МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ

по лабораторной работе №5

по дисциплине «Сети и телекоммуникации»

Тема: Изучение механизмов трансляции сетевых адресов: NAT, MASQUERADE

Студент гр. 3384 _____ Рудаков А.Л.

Преподаватель _____ Фирсов М.А.

Санкт-Петербург

2025

Цель работы.

Целью работы является изучение механизмов преобразования сетевых адресов: NAT, Masquerade. Подробно рассмотрены некоторые сетевые возможности VirtualBox, который будет использован для создания необходимой инфраструктуры. Необходимо решить следующие задачи:

1. Создать три виртуальные машины (лаб. работа № 1).

2. Настроить имена, IP-адреса для каждой из подсетей в соответствии со схемой.

3. Настроить переадресацию пакетов между сетевыми интерфейсами для машины с NAT. Запретить прямой доступ между двумя частными подсетями (необходимо для воссоздания условий, приближенных к реальным).

4. Настроить Masquerade на NAT-машине и проверить доступ к сети Интернет с других машин и отсутствие доступа друг к другу.

5. Настроить доступ к сети Интернет для одной из машин с помощью sNAT.

6. Добавить вторичный IP-адрес на NAT-машину, по которому в дальнейшем будет отвечать на внешние запросы машина, указанная в п. 5.

7. Настроить dNAT для доступа к машине из внешней сети. Проверить настройки.

Задание.

Вариант 22

1. Создать и настроить инфраструктуру для выполнения лабораторной работы. Развернуть три виртуальные машины (лаб. работа № 1). Настроить их в соответствии с подразделом «Построение инфраструктуры для выполнения работы».

2. Настройка доступа с ub1, ub2 в сеть Интернет с использованием Masquerade. Настройте ub-nat, используя Masqurade, так, чтобы машины ub1 и ub2 имели доступ в сеть Интернет.

3. Настройка доступа с ub1, ub2 в сеть Интернет с использованием sNAT. Настройте ub-nat, используя sNAT, так, чтобы машины ub1 и ub2 имели доступ в сеть Интернет.

4. Настройка доступа с ub2 на ub1 с использованием dNAT. Настройте ub-nat, используя dNAT, так, чтобы с машины ub2 можно было получить доступ к ub1, используя IP-адрес из NAT-сети. Проверить успешность настроек можно, выполнив с узла ub2 команду: `ssh «SecondaryNatIPaddress».`

В результате подключения будет отображено имя виртуальной машины ub1.

Пример:

```
root@ub2:/home/user# ssh user@10.0.2.100
user@10.0.2.100'spassword:
user@ub1:~$
```

В данном примере вторичный IP-адрес на ub-nat настроен на интерфейсе, подключенном к NAT-сети, – IP-адрес: 10.0.2.100. При правильной настройке ssh доступ к этому IP-адресу будет открывать сессию с ub1.

Выполнение работы.

1. Развернуты три виртуальные машины с именами ub1, ub2, ub3 в соответствии со схемой на рис.1.

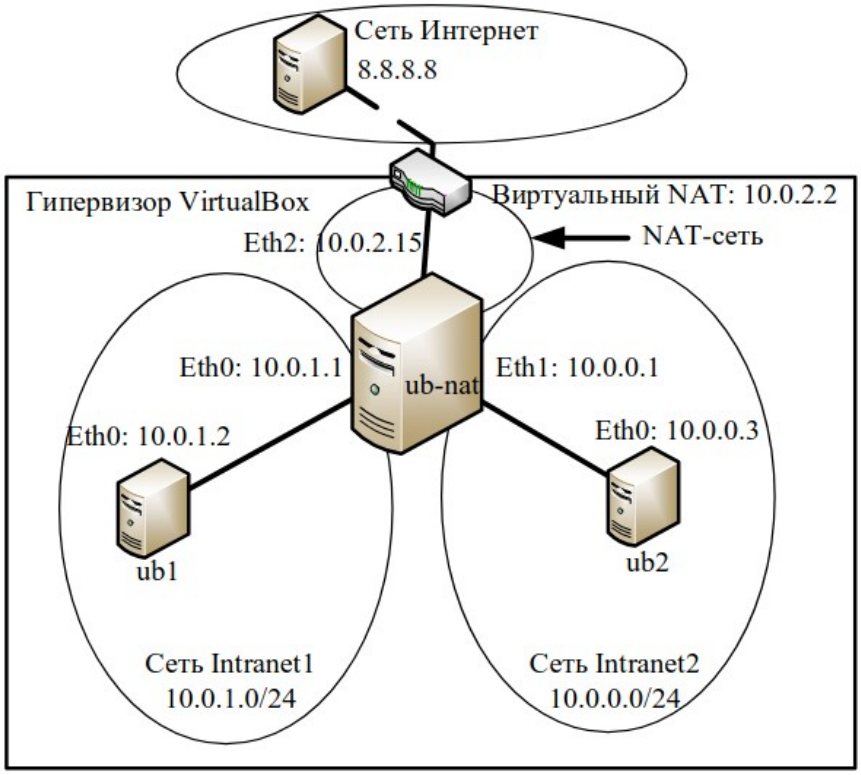

Рисунок 1 - схема сети

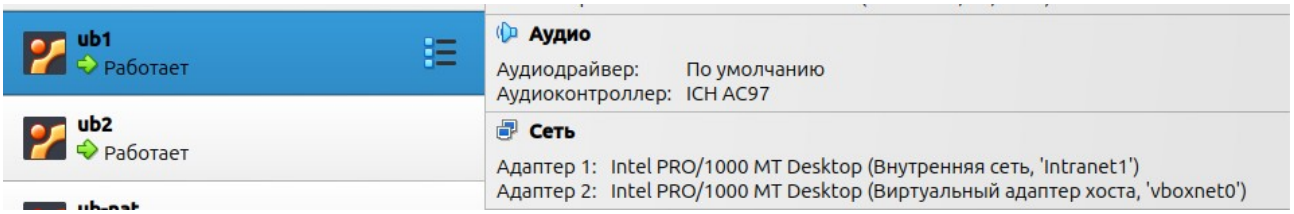

Рисунок 2 - настройка сети для ub1

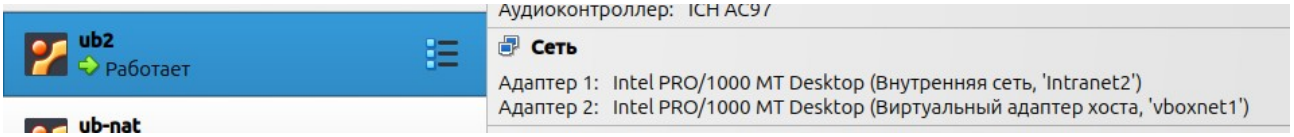

Рисунок 3 - настройка сети для ub2

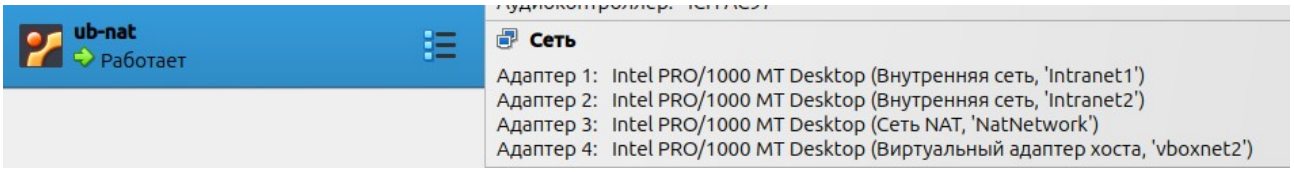

Рисунок 4 - настройка сети для ub-nat

Виртуальные машины были настроены в соответствии с табл. 1:

Таблица 1 – настройка сети

Узел	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
ub1	eth0(enp0s3)	10.0.94.22	255.255.255.0	10.0.94.1

ub2	eth0(enp0s3)	10.0.95.22	255.255.255.0	10.0.95.1
ub-nat	eth0(enp0s3)	10.0.94.1	255.255.255.0	10.0.2.2
ub-nat	eth1(enp0s8)	10.0.95.1	255.255.255.0	
ub-nat	eth2(enp0s9)	10.0.2.15	255.255.255.0	

Кроме этого был запрещен доступ с ub2 на ub1 при помощи команды:

sudo iptables -A OUTPUT -d 10.0.94.0/24 -j DROP

Были выполнены ping-запросы для проверки настройки сети. Ping-запросы завершились ожидаемо, в соответствии с условиями построения сети, следовательно сеть настроена корректно. Доступ к интернету есть только у ub-nat, у ub1 и ub2 доступа нет.

Ping - запрос с ub1 (10.0.94.22) на ub-nat (10.0.94.1) показан на рис.5.

```
ub1@first:~$ ping -c1 10.0.94.1
PING 10.0.94.1 (10.0.94.1) 56(84) bytes of data.
64 bytes from 10.0.94.1: icmp_seq=1 ttl=64 time=0.807 ms

--- 10.0.94.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.807/0.807/0.807/0.000 ms
```

Рисунок 5 - ping-запрос с ub1 на ub-nat

Ping - запрос с ub1 (10.0.94.22) в интернет (8.8.8.8) показан на рис.6.

```
ub1@first:~$ ping -c1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Рисунок 6 - ping-запрос с ub1 на 8.8.8.8

Ping - запрос с ub2 (10.0.95.22) на ub-nat (10.0.95.1) показан на рис.7.

```
ub2@first:~$ ping -c1 10.0.95.1
PING 10.0.95.1 (10.0.95.1) 56(84) bytes of data.
64 bytes from 10.0.95.1: icmp_seq=1 ttl=64 time=0.925 ms

--- 10.0.95.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.925/0.925/0.925/0.000 ms
```

Рисунок 7 - ping-запрос с ub2 на ub-nat

Ping - запрос с ub2 (10.0.95.22) в интернет (8.8.8.8) показан на рис.8.

```
ub2@first:~$ ping -c1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Рисунок 8 - ping-запрос с ub2 на 8.8.8.8

Ping - запрос с ub-nat (10.0.94.1) на ub1 (10.0.94.22) показан на рис.9.

```
ub-nat@first:~$ ping -c1 10.0.94.1
PING 10.0.94.1 (10.0.94.1) 56(84) bytes of data.
64 bytes from 10.0.94.1: icmp_seq=1 ttl=64 time=0.009 ms

--- 10.0.94.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.009/0.009/0.009/0.000 ms
```

Рисунок 9 - ping-запрос с ub-nat на ub1

Ping - запрос с ub-nat (10.0.95.1) на ub2 (10.0.95.22) показан на рис.10.

```
ub-nat@first:~$ ping -c1 10.0.95.1
PING 10.0.95.1 (10.0.95.1) 56(84) bytes of data.
64 bytes from 10.0.95.1: icmp_seq=1 ttl=64 time=0.027 ms

--- 10.0.95.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.027/0.027/0.027/0.000 ms
```

Рисунок 10 - ping-запрос с ub-nat на ub2

Ping - запрос с ub-nat (10.0.2.15) в интернет (8.8.8.8) показан на рис.11.

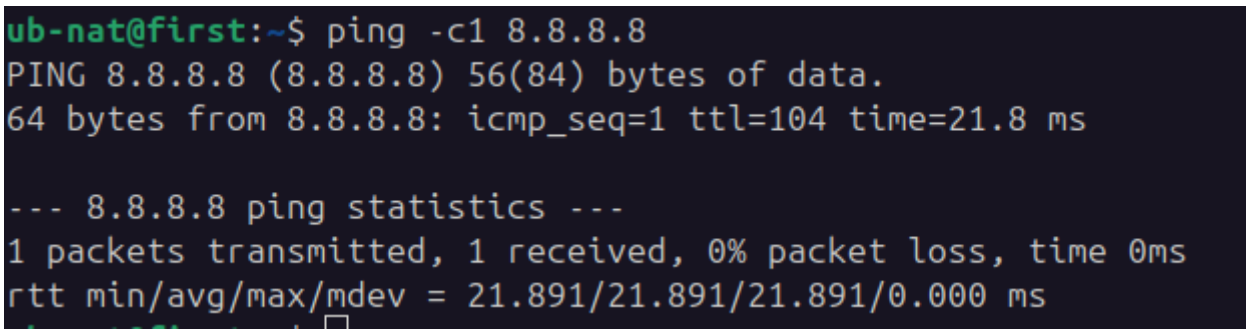

Рисунок 11 - ping-запрос с ub-nat на 8.8.8.8

Ping - запрос с ub1(10.0.94.22) на ub2 (10.0.95.22) показан на рис.12.

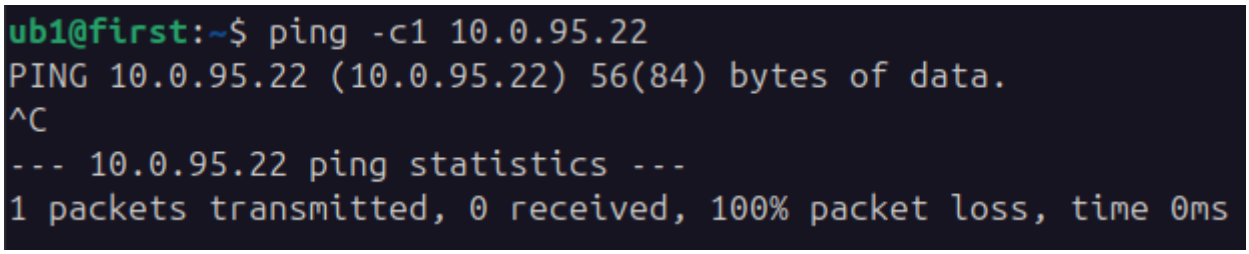

Рисунок 12 - ping-запрос с ub1 на ub2

Ping - запрос с ub2 (10.0.95.22) на ub1 (10.0.94.22) показан на рис.13.

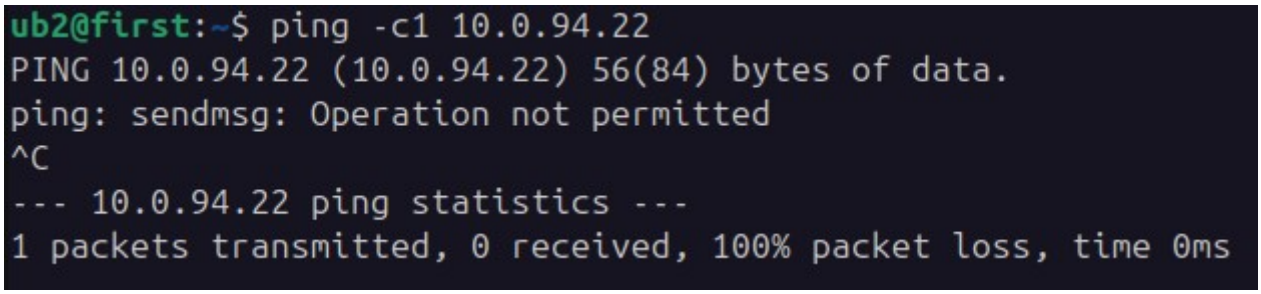

Рисунок 13 - ping-запрос с ub2 на ub1

2. Был настроен доступ в сеть интернет с ub1, ub2 с использованием Masquerade.

На ub-nat была настроена таблица маршрутизации:

Для доступа узлов из локальных сетей в интернет и обратно был разрешен проход через порты ub-nat:

```
ub-nat@first:~$ sudo iptables -A FORWARD -i enp0s3 -o enp0s9 -j ACCEPT
ub-nat@first:~$ sudo iptables -A FORWARD -i enp0s8 -o enp0s9 -j ACCEPT
ub-nat@first:~$ sudo iptables -A FORWARD -i enp0s9 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Кроме этого была включена пересылка пакетов на ub-nat.

```
ub-nat@first:~$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

Также был настроен MASQUERADE во внешний NAT-интерфейс.

```
ub-nat@first:~$ sudo iptables -t nat -A POSTROUTING -s 10.0.94.0/24 -o enp0s9 -j MASQUERADE
ub-nat@first:~$ sudo iptables -t nat -A POSTROUTING -s 10.0.95.0/24 -o enp0s9 -j MASQUERADE
```

Результат настройки сети показан на рис.14.

```
ub-nat@first:~$ sudo iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  10.0.95.0/24         anywhere
MASQUERADE  all  --  10.0.94.0/24         anywhere
```

Рисунок 14 - результат настройки сети

Были выполнены ping-запросы с ub1, ub2 в сеть интернет для проверки настройки. Ping-запросы прошли успешно, следовательно настройки верны.

Ping - запрос с ub1 (10.0.94.22) в интернет (8.8.8.8) показан на рис.15.

```
ub1@first:~$ ping -c1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=103 time=23.9 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 23.924/23.924/23.924/0.000 ms
```

Рисунок 15 - ping-запрос с ub1 на 8.8.8.8

Ping - запрос с ub2 (10.0.95.22) в интернет (8.8.8.8) показан на рис.16.

```
ub2@first:~$ ping -c1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=103 time=22.9 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 22.909/22.909/22.909/0.000 ms
```

Рисунок 16 - ping-запрос с ub2 на 8.8.8.8

Доступа от ub1 к ub2 и наоборот до сих пор нет, что видно на рис.17.

```
ub1@first:~$ ping -c1 10.0.95.22
PING 10.0.95.22 (10.0.95.22) 56(84) bytes of data.
^C
--- 10.0.95.22 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Рисунок 17 - ping-запрос с ub1 на ub2

3. Был настроен доступ в интернет для ub1, ub2 при помощи sNAT.

Сначала была очищена таблица маршрутизации:

ub-nat@first:~$ sudo iptables -F

ub-nat@first:~$ sudo iptables -t nat -F

Далее был разрешен форвардинг из внутренних сетей наружу и обратно:

ub-nat@first:~$ sudo iptables -A FORWARD -i enp0s3 -o enp0s9 -j ACCEPT

ub-nat@first:~$ sudo iptables -A FORWARD -i enp0s8 -o enp0s9 -j ACCEPT

ub-nat@first:~$ sudo iptables -A FORWARD -i enp0s9 -m state --state ESTABLISHED,RELATED -j ACCEPT

Был настроен sNAT:

ub-nat@first:~$ sudo iptables -t nat -A POSTROUTING -s 10.0.94.0/24 -o enp0s9 -j SNAT --to-source 10.0.2.15

ub-nat@first:~$ sudo iptables -t nat -A POSTROUTING -s 10.0.95.0/25 -o enp0s9 -j SNAT --to-source 10.0.2.15

Результат настройки сети показан на рис.18.

```
ub-nat@first:~$ sudo iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       all  --  10.0.94.0/24         anywhere             to:10.0.2.15
SNAT       all  --  10.0.95.0/25         anywhere             to:10.0.2.15
```

Рисунок 18 - результат настройки сети

Были выполнены ping-запросы с ub1, ub2 в сеть интернет для проверки настройки. Ping-запросы прошли успешно, следовательно всё настроено верно.

Ping - запрос с ub1 (10.0.94.22) в интернет (8.8.8.8) показан на рис.19.

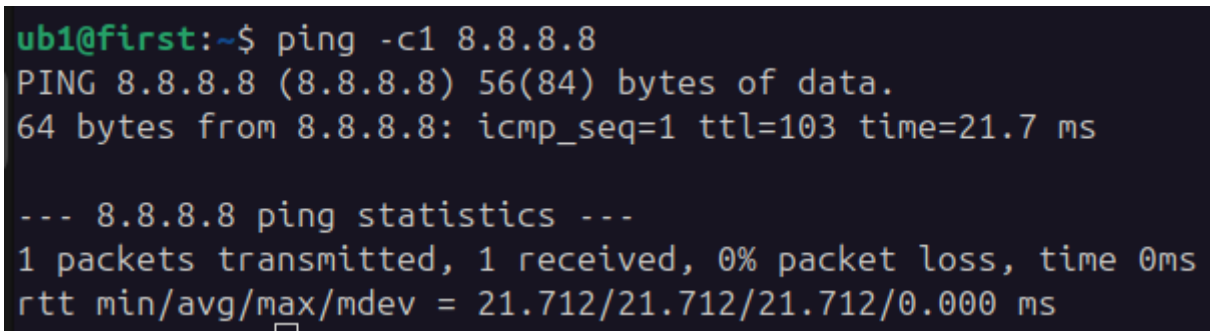

Рисунок 19 - ping-запрос с ub1 на 8.8.8.8

Ping - запрос с ub2 (10.0.95.22) в интернет (8.8.8.8) показан на рис.20.

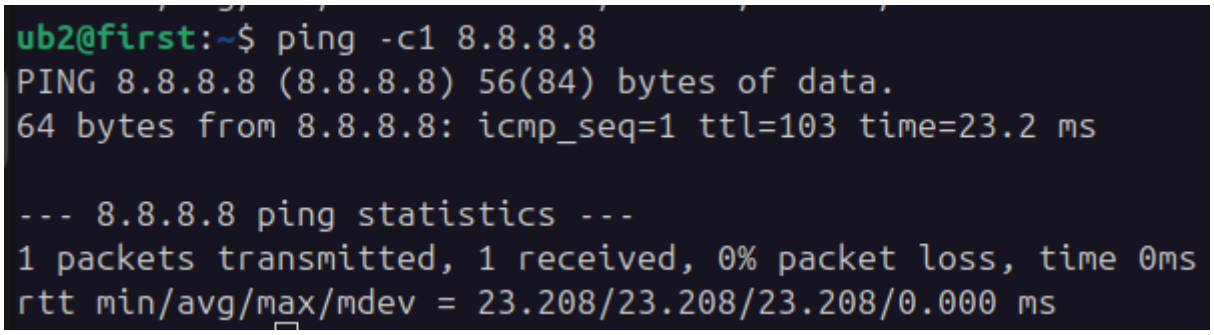

Рисунок 20 - ping-запрос с ub2 на 8.8.8.8

Доступа от ub1 к ub2 и наоборот до сих пор нет, что видно на рис.21.

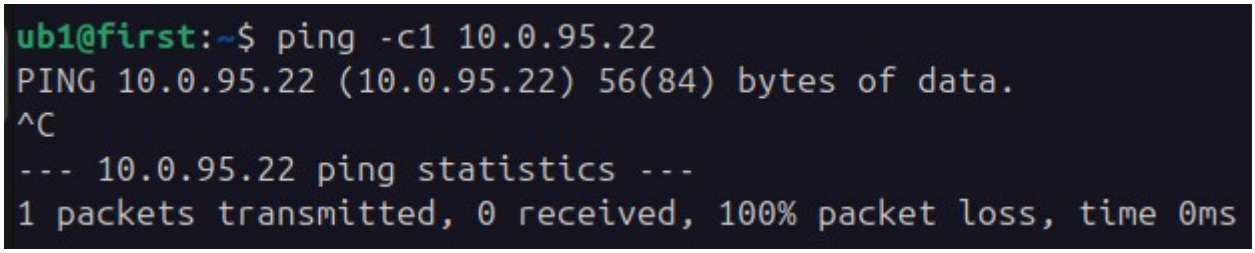

Рисунок 21 - ping-запрос с ub1 на ub2

4. Был настроен доступ с ub2 на ub1 при помощи dNAT.

Был добавлен второй NAT IP-адрес:

udo ip addr add 10.0.2.100/24 dev enp0s9

Был добавлен dNAT и разрешен форвардинг из внутренней сети наружу и обратно:

sudo iptables -t nat -A PREROUTING -d 10.0.2.100 -p tcp --dport 22 -j DNAT --to-destination 10.0.94.22:22

sudo iptables -A FORWARD -d 10.0.94.22 -p tcp --dport 22 -j ACCEPT

sudo iptables -A FORWARD -s 10.0.94.22 -m state --state ESTABLISHED,RELATED -j ACCEPT

Результат настройки сети показан на рис.22.

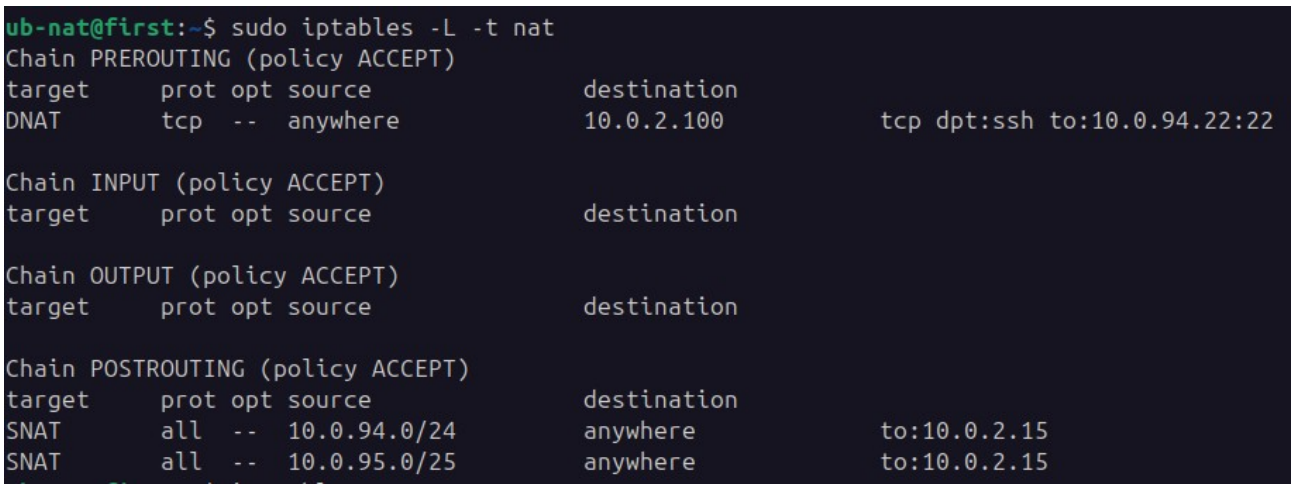

Рисунок 22 - результат настройки сети

Был получен доступ с ub2 на ub1 по ssh при помощи dNAT. Результат показан на рис.23.

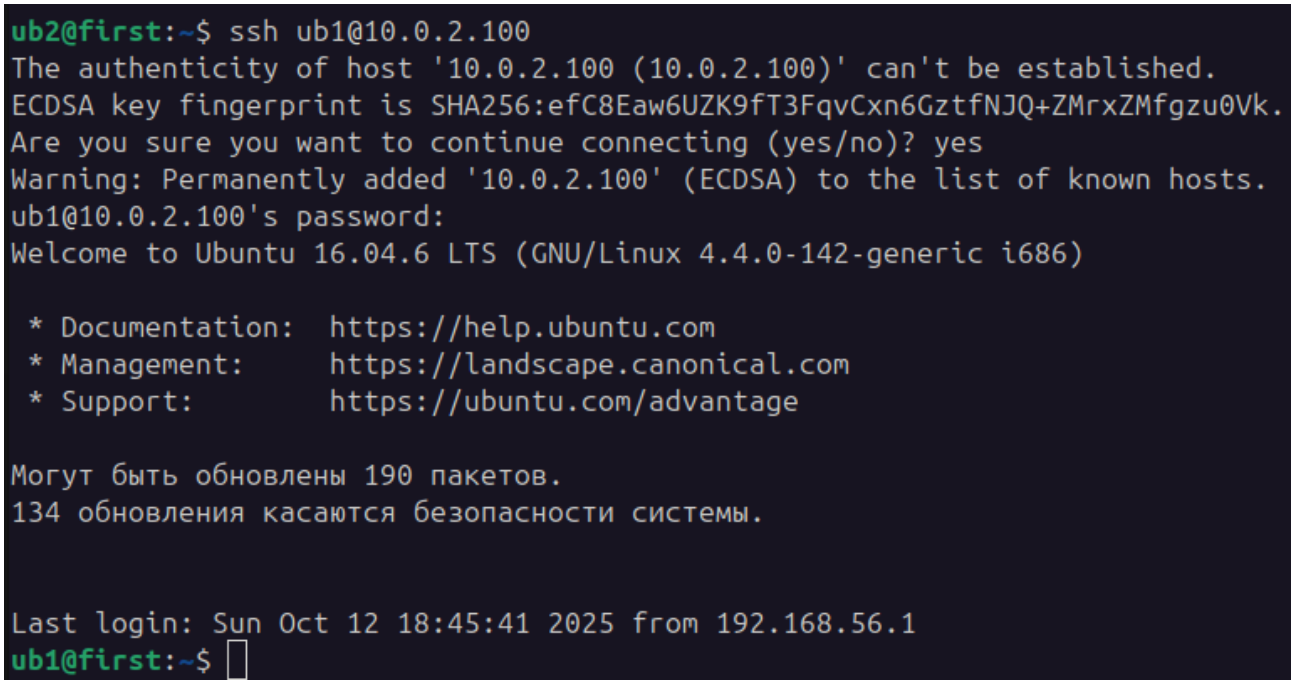

Рисунок 23 - подключение по shh с ub2 на ub1

Вывод.

Была проделана работа по настройке сети, были применены разные способы для настройки доступа из локальной в интернет, при помощи: NAT, sNAT, MASQUERADE, а также dNAT для доступа между двумя виртуальными машинами.