iptables -A INPUT -d 10.0.3.4 -j DROP

С Компьютера A выполните ping Компьютера Б:

ping <IP\_КОМПЬЮТЕРА\_Б>

**Результат**: Пакеты будут заблокированы на Компьютере Б.

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

Требование: Заблокировать ICMP-пакеты, если:

* Размер больше 1000 байт.
* TTL меньше 10.

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

Отправьте большой ICMP-пакет с Компьютера A на Компьютер Б:

ping <IP\_КОМПЬЮТЕРА\_Б> -s 1024 -t 9

**Результат**: Пакет будет заблокирован iptables.

**1.4 Проверка работоспособности правил iptables**

**1.4.1 Запрет передачи TCP на порт 12345**

Блокировка **OUTPUT** TCP-пакетов, отправляемых на порт **12345**.

Настройка на Компьютере A или Компьютере Б:

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

Запустите Netcat **сервер** на Компьютере Б: nc -l -p 12345

Подключитесь с Компьютера A: nc <IP\_КОМПЬЮТЕРА\_Б> 12345

**Результат**: Соединение не будет установлено, так как TCP-пакеты заблокированы.

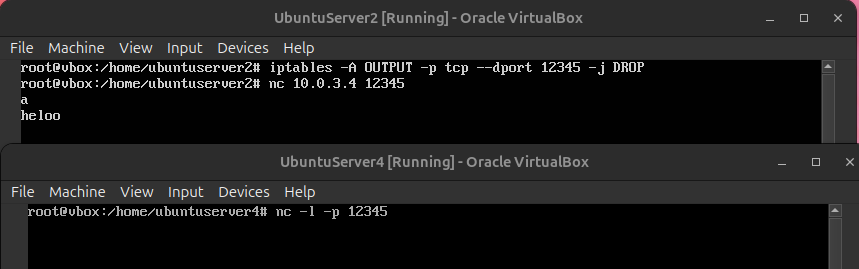


Рисунок 6 - Пример запрета передачи TCP на порт 12345

**1.4.2 Запрет приема UDP с порта 12345**

Блокировка **INPUT** UDP-пакетов, исходящих с порта **12345**.

Настройка на Компьютере A или Компьютере Б:

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

Запустите Netcat **UDP-сервер** на Компьютере A: nc -u -l -p 12345

С Компьютера Б отправьте UDP-сообщение:

echo "Hello" | nc -u <IP\_КОМПЬЮТЕРА\_A> 12345

**Результат**: Компьютер A не получит сообщение.

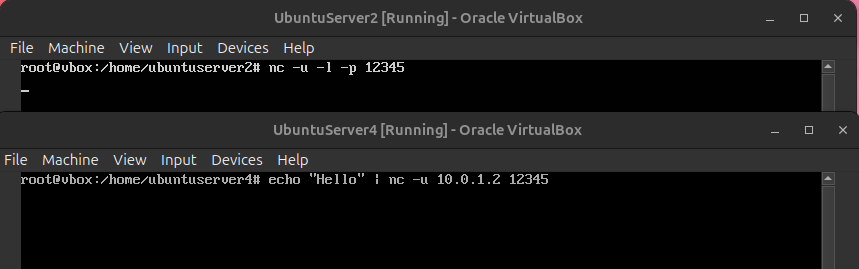


Рисунок 7 - Пример запрета передачи UDP на порт 12345

**1.4.3 Запрет передачи пакетов с IP-адреса компьютера A**

Блокировка OUTPUT всех пакетов с IP-адреса Компьютера A (например: 10.0.1.2).

Настройка на Компьютере Б:

sudo iptables -A OUTPUT -s 10.0.1.2 -j DROP

С Компьютера A выполните ping Компьютера Б:

ping <IP\_КОМПЬЮТЕРА\_Б>

**Результат**: Компьютер Б не получит пакеты от Компьютера A.

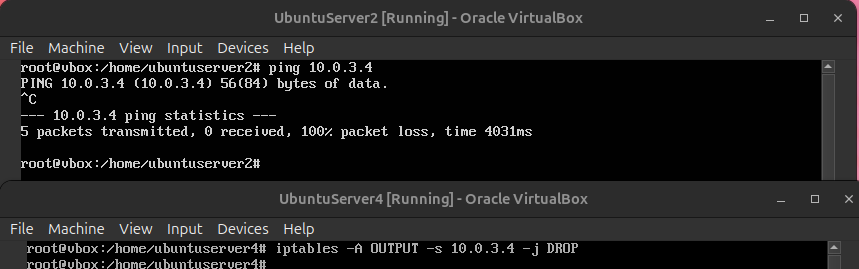


Рисунок 8 - Пример запрета передачи пакетов от IP машины A

**1.4.4 Запрет приёма пакетов на IP-адрес компьютера Б**

Блокировка **INPUT** всех пакетов, отправленных на IP-адрес Компьютера Б (например: 10.0.3.4).

Настройка на Компьютере Б:

sudo iptables -A INPUT -d 10.0.3.4 -j DROP

С Компьютера A отправьте сообщение Netcat на Компьютер Б:

echo "Test" | nc <IP\_КОМПЬЮТЕРА\_Б> 12345

**Результат**: Компьютер Б не получит пакеты.

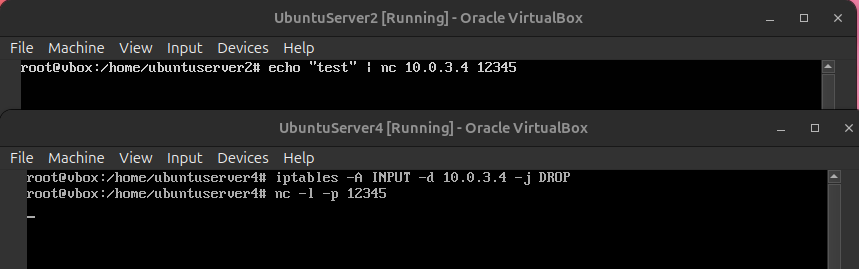


Рисунок 9 -Запрет приема пакетов на IP машины B

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

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

**На машине 1:** 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 10.0.0.1 -s 1200 -t 9

Машина 4 проигнорирует этот ICMP-пакет.

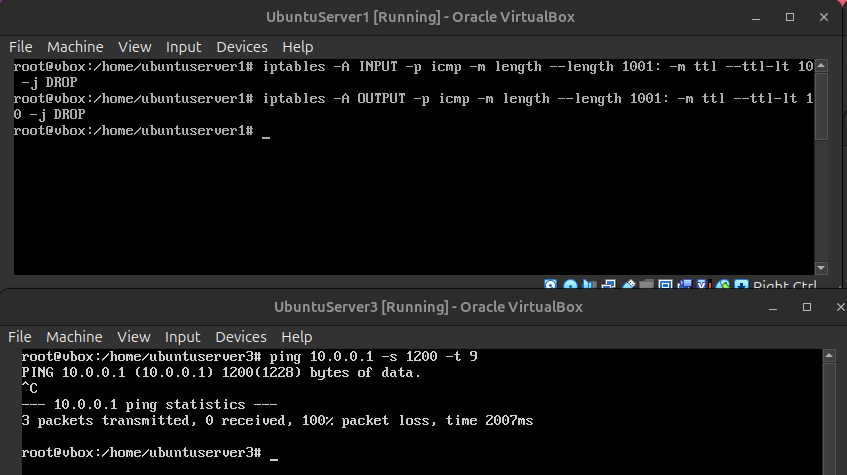


Рисунок 10 - Запрет ICMP-пакетов больше 1000 байт и TTL меньше 10

**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.