

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. 9304

Прокофьев М.Д.

Преподаватель

Фирсов М.А.

Санкт-Петербург

2021

Цель работы.

Изучение механизмов преобразования сетевых адресов: NAT, Masquerade.

Задание.

Вариант 16

1. **Создать и настроить инфраструктуру для выполнения лабораторной работы.** Развернуть 3 виртуальных машины (лабораторная 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 MASQUERADE, 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.

Выполнение работы.

1) Создать и настроить инфраструктуру для выполнения лабораторной работы. Развернуть 3 виртуальных машины (лабораторная 1). Настроить их в соответствии с подразделом «Построение инфраструктуры для выполнения работы».

Изначально были созданы три виртуальные машины: ub1, ub2 и ub-nat. Их настройка проведена в соответствии с подразделом «Построение

инфраструктуры для выполнения работы». Конфигурация виртуальных машин представлена на рисунках 1-2:

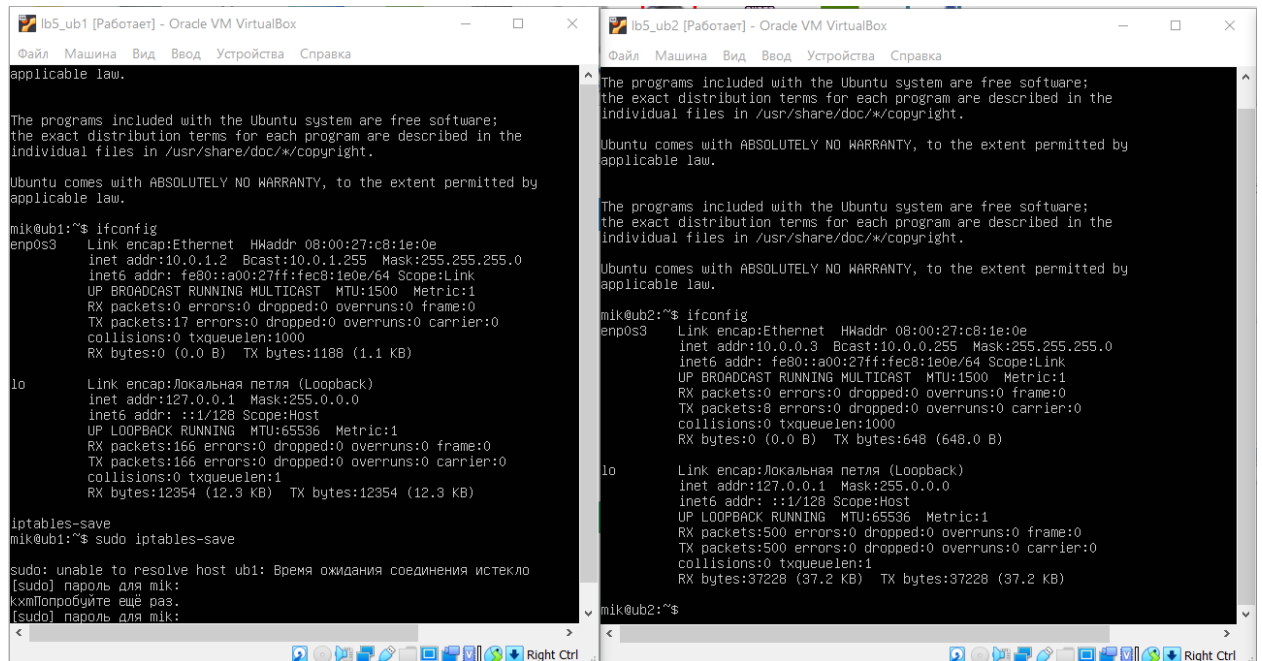


Рисунок 1 – Конфигурация ub1 и ub2

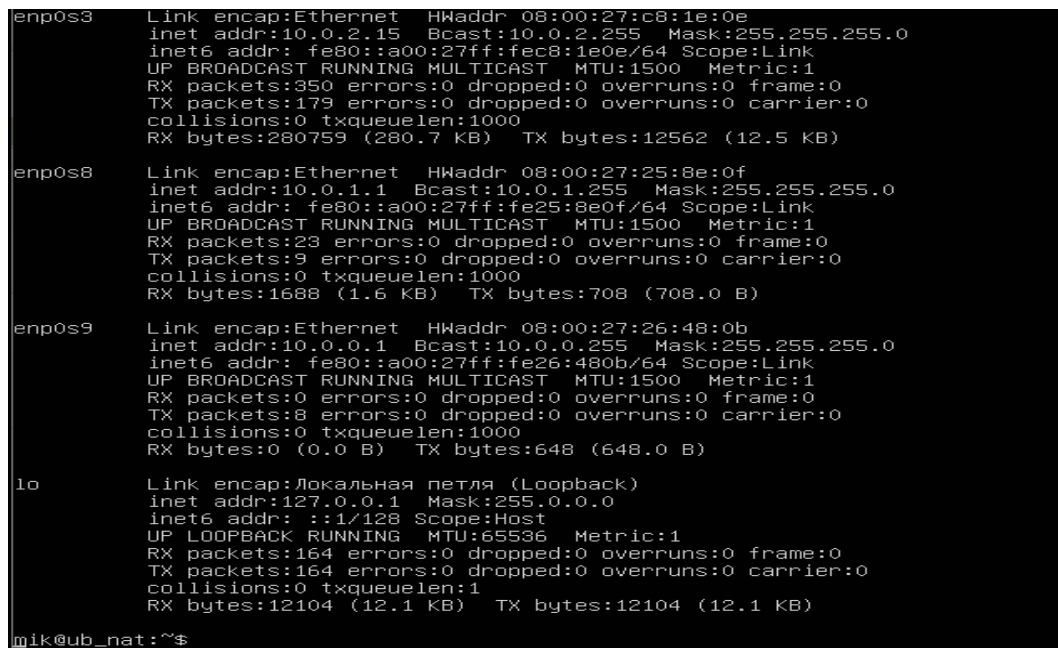
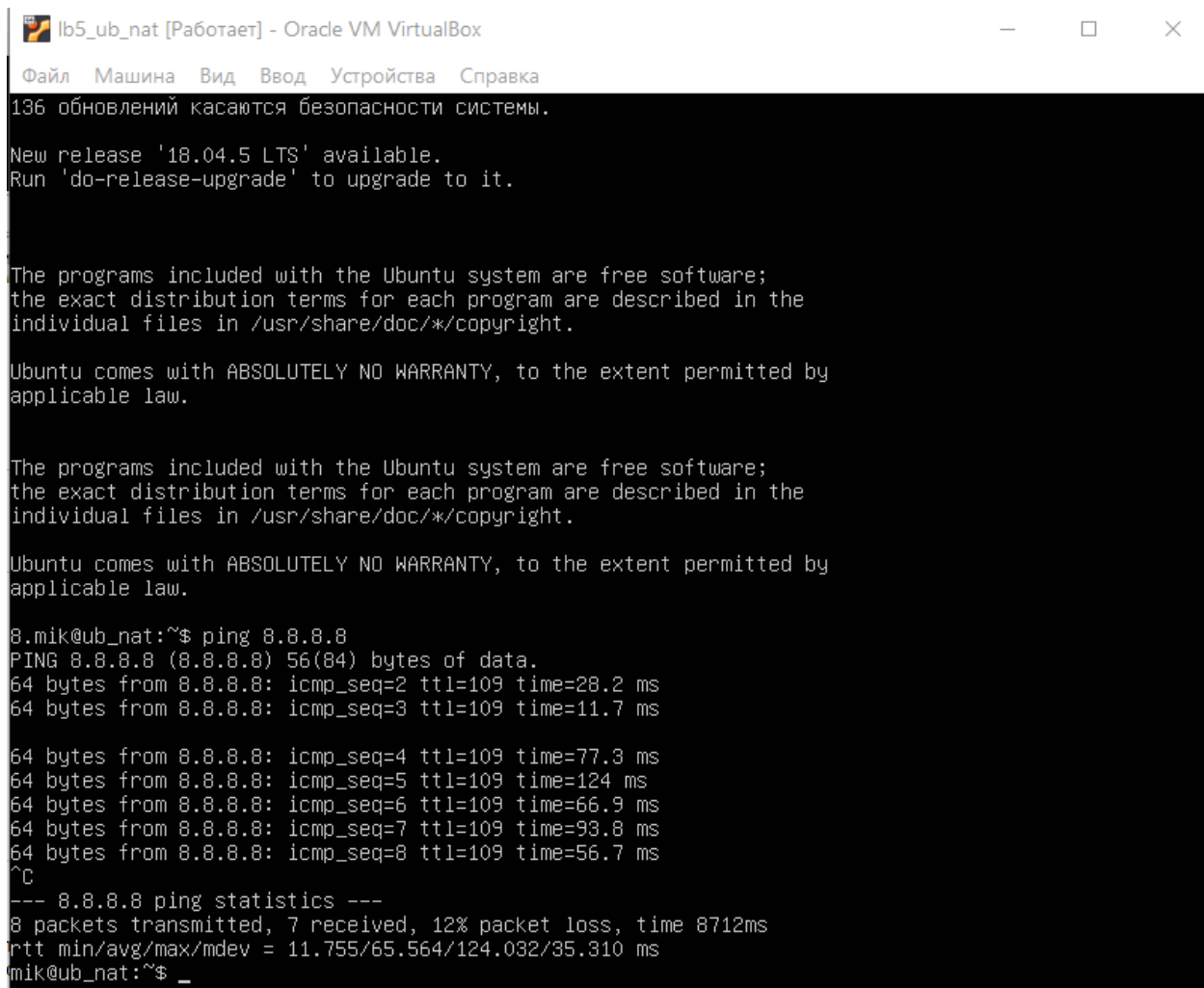


Рисунок 2 – Конфигурация ub_nat

Для проверки доступа ub_nat к интернету была прописана команда *ping*

8.8.8.8:



```
lb5_ub_nat [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
136 обновлений касаются безопасности системы.
New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

8.mik@ub_nat:~$ 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=2 ttl=109 time=28.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=11.7 ms

64 bytes from 8.8.8.8: icmp_seq=4 ttl=109 time=77.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=109 time=124 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=109 time=66.9 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=109 time=93.8 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=109 time=56.7 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 7 received, 12% packet loss, time 8712ms
rtt min/avg/max/mdev = 11.755/65.564/124.032/35.310 ms
mik@ub_nat:~$ _
```

Рисунок 3 – Доступ в интернет с ub_nat

Из рисунка видно, что ub_nat действительно имеет соединение с интернетом.

Затем, чтобы убрать доступ с ub2 на ub1, была прописана команда: *sudo iptables -A OUTPUT -d 10.0.0.0/24 -j DROP*. После чего проведена проверка, действительно ли ub2 не имеет доступ к ub1. Результат выполнения этой проверки представлен на рисунке 4:

```

    inet6 addr: fe80::a00:27ff:fec8:1e0e/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:17 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B)  TX bytes:1188 (1.1 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:166 errors:0 dropped:0 overruns:0 frame:0
      TX packets:166 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1
      RX bytes:12354 (12.3 KB)  TX bytes:12354 (12.3 KB)

iptables-save
mik@ub1:~$ sudo iptables-save

sudo: unable to resolve host ub1: Время ожидания соединения истекло
[sudo] пароль для mik:
kxmПопробуйте ещё раз.
[sudo] пароль для mik:
mik@ub1:~$ sudo iptables -A OUTPUT -d 10.0.0.0/24 -j DROP
ping 10.0.0.3
sudo: unable to resolve host ub1: Время ожидания соединения истекло
mik@ub1:~$ 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 3023ms
mik@ub1:~$ _

```

Рисунок 4 – Недоступность подсети ub1 с ub2

Аналогичная проверка была совершена со стороны ub2 с ub1, результат представлен на рисунке 5:

```

mik@ub2:~$ 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 ---
7 packets transmitted, 0 received, 100% packet loss, time 6047ms
mik@ub2:~$ _

```

Рисунок 5 – Недоступность подсети ub2 с ub1

После чего была проведена проверка, имеют ли ub1 и ub2 прямой доступ в интернет. Результат проверки продемонстрирован на рисунке 6:

```
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:166 errors:0 dropped:0 overruns:0 frame:0
        TX packets:166 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:12354 (12.3 KB)  TX bytes:12354 (12.3 KB)

iptables-save
mik@ub1:~$ sudo iptables-save
[sudo] пароль для mik:
kxmПопробуйте ещё раз.
[sudo] пароль для mik:
mik@ub1:~$ sudo iptables -A OUTPUT -d 10.0.0.0/24 -j DROP
ping 10.0.0.3
[sudo] unable to resolve host ub1: Время ожидания соединения истекло
mik@ub1:~$ 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 3023ms

mik@ub1:~$ 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 ---
12 packets transmitted, 0 received, 100% packet loss, time 11088ms

mik@ub1:~$

individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

mik@ub2:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:c8:1e:0e
        inet addr:10.0.0.3  Bcast:10.0.0.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fec8:1e0e/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:648 (648.0 B)

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:500 errors:0 dropped:0 overruns:0 frame:0
        TX packets:500 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:37228 (37.2 KB)  TX bytes:37228 (37.2 KB)

mik@ub2:~$ 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 ---
7 packets transmitted, 0 received, 100% packet loss, time 6047ms

mik@ub2:~$ 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 ---
10 packets transmitted, 0 received, 100% packet loss, time 9071ms

mik@ub2:~$ _
```

Рисунок 6 – отсутствие доступа в интернет с ub1 и ub2

Но при этом ub1 и ub2 имеют доступ ub_nat, что и показано на рисунке 7:

```
[sudo] пароль для mik:
mik@ub1:~$ sudo iptables -A OUTPUT -d 10.0.0.0/24 -j DROP
ping 10.0.0.3
[sudo] unable to resolve host ub1: Время ожидания соединения истекло
mik@ub1:~$ 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 3023ms

mik@ub1:~$ 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 ---
12 packets transmitted, 0 received, 100% packet loss, time 11088ms

mik@ub1:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.357 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.390 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.493 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.507 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.520 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.512 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.475 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.423 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.404 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.416 ms
^C
--- 10.0.2.15 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9007ms
rtt min/avg/max/mdev = 0.357/0.449/0.520/0.060 ms
mik@ub1:~$

TX packets:500 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:37228 (37.2 KB)  TX bytes:37228 (37.2 KB)

mik@ub2:~$ 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 ---
7 packets transmitted, 0 received, 100% packet loss, time 6047ms

mik@ub2:~$ 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 ---
10 packets transmitted, 0 received, 100% packet loss, time 9071ms

mik@ub2:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.480 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.534 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.546 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.466 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.528 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.486 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.404 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.527 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.400 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.478 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.550 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.465 ms
64 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=0.553 ms
64 bytes from 10.0.2.15: icmp_seq=14 ttl=64 time=0.556 ms
^C
--- 10.0.2.15 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13017ms
rtt min/avg/max/mdev = 0.400/0.498/0.556/0.051 ms
mik@ub2:~$ _
```

Рисунок 7 – доступ к интерфейсу ub-nat с ub1 и ub2

Для сохранения настроек iptables, в /etc/network/interfaces написана строка *pre-up iptables-restore < /root/firewall.rules*. Это показано на рисунке 8:

```
# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 10.0.1.2
netmask 255.255.255.0
gateway 10.0.1.1
pre-up iptables-restore < /root/firewall.rules
```

Рисунок 8 – Сохранение настроек iptables на ub1

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

Был настроен Masquerade на ub_nat. Настройка проходила с помощью функции: *sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE*. Процесс настройки представлен на рисунке 9:

```
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:350 errors:0 dropped:0 overruns:0 frame:0
TX packets:179 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:280759 (280.7 KB)  TX bytes:12562 (12.5 KB)

enp0s8  Link encap:Ethernet  HWaddr 08:00:27:25:8e:0f
        inet addr:10.0.1.1  Bcast:10.0.1.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe25:8e0f/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:23 errors:0 dropped:0 overruns:0 frame:0
        TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1688 (1.6 KB)  TX bytes:708 (708.0 B)

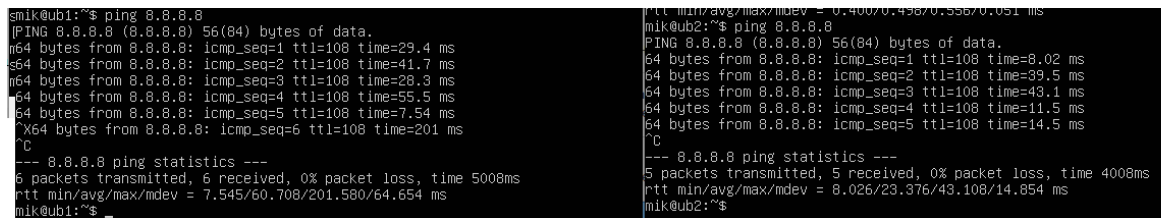
enp0s9  Link encap:Ethernet  HWaddr 08:00:27:26:48:0b
        inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe26:480b/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:648 (648.0 B)

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:164 errors:0 dropped:0 overruns:0 frame:0
        TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:12104 (12.1 KB)  TX bytes:12104 (12.1 KB)

sudo iptables -t nat -A POSTROUTING -o enp0s -j MASQUERADE
sudo: unable to resolve host ub_nat
[sudo] пароль для mik:
mik@ub_nat:~$
```

Рисунок 9 – Настройка Masquerade на ub-nat

После настройки ub1 и ub2 имеют доступ к интернету, что и представлено на рисунке 10:

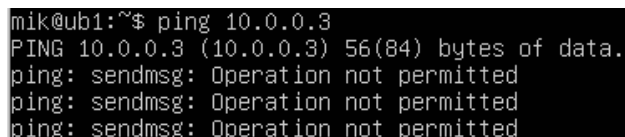


```
mik@ub1:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=108 time=29.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=41.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=108 time=28.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=108 time=55.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=108 time=7.54 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=108 time=201 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 7.545/60.708/201.580/64.654 ms
mik@ub1:~$ _

mik@ub2:~$ 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=108 time=8.02 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=39.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=108 time=43.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=108 time=11.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=108 time=14.5 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 8.026/23.376/43.108/14.854 ms
mik@ub2:~$
```

Рисунок 10 – Доступ в интернет с ub1 и ub2

И при этом с ub1 на ub2 по-прежнему нет доступа, что и показано на рисунке 11:



```
mik@ub1:~$ 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
```

Рисунок 11 – Отсутствие доступа с ub1 к ub2

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.

Для настройки sNAT, первоначально был изменен IP-адрес на ub_nat. В данном случае вторичным IP-адресом будет 48.84.48.84. Его настройка представлена на рисунке 12:


```
GNU nano 2.5.3      Файл: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet dhcp

iface enp0s3 inet static
address 48.84.48.84
netmask 255.255.255.0

auto enp0s8
iface enp0s8 inet static
address 10.0.1.1
netmask 255.255.255.0

auto enp0s9
iface enp0s9 inet static
address 10.0.0.1
netmask 255.255.255.0

pre-up iptables-restore < /root/firewall.rules
```

Рисунок 12 – Настройка вторичного IP-адреса на `ub_nat`

Затем, на `ub_nat` был настроен sNAT для `ub1` с помощью команды: `sudo iptables -t nat -A POSTROUTING -s 10.0.1.2/32 -o enp0s3 -j SNAT --to-source 48.84.48.84`, результат настройки показан на рисунке 13:

```
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:c8:1e:0e
       inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
       inet6 addr: fe80::a00:27ff:fec8:1e0e/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:359 errors:0 dropped:0 overruns:0 frame:0
       TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:281607 (281.6 KB)  TX bytes:13444 (13.4 KB)

enp0s8  Link encap:Ethernet  HWaddr 08:00:27:25:8e:0f
       inet addr:10.0.1.1  Bcast:10.0.1.255  Mask:255.255.255.0
       inet6 addr: fe80::a00:27ff:fe25:8e0f/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B)  TX bytes:648 (648.0 B)

enp0s9  Link encap:Ethernet  HWaddr 08:00:27:26:48:0b
       inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
       inet6 addr: fe80::a00:27ff:fe26:480b/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B)  TX bytes:648 (648.0 B)

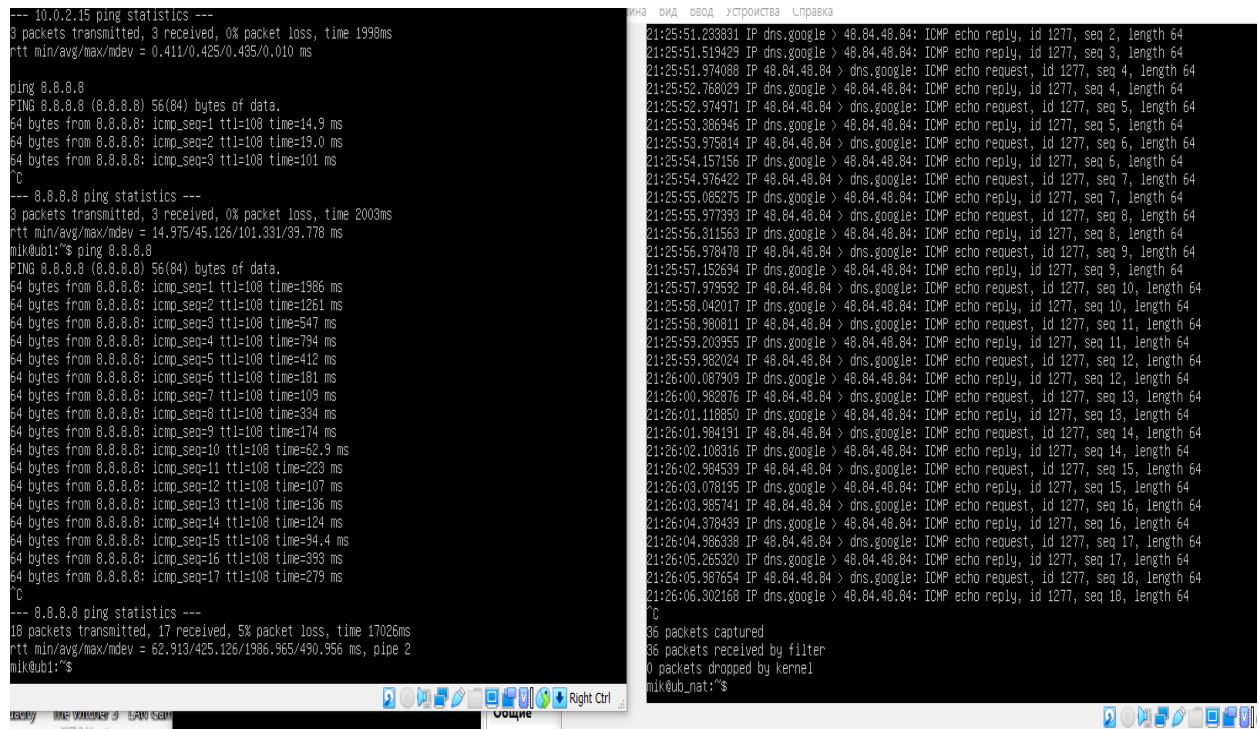
lo      Link encap:Локальная петля (Loopback)
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING  MTU:65536  Metric:1
       RX packets:160 errors:0 dropped:0 overruns:0 frame:0
       TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1
       RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

sudo iptables -t nat -A POSTROUTING -s 10.0.1.2/32 -o enp0s3 -j SNAT --to-source 48.84.48.84
```

Рисунок 13 – Настройка sNAT для `ub1`

После этого была введена команда *sudo tcpdump -p icmp -I enp0s3* на *ub_nat*.

Для проверки работы, с *ub1* была совершена команда *ping 8.8.8.8* для отправки пакетов во внешнюю сеть. Результат работы представлен на рисунке 14:



```
--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.411/0.425/0.435/0.010 ms

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=108 time=14.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=19.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=108 time=101 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 14.975/45.126/101.331/39.778 ms
mik@ub1:~$ 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=108 time=1986 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=1261 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=108 time=547 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=108 time=794 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=108 time=412 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=108 time=181 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=108 time=109 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=108 time=334 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=108 time=174 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=108 time=62.9 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=108 time=223 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=108 time=107 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=108 time=136 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=108 time=124 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=108 time=94.4 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=108 time=399 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=108 time=279 ms
^C
--- 8.8.8.8 ping statistics ---
18 packets transmitted, 17 received, 5% packet loss, time 17026ms
rtt min/avg/max/mdev = 62.913/425.126/1986.965/490.956 ms, pipe 2
mik@ub1:~$
```

```
21:25:51.233831 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 2, length 64
21:25:51.519429 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 3, length 64
21:25:51.974088 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 4, length 64
21:25:52.768029 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 4, length 64
21:25:52.974971 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 5, length 64
21:25:53.966946 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 5, length 64
21:25:53.975814 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 6, length 64
21:25:54.157156 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 6, length 64
21:25:54.976422 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 7, length 64
21:25:55.085275 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 7, length 64
21:25:55.977393 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 8, length 64
21:25:56.311563 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 8, length 64
21:25:56.978478 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 9, length 64
21:25:57.152694 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 9, length 64
21:25:57.979532 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 10, length 64
21:25:58.042017 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 10, length 64
21:25:58.980811 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 11, length 64
21:25:59.203955 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 11, length 64
21:25:59.982024 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 12, length 64
21:26:00.087909 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 12, length 64
21:26:00.982876 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 13, length 64
21:26:01.118850 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 13, length 64
21:26:01.984191 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 14, length 64
21:26:02.108316 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 14, length 64
21:26:02.984539 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 15, length 64
21:26:03.078195 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 15, length 64
21:26:03.985741 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 16, length 64
21:26:04.378439 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 16, length 64
21:26:04.986338 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 17, length 64
21:26:05.265320 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 17, length 64
21:26:05.987654 IP 48.84.48.84 > dns.google: ICMP echo request, id 1277, seq 18, length 64
21:26:06.302168 IP dns.google > 48.84.48.84: ICMP echo reply, id 1277, seq 18, length 64
^C
36 packets captured
36 packets received by filter
0 packets dropped by kernel
mik@ub_nat:~$
```

Рисунок 14 – Работа sNAT при отправке пакетов по внешнюю сеть с *ub1*

Аналогичные действия были проделаны и для *ub2*, был настроен sNAT для 10.0.0.3, что показано на рисунке 15:

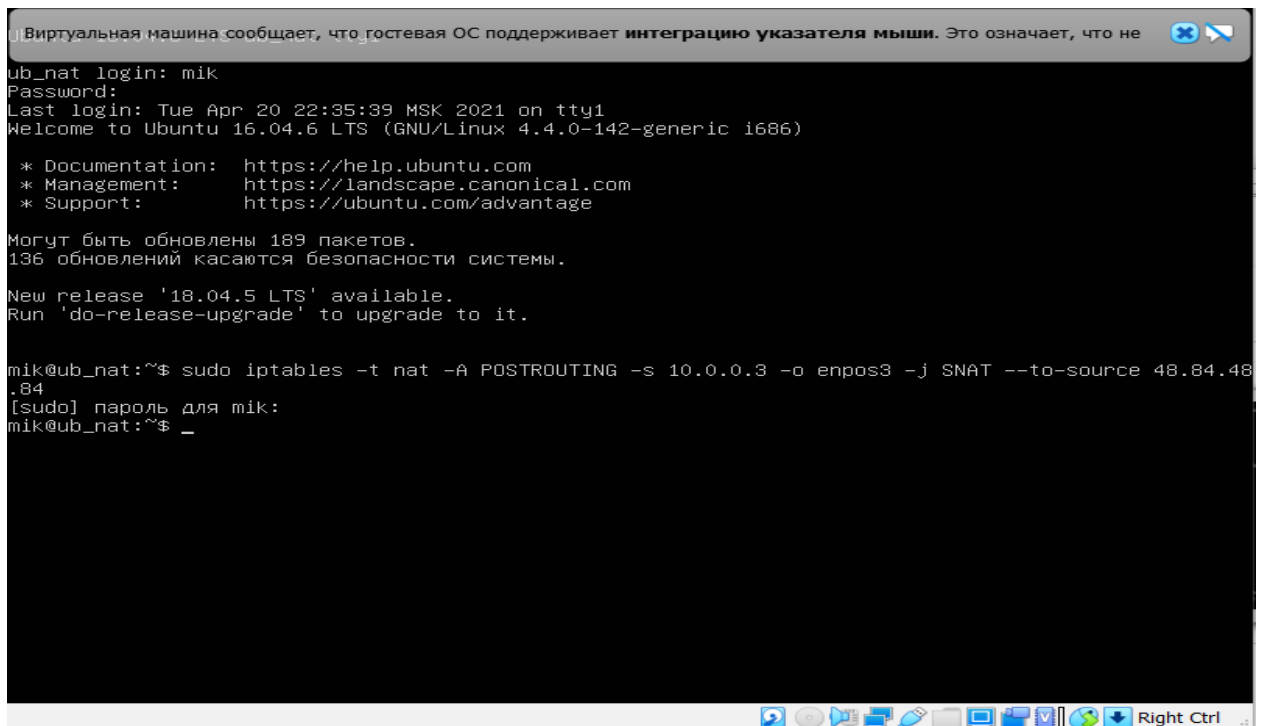


Рисунок 15 – Настройка sNAT для ub2

После чего, с ub2 были отправлены пакеты по внешнюю сеть, что иллюстрирует рисунок 16:

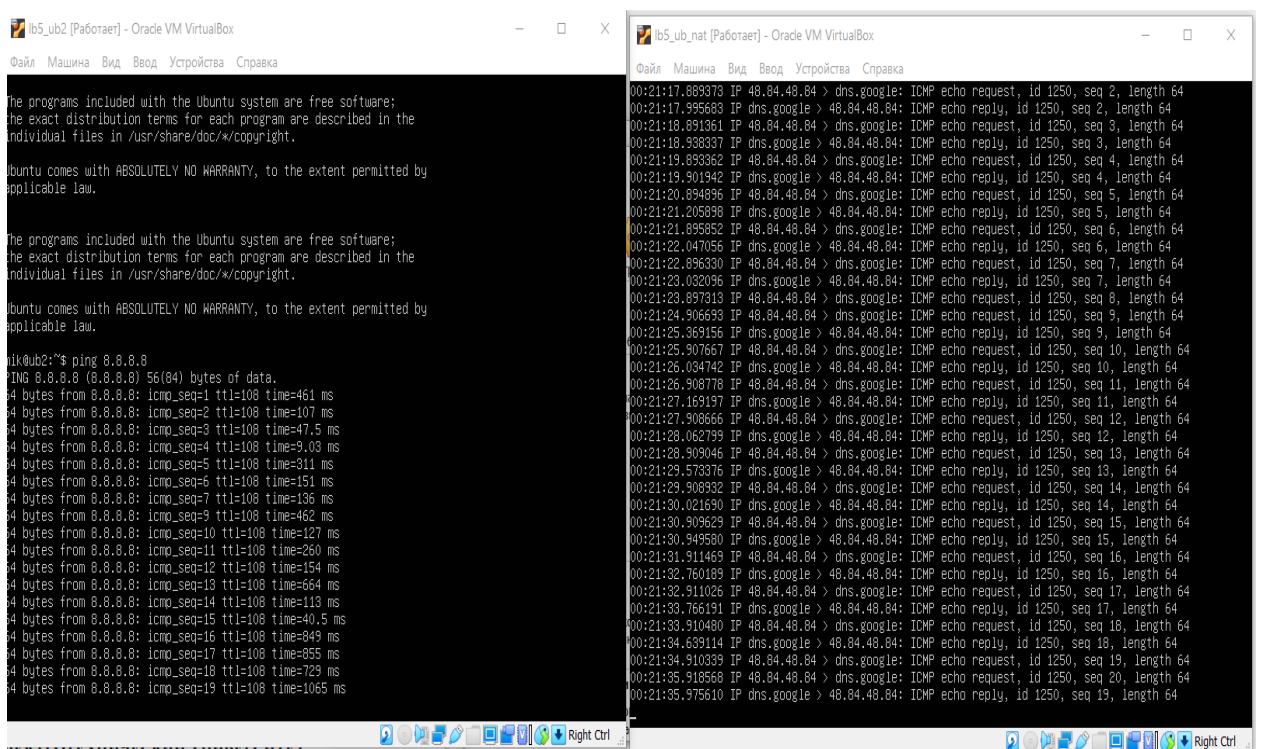
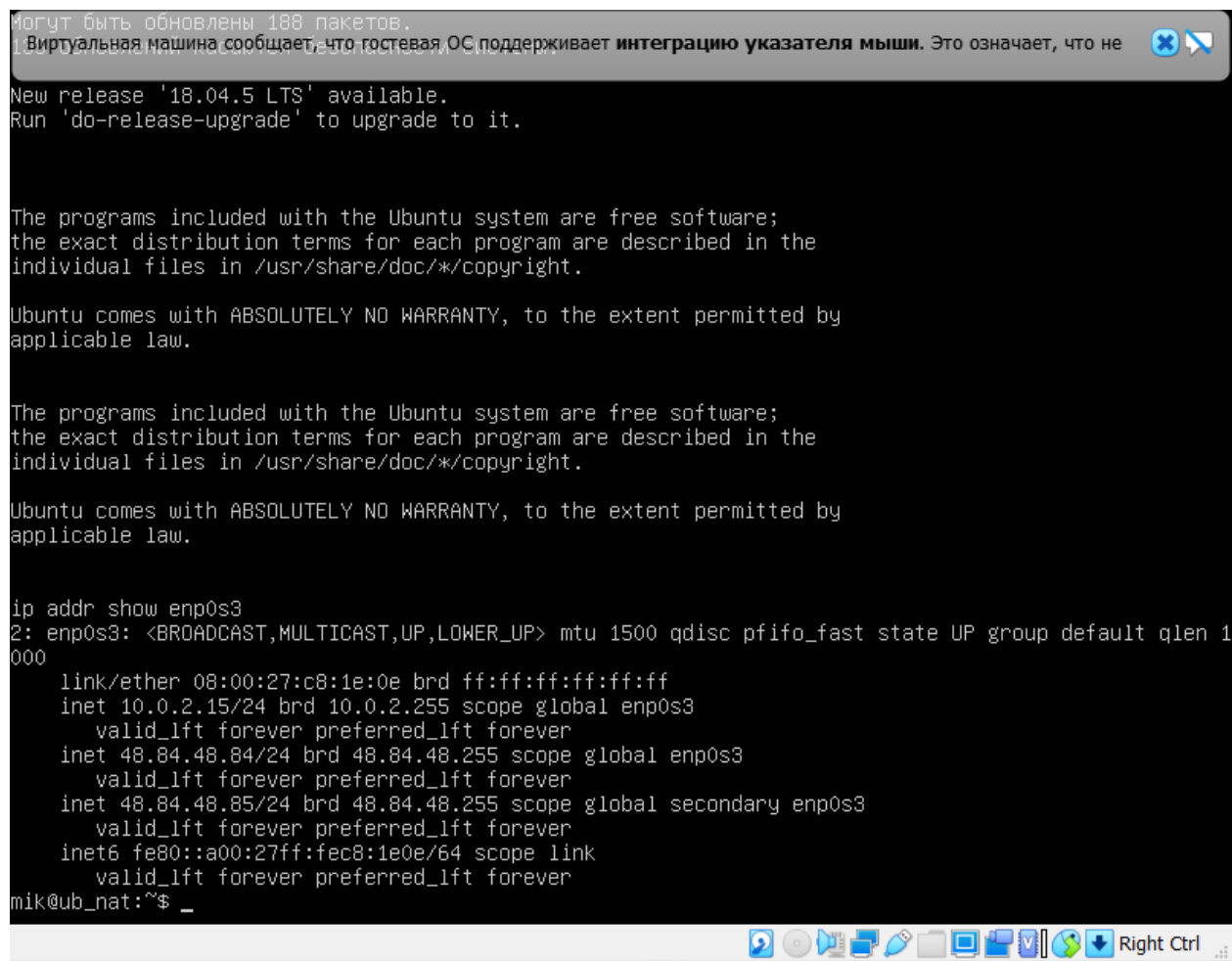


Рисунок 16 – Работа sNAT при отправке пакетов по внешнюю сеть с ub2

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`.

Для выполнения этого пункта задания был изначально создан вторичный IP-адрес на `ub_nat` результаты настройки представлены на рисунке 17:



```
Могут быть обновлены 188 пакетов.
Виртуальная машина сообщает, что гостевая ОС поддерживает интеграцию указателя мыши. Это означает, что не
New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:c8:1e:0e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet 48.84.48.84/24 brd 48.84.48.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet 48.84.48.85/24 brd 48.84.48.255 scope global secondary enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec8:1e0e/64 scope link
        valid_lft forever preferred_lft forever
mik@ub_nat:~$
```

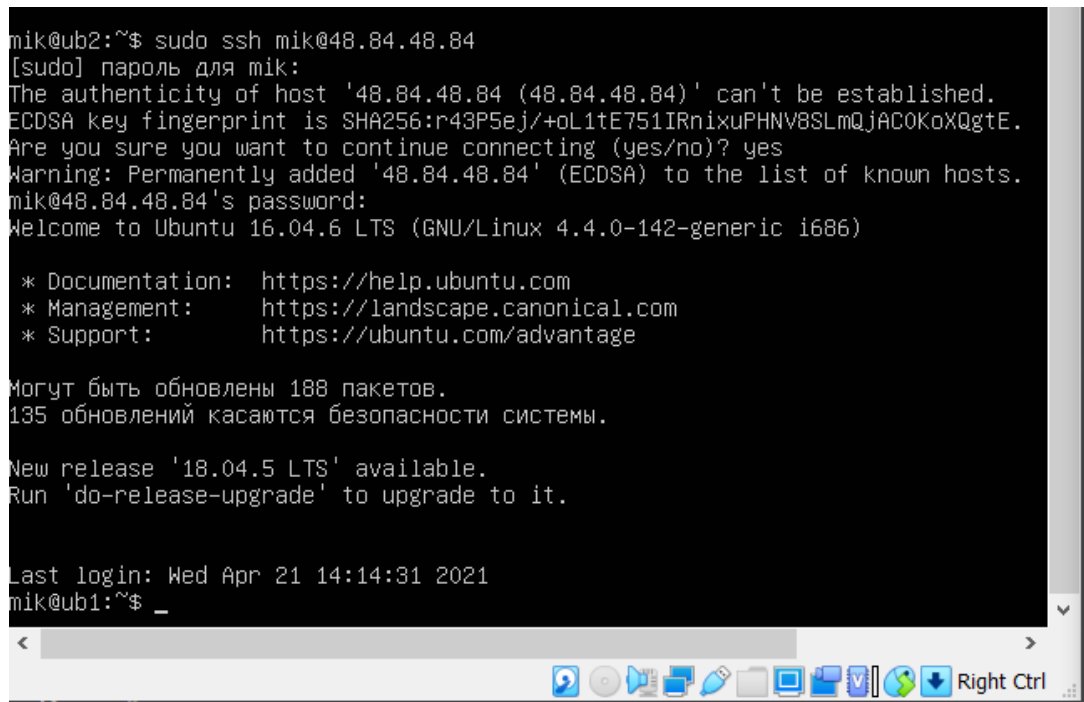
Рисунок 17 – Настройка вторичного IP-адреса

Затем, была выполнена команда настройки dNAT для `ub1` и `ub2`, что и показано на рисунке 18:

```
mik@ub_nat:~$ sudo iptables -t nat -A PREROUTING -d 48.84.48.84 -j DNAT --to-destination 10.0.1.2
mik@ub_nat:~$ sudo iptables -t nat -A PREROUTING -d 48.84.48.85 -j DNAT --to-destination 10.0.0.3
```

Рисунок 18 – Выполнение команды настройки dNAT для ub1 и ub2

После чего была совершена проверка подключения с ub2 на ub1 по ssh. Результат проверки представлен на рисунке 19:



```
mik@ub2:~$ sudo ssh mik@48.84.48.84
[sudo] пароль для mik:
The authenticity of host '48.84.48.84 (48.84.48.84)' can't be established.
ECDSA key fingerprint is SHA256:r43P5ej/+oL1tE751IRnixuPHNV8SLmQjAC0KoXQgtE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '48.84.48.84' (ECDSA) to the list of known hosts.
mik@48.84.48.84's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

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

Могут быть обновлены 188 пакетов.
135 обновлений касаются безопасности системы.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Apr 21 14:14:31 2021
mik@ub1:~$ _
```

Рисунок 19 – Подключение по SSH с ub2 на ub1

Из рисунка видно, что подключение с ub2 на ub1 по ssh прошло успешно.

Выводы.

Были изучены механизмы преобразования сетевых адресов: NAT, Masquerade.