**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.

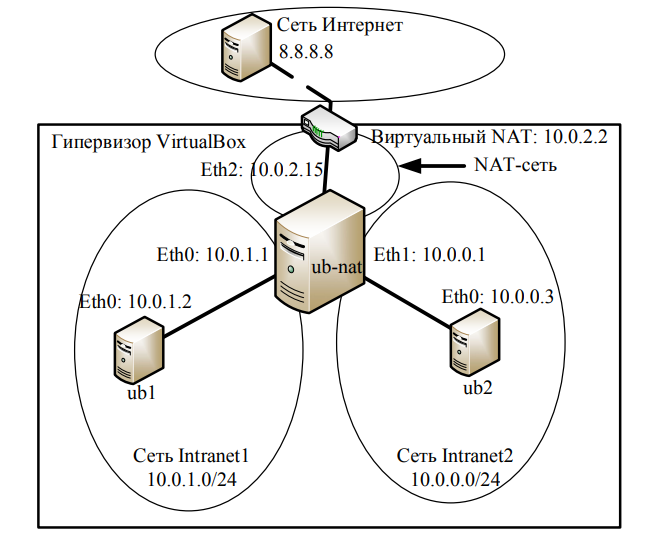
5. Настроить доступ к сети Интернет для одной из машин с помощью sNAT.

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.

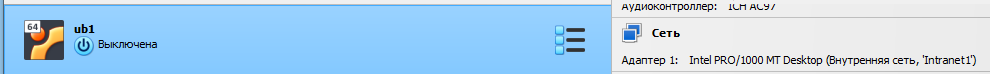


Рисунок 1 – настройка сети для ub1.

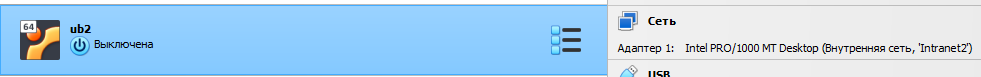


Рисунок 2 – настройка сети для ub2.

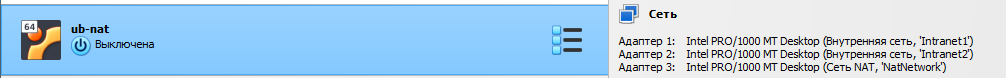


Рисунок 3 – настройка сети для ub-nat.

Настройка конфигурации сетевых интерфейсов на машинах:

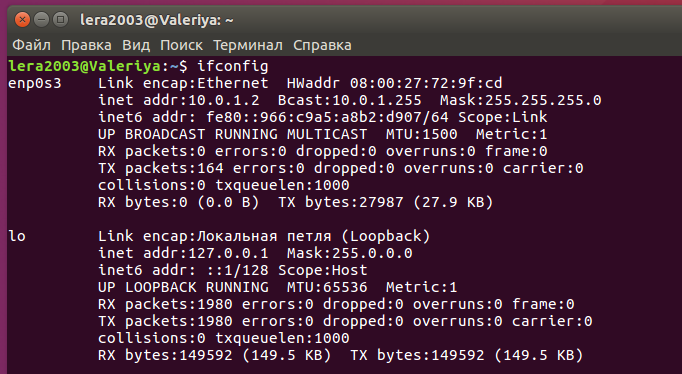


Рисунок 4 – ub1.

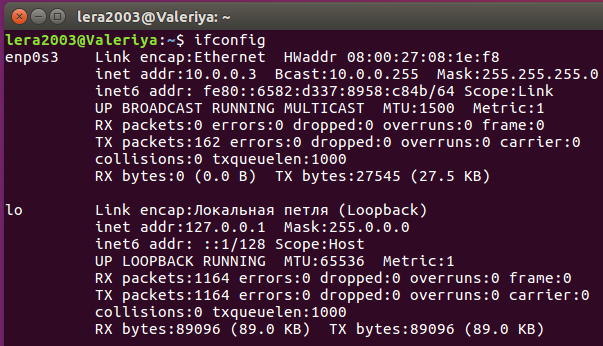


Рисунок 5 – ub2.

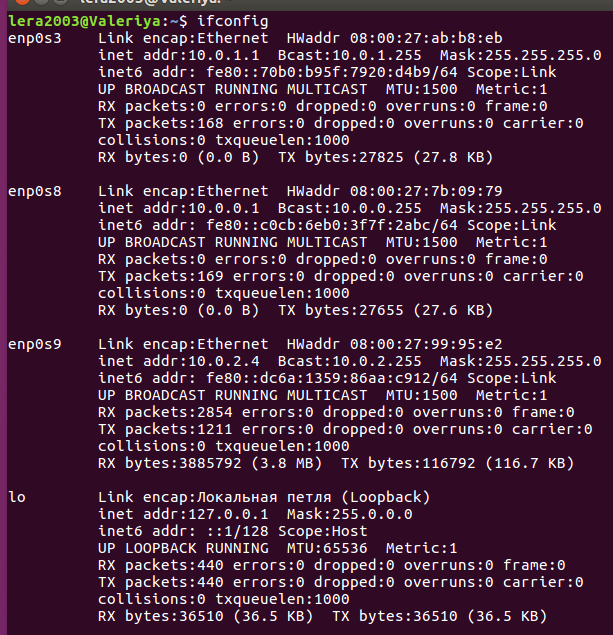


Рисунок 6 – ub-nat.

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:

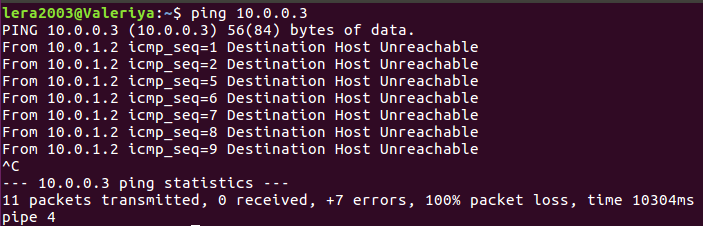


Рисунок 7 – проверка доступности с ub1 до ub2.

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

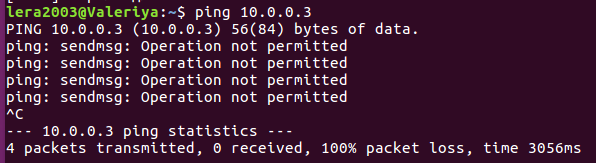


Рисунок 8 – проверка доступности с ub1 до ub2 после закрытия прямого доступа.

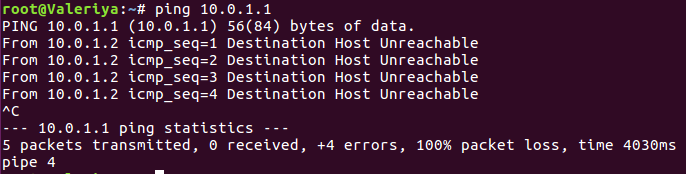


Рисунок 9 – проверка доступности c ub1 до ub-nat.

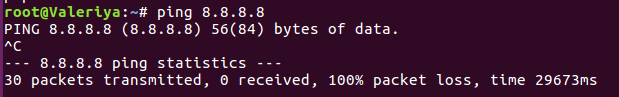


Рисунок 10 – проверка выхода в интернет с ub1.

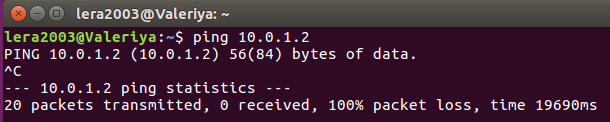


Рисунок 11 – проверка доступности с ub2 до ub1.

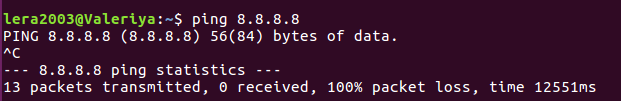


Рисунок 12 – проверка выхода в интернет с ub2.

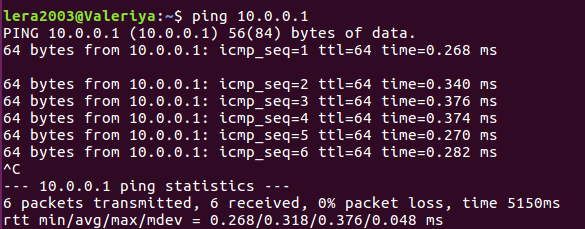


Рисунок 13 – проверка доступности c ub2 до ub-nat.

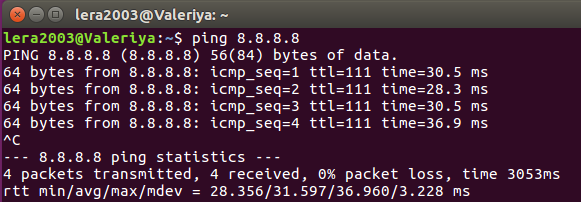
****

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

1. 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

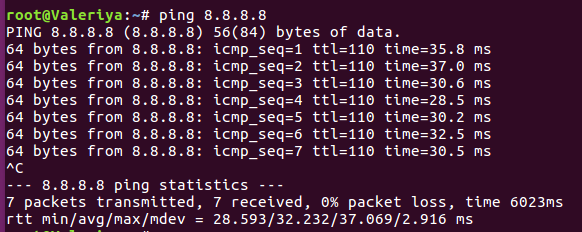


Рисунок 15 – проверка выхода в интернет с ub1.

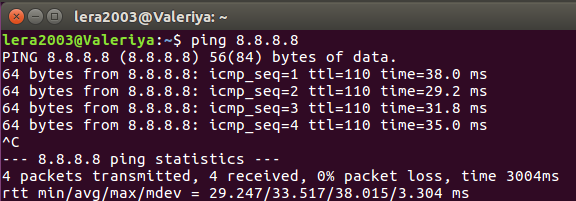


Рисунок 16 – проверка выхода в интернет с ub2.

1. 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.

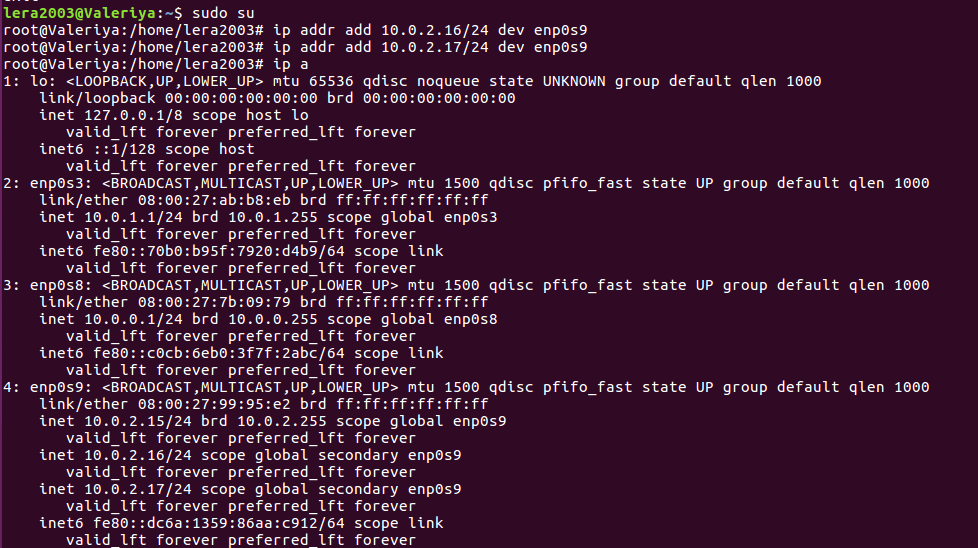


Рисунок 17 – добавление адресов на ub-nat.

Теперь настроим на узле маршрутизации sNAT:



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.

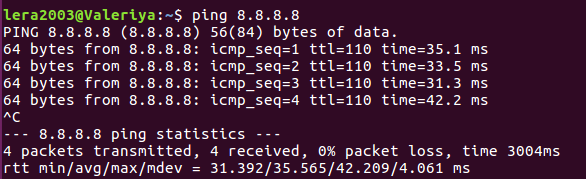


Рисунок 19 – проверка выхода в интернет с ub1.

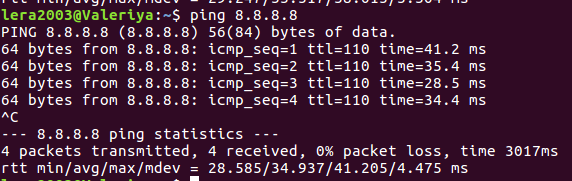


Рисунок 20 – проверка выхода в интернет с ub2.

1. 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.



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:

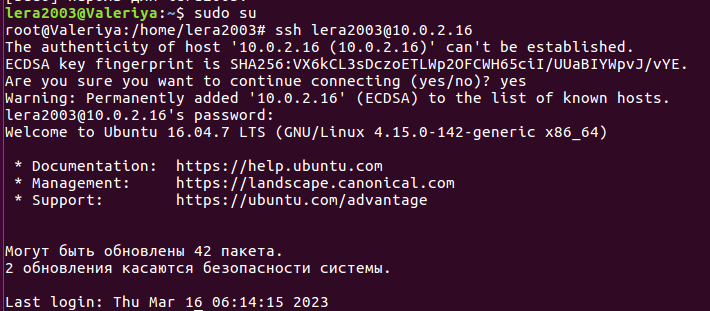


Рисунок 22 – подключение по ssh.

**Выводы.**

Входе 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).