**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 |  | Лойконен М.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 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 c 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 10.0.1.10, для ub2 – 10.0.0.5.

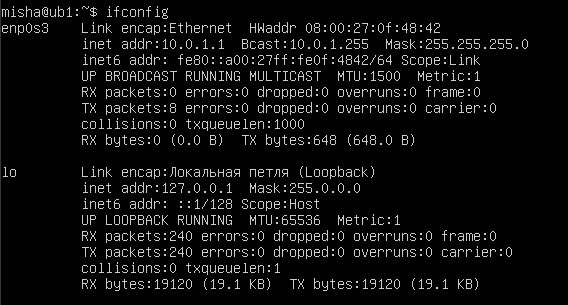


Рисунок 1 - Настройки ub1

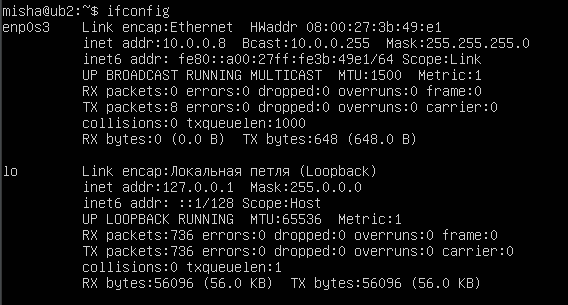


Рисунок 2 - Настройки ub2



Рисунок 3 - Настройки ub-nat

Далее запретим на ub2 доступ к ub1. Команда для этого действия представлена на рис. 4.

запрет доступа с ub2 на ub1.PNG

Рисунок 4 - Запрет доступа с ub2 на ub1

На рис. 5 представлен пинг с ub1 на ub2 до запрета доступа.

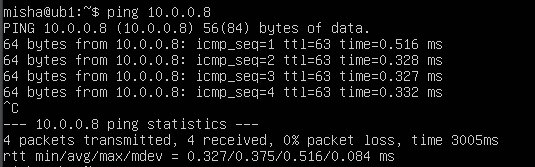


Рисунок 5 - Пинг с ub1 на ub2 до запрета доступа

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

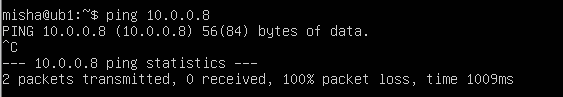


Рисунок 6 - Пинг с ub1 на ub2 после запрета доступа

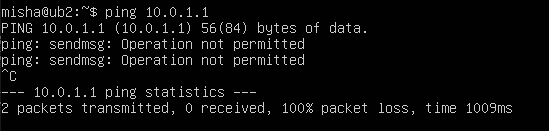


Рисунок 7 - Пинг с ub2 на ub1 после запрета доступа

На рисунках 8, 9 показано, что ub1 и ub2 не имеют доступ в интернет. На рисунках 10, 11 показано, что ub1 и ub2 имеют доступ к ub-nat, а на рисунке 12 изображен доступ ub-nat в интернет.

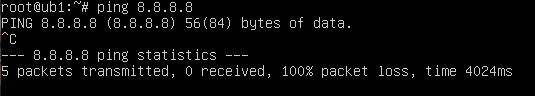


Рисунок 8 - Отсутствие доступа в интернет с ub1

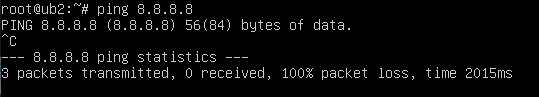


Рисунок 9 - Отсутствие доступа в интернет с ub2

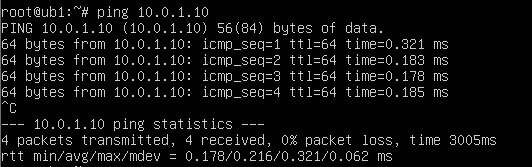


Рисунок 10 - Доступ с ub1 на ub-nat

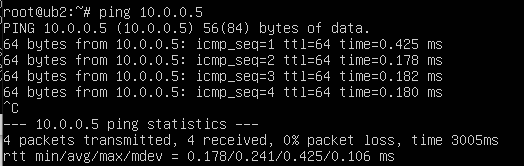


Рисунок 11 - Доступ с ub2 на ub-nat

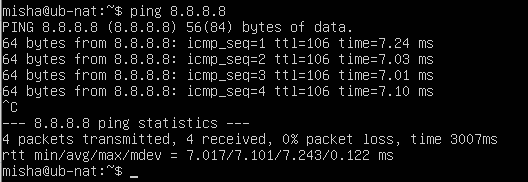


Рисунок 12 - Доступ в интернет с ub-nat

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

Настроим Masquerade на ub-nat с помощью команды, представленной на рис. 13.

команда для настройки маскарада.PNG

Рисунок 13 - Команда настройки Masquerade

На рисунках 14, 15 показано, что ub1 и ub2 теперь имеют доступ в интернет. А на рисунке 16 показано, что ub1 не имеет доступа к ub2.

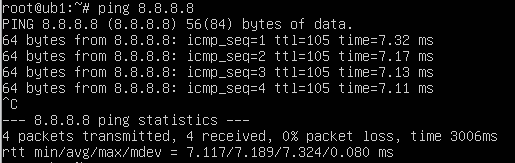


Рисунок 14 - Доступ в интернет с ub1 после настройки Masquerade

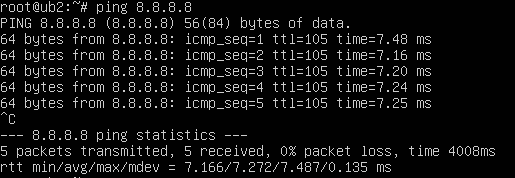


Рисунок 15 - Доступ в интернет с ub2 после настройки Masquerade

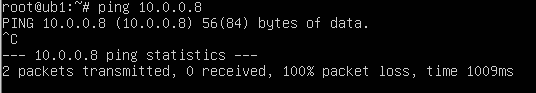


Рисунок 16 - Отсутствие доступа с ub1 на ub2 после настройки Masquerade

На рисунке 17 представлена работа Masquerade при пинге с ub2 в интернет.



Рисунок 17 - Работа Masquerade

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

Для настройки sNAT на ub-nat были добавлены 2 вторичных ip-адреса – 10.144.2.100/24 и 10.144.2.200/24. Их можно увидеть на рис. 18. Далее, с помощью команд, изображенных на рисунках 19 и 20, был настроен sNAT для ub1 и ub2 на ub-nat. На рисунках 21 и 22 показана работа sNAT при пинге с ub1 и ub2 в интернет. На рисунке 23 показано, что доступ с ub1 на ub2 все также отсутствует.



Рисунок 18 - Вторичные адреса на ub-nat

команда для добавления snat для ub1.PNG

Рисунок 19 - Команда настройки sNAT для ub1

команда для добавления snat для ub2.PNG

Рисунок 20 - Команда настройки sNAT для ub2

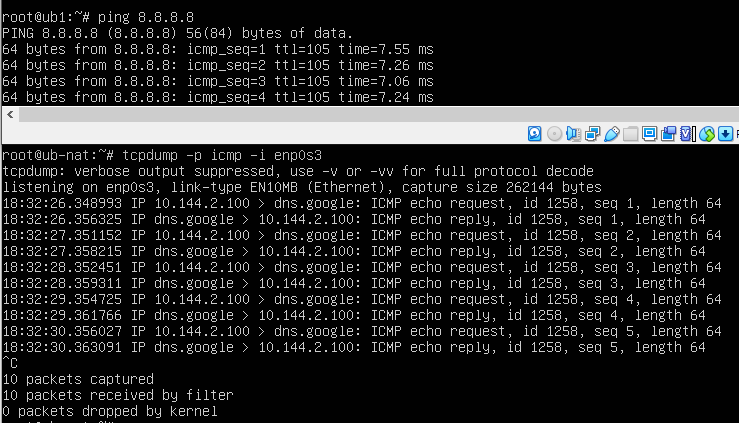


Рисунок 21 - Работа sNAT при пинге с ub1 в интернет

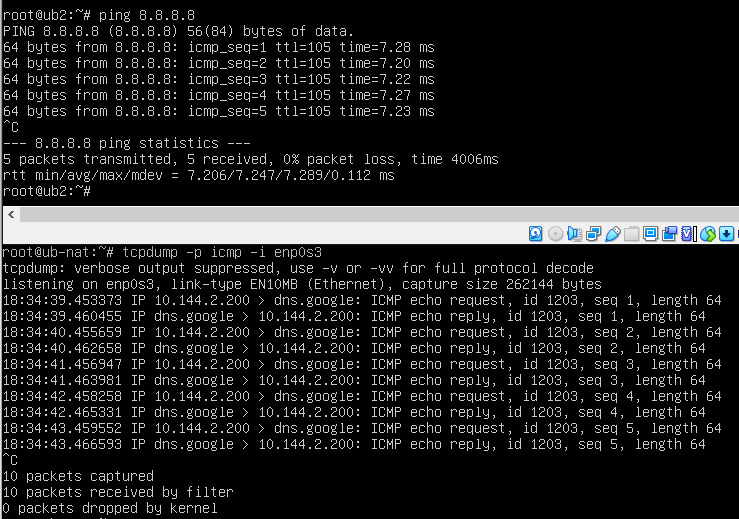


Рисунок 22 - Работа sNAT при пинге с ub2 в интернет

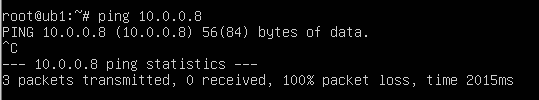


Рисунок 23 - Отсутствие доступа с ub1 на ub2 после настройки sNAT

1. *Настройка доступа с ub2 на ub1 с использованием dNAT.*

На рисунках 24 и 25 показаны команды для настройки dNAT для ub1 и ub2 на ub-nat.

команда настройки dnat.PNG

Рисунок 24 - Команда настройки dNAT для ub1

настройка dnat для ub2.PNG

Рисунок 25 - Команда настройки dNAT для ub2

На рисунке 26 показано подключение с ub2 на ub1 по ssh при помощи dNAT.

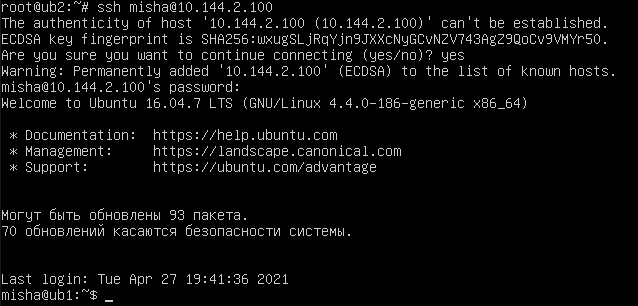


Рисунок 26 - Подключение с ub2 к ub1 по ssh

**Выводы.**

Были изучены механизмы преобразования сетевых адресов: NAT, Masquerade. Были созданы 3 виртуальные машины – ub1, ub2 и ub-nat. Ub-nat выступал в качестве маршрутизатора. На ub2 был запрещен доступ к ub1, чтобы создать условия, наиболее приближенные к реальным. Был настроен доступ в интернет с ub1 и ub2 сначала с помощью Masquerade, а затем с помощью NAT.