

**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**

Студентка гр. 1304

Чернякова В.А.

Преподаватель

Ефремов М.А.

Санкт-Петербург

2023

### **Цель работы.**

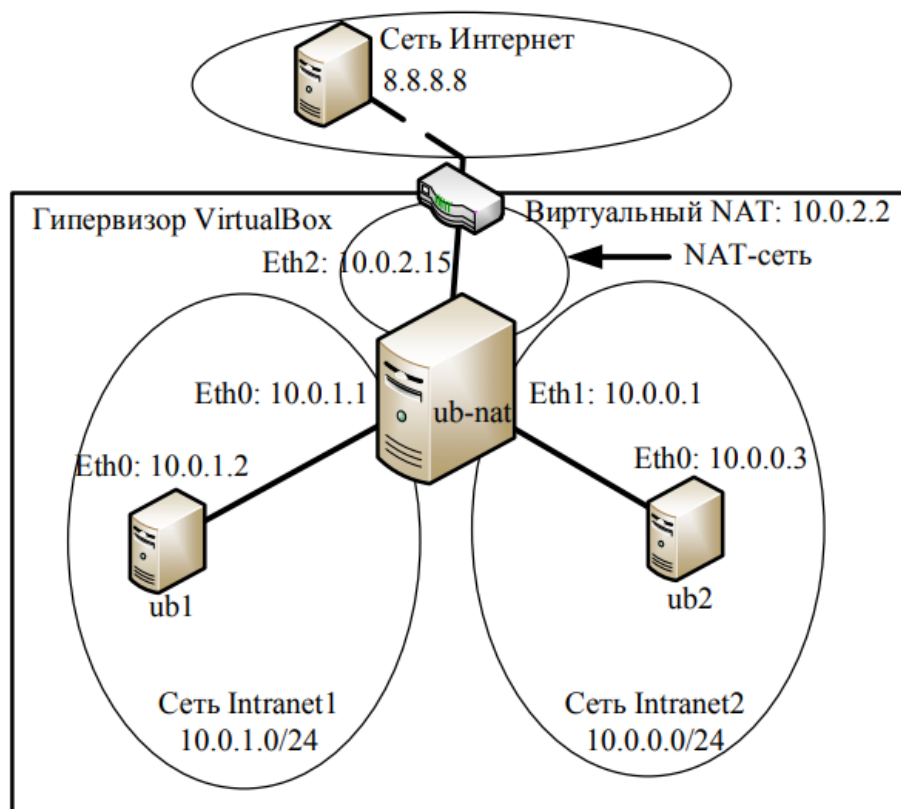
Целью работы является изучение механизмов преобразования сетевых адресов: NAT, Masquerade. Подробно рассмотрены некоторые сетевые возможности VirtualBox, который будет использован для создания необходимой инфраструктуры.

### **Задание.**

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.

### **Выполнение работы.**

1. Развернем три виртуальные машины. Настроим их в соответствии с подразделом «Построение инфраструктуры для выполнения работы».



Настройка ub1, ub2, ub-nat.

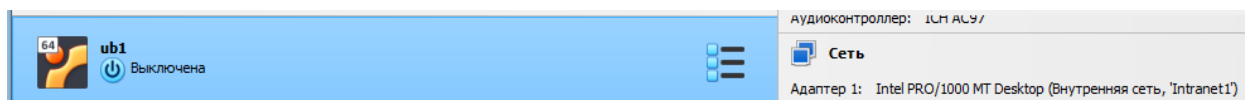


Рисунок 1 – настройка сети для ub1.

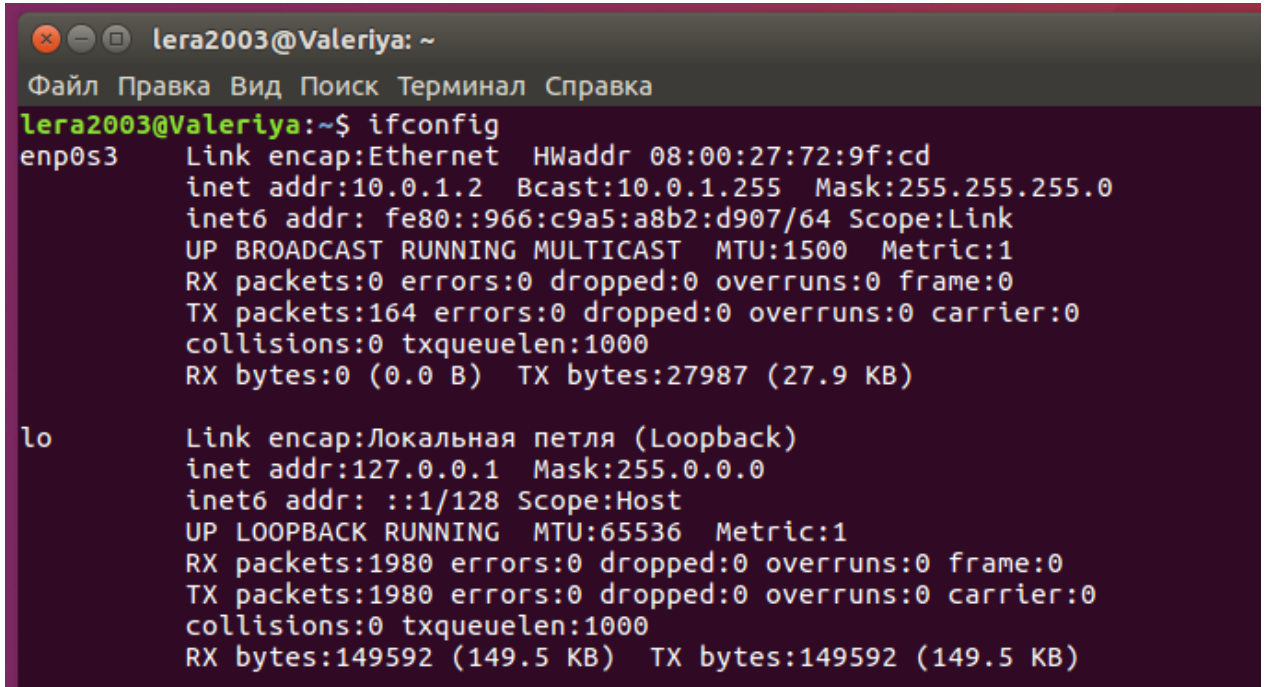


Рисунок 2 – настройка сети для ub2.



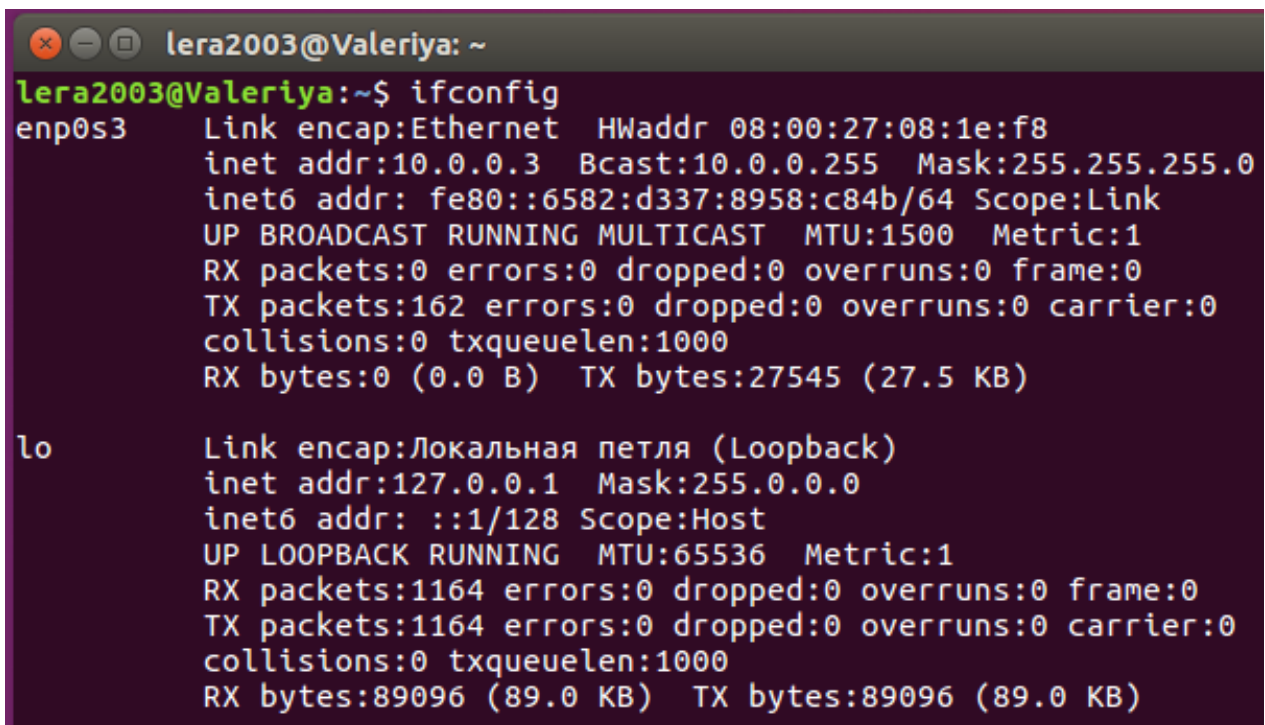
Рисунок 3 – настройка сети для ub-nat.

## Настройка конфигурации сетевых интерфейсов на машинах:



```
lera2003@Valeriya: ~  
Файл Правка Вид Поиск Терминал Справка  
lera2003@Valeriya:~$ ifconfig  
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:72:9f:cd  
            inet addr:10.0.1.2  Bcast:10.0.1.255  Mask:255.255.255.0  
            inet6 addr: fe80::966:c9a5:a8b2:d907/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:164 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:0 (0.0 B)  TX bytes:27987 (27.9 KB)  
  
lo          Link encap:Локальная петля (Loopback)  
            inet addr:127.0.0.1  Mask:255.0.0.0  
            inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING  MTU:65536  Metric:1  
            RX packets:1980 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:1980 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:149592 (149.5 KB)  TX bytes:149592 (149.5 KB)
```

Рисунок 4 – ub1.



```
lera2003@Valeriya: ~  
lera2003@Valeriya:~$ ifconfig  
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:08:1e:f8  
            inet addr:10.0.0.3  Bcast:10.0.0.255  Mask:255.255.255.0  
            inet6 addr: fe80::6582:d337:8958:c84b/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:162 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:0 (0.0 B)  TX bytes:27545 (27.5 KB)  
  
lo          Link encap:Локальная петля (Loopback)  
            inet addr:127.0.0.1  Mask:255.0.0.0  
            inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING  MTU:65536  Metric:1  
            RX packets:1164 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:1164 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:89096 (89.0 KB)  TX bytes:89096 (89.0 KB)
```

Рисунок 5 – ub2.

```
lera2003@Valeriya:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:ab:b8:eb
            inet addr:10.0.1.1  Bcast:10.0.1.255  Mask:255.255.255.0
            inet6 addr: fe80::70b0:b95f:7920:d4b9/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:168 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:0 (0.0 B)  TX bytes:27825 (27.8 KB)

enp0s8      Link encap:Ethernet  HWaddr 08:00:27:7b:09:79
            inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
            inet6 addr: fe80::c0cb:6eb0:3f7f:2abc/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:169 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:0 (0.0 B)  TX bytes:27655 (27.6 KB)

enp0s9      Link encap:Ethernet  HWaddr 08:00:27:99:95:e2
            inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::dc6a:1359:86aa:c912/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:2854 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1211 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:3885792 (3.8 MB)  TX bytes:116792 (116.7 KB)

lo          Link encap:Локальная петля (Loopback)
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:440 errors:0 dropped:0 overruns:0 frame:0
            TX packets:440 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:36510 (36.5 KB)  TX bytes:36510 (36.5 KB)
```

Рисунок 6 – ub-nat.

В качестве маршрутизатора будет выступать виртуальная машина «ub-nat», которая будет иметь выход в сеть Интернет посредством NAT-сети, а также подключена к двум внутренним сетям Intranet1 и Intranet2. Для обеспечения возможности переадресации трафика между интерфейсами внутри «ub-nat» включим данную опцию в sysctl. Для этого в файле /etc/sysctl.conf зададим следующую переменную:

```
net.ipv4.ip_forward = 1
```

В начале проверим доступность с ub1 до ub2 с помощью команды ping:

```
lera2003@Valeriya:~$ ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
From 10.0.1.2 icmp_seq=1 Destination Host Unreachable
From 10.0.1.2 icmp_seq=2 Destination Host Unreachable
From 10.0.1.2 icmp_seq=5 Destination Host Unreachable
From 10.0.1.2 icmp_seq=6 Destination Host Unreachable
From 10.0.1.2 icmp_seq=7 Destination Host Unreachable
From 10.0.1.2 icmp_seq=8 Destination Host Unreachable
From 10.0.1.2 icmp_seq=9 Destination Host Unreachable
^C
--- 10.0.0.3 ping statistics ---
11 packets transmitted, 0 received, +7 errors, 100% packet loss, time 10304ms
pipe 4
```

Рисунок 7 – проверка доступности с ub1 до ub2.

На машине ub1 закроем прямой доступ в соседнюю внутреннюю сеть. Это необходимо для создания условий, соответствующих предлагаемой в задании инфраструктуре. Для этого воспользуемся следующей командой:

```
iptables -A OUTPUT -d 10.0.0.0/24 -j DROP
```

```
lera2003@Valeriya:~$ ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 10.0.0.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3056ms
```

Рисунок 8 – проверка доступности с ub1 до ub2 после закрытия прямого доступа.

```
root@Valeriya:~# ping 10.0.1.1
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of data.
From 10.0.1.2 icmp_seq=1 Destination Host Unreachable
From 10.0.1.2 icmp_seq=2 Destination Host Unreachable
From 10.0.1.2 icmp_seq=3 Destination Host Unreachable
From 10.0.1.2 icmp_seq=4 Destination Host Unreachable
^C
--- 10.0.1.1 ping statistics ---
5 packets transmitted, 0 received, +4 errors, 100% packet loss, time 4030ms
pipe 4
```

Рисунок 9 – проверка доступности с ub1 до ub-nat.

```
root@Valeriya:~# ping 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 ---
30 packets transmitted, 0 received, 100% packet loss, time 29673ms
```

Рисунок 10 – проверка выхода в интернет с ub1.



```
lera2003@Valeriya: ~  
lera2003@Valeriya:~$ ping 10.0.1.2  
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.  
^C  
--- 10.0.1.2 ping statistics ---  
20 packets transmitted, 0 received, 100% packet loss, time 19690ms
```

Рисунок 11 – проверка доступности с ub2 до ub1.

```
lera2003@Valeriya:~$ ping 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 ---  
13 packets transmitted, 0 received, 100% packet loss, time 12551ms
```

Рисунок 12 – проверка выхода в интернет с ub2.

```
lera2003@Valeriya:~$ ping 10.0.0.1  
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.  
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.268 ms  
  
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.340 ms  
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.376 ms  
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.374 ms  
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=0.270 ms  
64 bytes from 10.0.0.1: icmp_seq=6 ttl=64 time=0.282 ms  
^C  
--- 10.0.0.1 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5150ms  
rtt min/avg/max/mdev = 0.268/0.318/0.376/0.048 ms
```

Рисунок 13 – проверка доступности с ub2 до ub-nat.

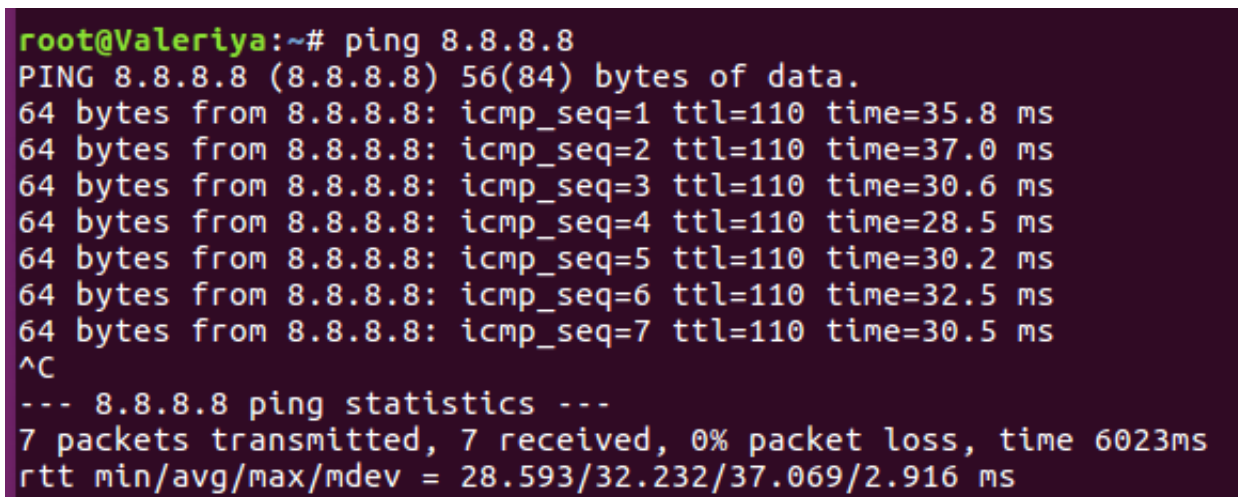
```
lera2003@Valeriya: ~  
lera2003@Valeriya:~$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=30.5 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=28.3 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=30.5 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=36.9 ms  
^C  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3053ms  
rtt min/avg/max/mdev = 28.356/31.597/36.960/3.228 ms
```

Рисунок 14 – проверка выхода в интернет с ub-nat.

2. Настроим доступ с ub1, ub2 в сеть Интернет с использованием Masquerade.

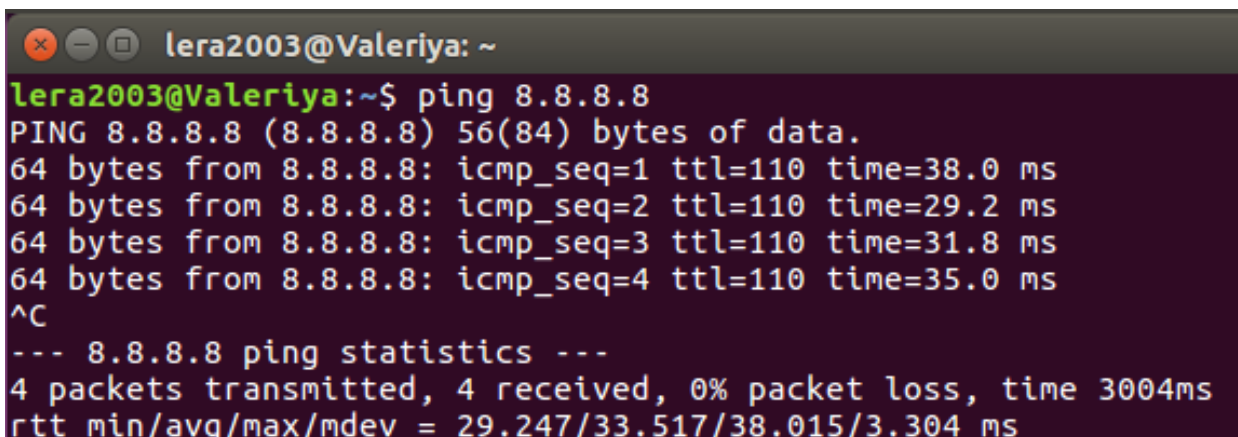
Настроим маршрутизатор ub-nat с помощью следующей команды:

```
iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE
```



```
root@Valeriya:~# ping 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=110 time=35.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=37.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=30.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=28.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=110 time=30.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=110 time=32.5 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=110 time=30.5 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6023ms
rtt min/avg/max/mdev = 28.593/32.232/37.069/2.916 ms
```

Рисунок 15 – проверка выхода в интернет с ub1.



```
lera2003@Valeriya: ~
lera2003@Valeriya:~$ ping 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=110 time=38.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=29.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=31.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=35.0 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 29.247/33.517/38.015/3.304 ms
```

Рисунок 16 – проверка выхода в интернет с ub2.

3. Настройка доступа с ub1, ub2 в сеть Интернет с использованием sNAT.

Прежде всего сбросим предыдущие настройки iptables на ub-nat. Для этого можно воспользоваться следующими командами:

```
iptables -F; iptables -t nat -F; iptables -t mangle -F
```

Рассмотрим настройку sNAT. Для этого на узле, который имеет выход во внешнюю сеть, необходимо настроить вторичный IP-адрес. Он будет связующим звеном между частной и внешней сетями.

Добавим новые ip-адреса в соответствующей сети.



```

lera2003@Valeriya:~$ sudo su
root@Valeriya:/home/lera2003# ip addr add 10.0.2.16/24 dev enp0s9
root@Valeriya:/home/lera2003# ip addr add 10.0.2.17/24 dev enp0s9
root@Valeriya:/home/lera2003# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ab:b8:eb brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.1/24 brd 10.0.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::70b0:b95f:7920:d4b9/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:7b:09:79 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/24 brd 10.0.0.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::c0cb:6eb0:3f7f:2abc/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:99:95:e2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s9
        valid_lft forever preferred_lft forever
    inet 10.0.2.16/24 scope global secondary enp0s9
        valid_lft forever preferred_lft forever
    inet 10.0.2.17/24 scope global secondary enp0s9
        valid_lft forever preferred_lft forever
    inet6 fe80::dc6a:1359:86aa:c912/64 scope link
        valid_lft forever preferred_lft forever

```

Рисунок 17 – добавление адресов на ub-nat.

Теперь настроим на узле маршрутизации sNAT:

```

iptables -t nat -A POSTROUTING -s 10.0.1.2/32 -o enp0s9 -j SNAT --to-source 10.0.2.16
iptables -t nat -A POSTROUTING -s 10.0.0.3/32 -o enp0s9 -j SNAT --to-source 10.0.2.17

```

Рисунок 18 – настройка sNAT на ub-nat.

Данное правило означает, что в цепочке NAT после обработки пакета для всех пакетов, IP-адрес источника которых равен 10.0.1.2/10.0.0.3 (т. е. они были отправлены с этого узла), будет происходить его смена на 10.0.2.16/10.0.2.17 (IP-адрес, доступный во внешней сети). Благодаря этому правилу пакет, отправленный из частной сети, сможет дойти до необходимого узла во внешней сети и получить ответ.

```

lera2003@Valeriya:~$ ping 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=110 time=35.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=33.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=31.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=42.2 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 31.392/35.565/42.209/4.061 ms

```

Рисунок 19 – проверка выхода в интернет с ub1.

```

ler2003@Valeriya:~$ ping 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=110 time=41.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=35.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=28.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=34.4 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 28.585/34.937/41.205/4.475 ms

```

Рисунок 20 – проверка выхода в интернет с ub2.

#### 4. Настройка доступа с ub2 на ub1 с использованием dNAT.

Настроим dNAT на ub-nat так, чтобы с машины ub2 можно было получить доступ к ub1, используя адрес из NAT-сети. Перед этим сбросим настройки iptables.

```

iptables -t nat -A PREROUTING -d 10.0.2.16 -j DNAT --to-destination 10.0.1.2
iptables -t nat -A PREROUTING -d 10.0.2.17 -j DNAT --to-destination 10.0.0.3

```

Рисунок 21 – настройка dNAT на ub-nat.

Данное правило означает, что если из внешней («публичной») сети пакет будет отправлен на 10.0.2.16/10.0.2.17, то при прохождении через узел, на котором это правило настроено, произойдет подмена IP-адреса назначения, и пакет дойдет до требуемого узла в частной сети с IP-адресом 10.0.1.2/10.0.0.3.

Об успешном выполнении данной задачи свидетельствует демонстрация ssh-подключения к вторичному IP-адресу, в результате которой будет открываться сессия с ub1:

```

ler2003@Valeriya:~$ sudo su
root@Valeriya:/home/lera2003# ssh lera2003@10.0.2.16
The authenticity of host '10.0.2.16 (10.0.2.16)' can't be established.
ECDSA key fingerprint is SHA256:VX6kCL3sDczoETLWp20FCWH65ciI/UUaBIYWpVJ/vYE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.16' (ECDSA) to the list of known hosts.
lera2003@10.0.2.16's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Могут быть обновлены 42 пакета.
2 обновления касаются безопасности системы.

Last login: Thu Mar 16 06:14:15 2023

```

Рисунок 22 – подключение по ssh.

## **Выводы.**

В ходе выполнения работы были изучены протоколы трансляции сетевых адресов (NAT), а именно: Masquerade, SNAT и DNAT. Построена сеть из виртуальных машин для тестирования работы механизмов трансляции сетевых адресов. Каждый тип NAT был настроен и была проверена его работа (выход в глобальную сеть с помощью Masquerade и SNAT, доступ к внутренним сетям через DNAT).