

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

ОТЧЕТ
по лабораторной работе №5
по дисциплине «Сети и телекоммуникации»
ТЕМА: ИЗУЧЕНИЕ МЕХАНИЗМОВ ТРАНСЛЯЦИИ СЕТЕВЫХ АДРЕСОВ: NAT,
MASQUERADE

Студент гр. 9303

Павлов Д.Р.

Преподаватель

Лавров А.А.

Санкт-Петербург

2021

Цель работы.

Изучение механизмов преобразования сетевых адресов: NAT, Masquerade.

Постановка задачи.

1. Создать и настроить инфраструктуру для выполнения лабораторной работы. Развернуть три виртуальные машины. 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»`.

Выполнение работы.

1) Создать и настроить инфраструктуру для выполнения лабораторной работы.

На рисунках 1-3 можно увидеть настройки виртуальных машин ub1, ub2 и ub-nat. Также на ub1 и ub2 были настроены шлюзы по умолчанию, для ub1 им будет являться 10.0.1.2, для ub2 – 10.0.0.3.

```

enp0s3  Link encap:Ethernet  HWaddr 08:00:27:c8:1e:0e
        inet addr:10.0.1.2  Bcast:10.0.1.255  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: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)

```

Рисунок 1 - Настройки ub1

```

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)

```

Рисунок 2 - Настройки ub2

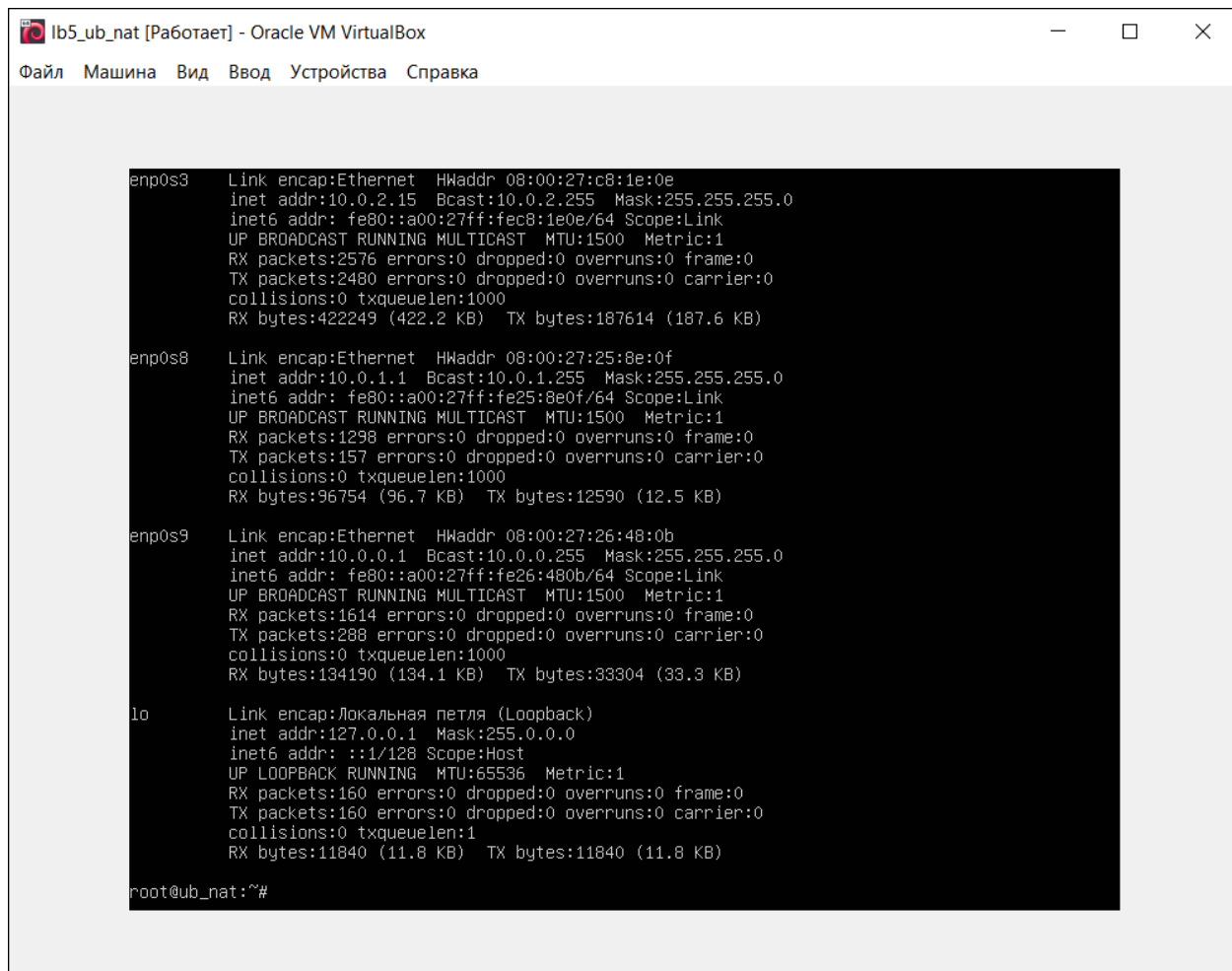


Рисунок 3 - Настройки ub-nat

Далее запретим на ub2 доступ к ub1. Команда для этого действия *sudo iptables -A OUTPUT -d 10.0.0.0/24 -j DROP*

На рис. 6 и 7 представлены результаты пинга после запрета доступа.

```

root@ub1:~# sudo iptables -A OUTPUT -d 10.0.0.0/24 -j DROP
root@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
ping: sendmsg: Operation not permitted
^C
--- 10.0.0.3 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 3999ms

```

Рисунок 4 - Пинг с ub1 на ub2 после запрета доступа

```
--- 10.0.1.2 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7014ms
rtt min/avg/max/mdev = 0.804/1.040/1.752/0.275 ms
root@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 ---
4 packets transmitted, 0 received, 100% packet loss, time 3000ms
```

Рисунок 5 - Пинг с ub2 на ub1 после запрета доступа.

На рисунках 8, 9 показано, что ub1 и ub2 не имеют доступ в интернет. На рисунках 10 показано, что ub2 имеют доступ к ub-nat, а на рисунке 11 изображен доступ ub-nat в интернет.

```
root@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 ---
5 packets transmitted, 0 received, 100% packet loss, time 3998ms
```

Рисунок 6 - Отсутствие доступа в интернет с ub1

```
root@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 ---
2 packets transmitted, 0 received, 100% packet loss, time 1000ms
```

Рисунок 7 - Отсутствие доступа в интернет с ub2

```

root@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=0.552 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.561 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.537 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.545 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.999 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.382 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.560 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.967 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.564 ms
^C
--- 10.0.2.15 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8026ms
rtt min/avg/max/mdev = 0.382/0.629/0.999/0.198 ms

```

Рисунок 80 - Доступ с ub2 на ub-nat

```

root@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=1 ttl=111 time=14.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=8.49 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=25.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=11.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=111 time=25.6 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=111 time=21.5 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5011ms
rtt min/avg/max/mdev = 8.494/17.904/25.825/6.826 ms

```

Рисунок 11 - Доступ в интернет с ub-nat

2) *Настройка доступа с ub1, ub2 в сеть Интернет с использованием Masquerade.*

Настроим Masquerade на ub-nat с помощью команды, представленной на рис. 12.

```

root@ub_nat:~# sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

```

Рисунок 12 - Команда настройки Masquerade

На рисунках 13, 14 показано, что ub1 и ub2 теперь имеют доступ в интернет.

```

root@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=110 time=12.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=11.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=11.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=36.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=110 time=12.8 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=110 time=13.4 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=110 time=32.0 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 11.919/18.712/36.225/9.844 ms

```

Рисунок 13 - Доступ в интернет с ub1 после настройки Masquerade

```

root@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=110 time=21.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=10.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=14.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=13.6 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3012ms
rtt min/avg/max/mdev = 10.117/14.728/21.072/3.973 ms

```

Рисунок 14 - Доступ в интернет с ub2 после настройки Masquerade

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

Для настройки sNAT на ub-nat были добавлены 2 вторичных ip-адреса – 10.25.26.27/24 и 10.25.26.28/24. Их можно увидеть на рис. 15. Далее, с помощью команд, изображенных на рисунке 16, был настроен sNAT для ub2 и ub2 на ub-nat. На рисунках 17 показана работа sNAT при пинге .

```

root@ub_nat:~# ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    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 10.25.26.27/24 brd 10.25.26.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet 10.25.26.28/24 brd 10.25.26.255 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
root@ub_nat:~#

```

Рисунок 15 - Вторичные адреса на ub-nat

```
root@ub_nat:~# sudo iptables -t nat -A POSTROUTING -s 10.0.0.3/32 -o enp0s3 -j SNAT --to-source 10.25.26.28
```

Рисунок 16 - Команда настройки sNAT для ub2

```
root@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=110 time=13.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=33.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=26.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=18.1 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 13.339/22.763/33.026/7.583 ms
```

Рисунок 17 - Работа sNAT при пинге с ub2 в интернет

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

На рисунках 18 и 19 показаны команды для настройки dNAT для ub1 и ub2 на ub-nat.

```
root@ub_nat:~# sudo iptables -t nat -A PREROUTING -d 10.25.26.27 -j DNAT --to-destination 10.0.1.2
```

Рисунок 18 - Команда настройки dNAT для ub1

```
root@ub_nat:~# sudo iptables -t nat -A PREROUTING -d 10.25.26.28 -j DNAT --to-destination 10.0.0.3
```

Рисунок 19 - Команда настройки dNAT для ub2

На рисунке 20 показано подключение с ub2 на ub1 по ssh при помощи dNAT.

```
root@ub2:~# sudo ssh root@10.25.26.27
The authenticity of host '10.25.26.27 (10.25.26.27)' 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 '10.25.26.27' (ECDSA) to the list of known hosts.
root@10.25.26.27'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.

Last login: Sat May 15 16:29:26 2021
root@ub1:~#
```

Рисунок 20 - Подключение с ub2 к ub1 по ssh

Выводы.

Были изучены механизмы преобразования сетевых адресов: NAT, Masquerade.