Министерство цифрового развития, связи и массовых коммуникаций
Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Сибирский государственный университет
телекоммуникаций и информатики»
(СибГУТИ)

Кафедра прикладной математики и кибернетики

Сети ЭВМ и телекоммуникации

Практическое задание №5
«Фильтрация пакетов и трансляция сетевых адресов»

Выполнил: Студент 2-го курса,
группы ИП-111
Гердележов Даниил Дмитриевич

Проверил преподаватель:
Крамаренко Константин Евгеньевич.

Новосибирск
2023

Выполнение работы:

1. Собрал конфигурацию сети, представленной на рисунке 1.

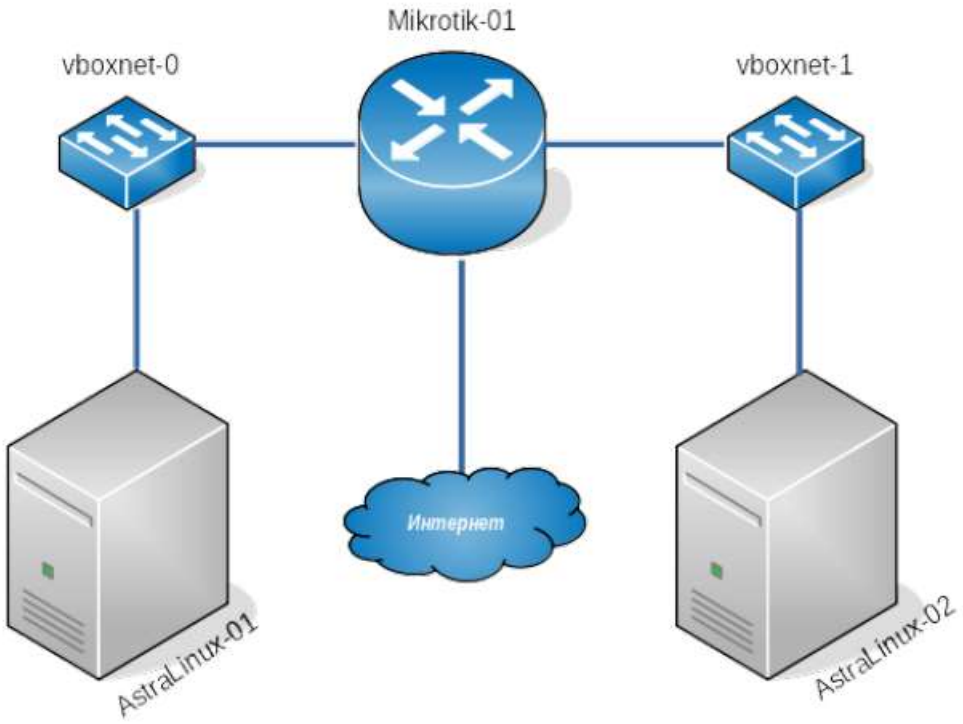
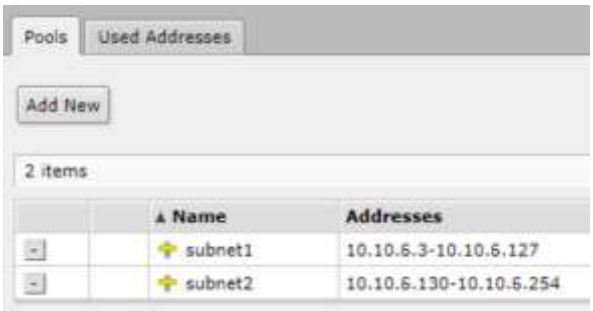


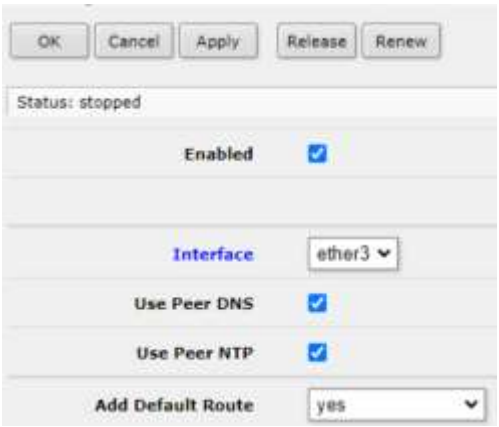
Рисунок 1 – Конфигурация сети для практического занятия

2. Сконфигурировал маршрутизатор mikrotik следующим образом: на интерфейсе, подключенном в режиме NAT настроил DHCP-клиент; на двух других интерфейсах настроил DHCP-сервера. В настройках DHCP серверов передаётся опция «маршрут по умолчанию».

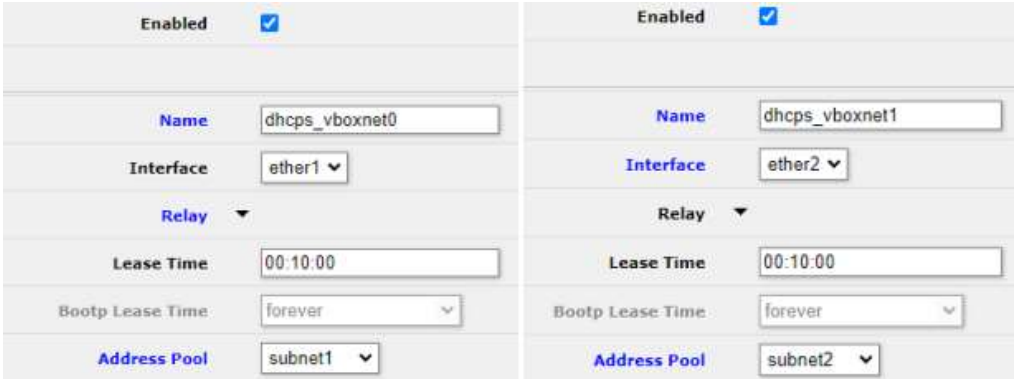
Список настроенных пулов подсетей:



Настроенный DHCP-клиент (ether3):

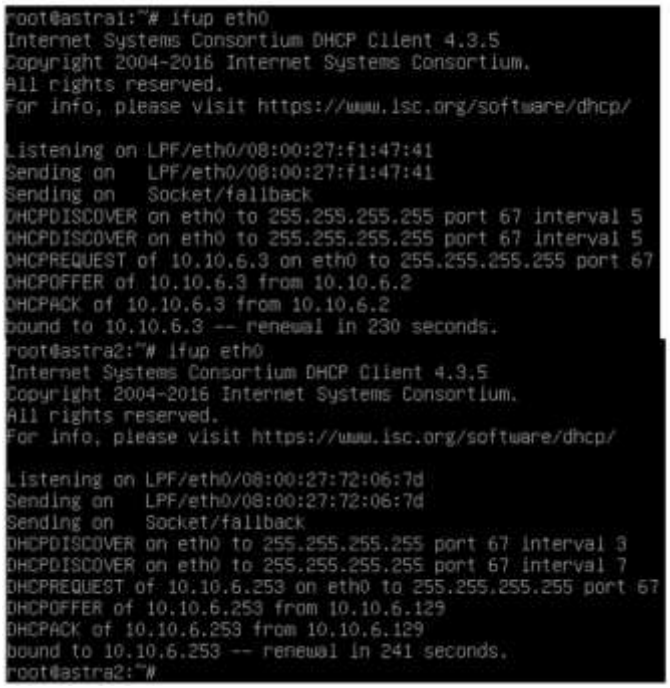


Настроенные DHCP-сервера для двух интерфейсов:



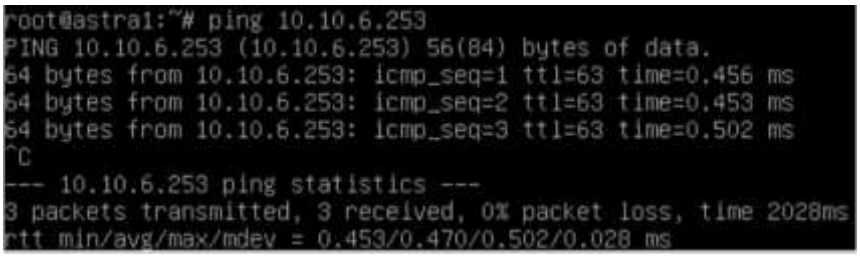
Настройка DHCP Network: для subnet1 (vboxnet0) маршрут по умолчанию - ether1 router1, для subnet2 (vboxnet1) - ether2 router1.

Проверил выдачу адресов машинам astra1 и astra2 от DHCP-серверов на router1:



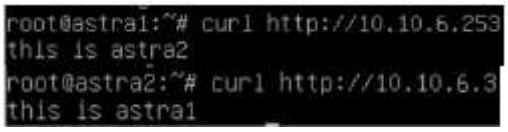
Адреса получены: 10.10.3.3 на astra1, 10.10.3.253 на astra2.

Попробую пинговать их между собой: успех.



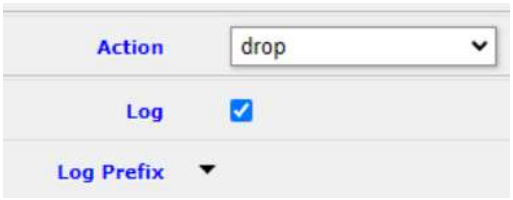
3. На узлах astralinux-01 и astralinux-02 задал соответствующие сетевые имена: для MikroTik-роутера командой **“system identity set name=...”**, для astra1 и astra2 - **“hostnamectl set-name …”**.
4. Переведя сетевые интерфейсы astra1, astra2 в режим NAT, были установлены пакеты curl и nginx-light командой “sudo apt-get install …”. Далее машины выключены и возвращены в изначальное состояние сетевых интерфейсов. Был изменён файл, по умолчанию отдаваемый nginx протоколом HTTP (/var/www/html/index.nginx-debian.html):

Попробую запросить содержимое этих файлов по протоколу HTTP с помощью curl: успех



Попробую подключиться к машинам по протоколу SSH: успех.

5. Настрою фильтрацию на MikroTik таким образом, чтобы с astra1 был запрещён доступ до astra2 по протоколу http, а с astra2 был запрещен доступ до astra1 по протоколу ssh: зайдём в меню WebFig -> IP -> Firewall и настрою новое правило фаервола MikroTik: указываем цепочку forward (пропуск пакета через устройство), адрес отправителя и получателя и протокол с портом назначения пакета. Для протокола HTTP это порт 80. Action - действие, выполняемое при попадании в наше правило, указано в drop (“скидывание” пакета). Дополнительно включен параметр Log, чтобы можно было посмотреть “скидывание” таких пакетов в логе. Создам ещё одно правило Firewall для пакетов по протоколу SSH от astra2 до astra1. Порт в данном случае - 22.



Попробую получить с astra1 http-информацию с astra2: ничего не выходит.

```
root@astra1:~# curl http://10.10.6.253
```

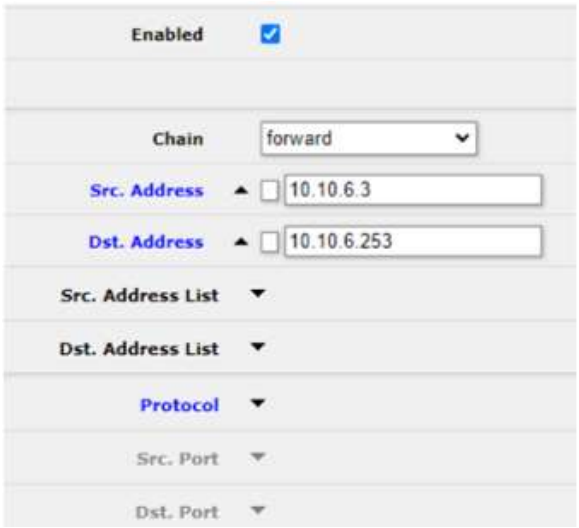
Попробую подключиться к astra1 с astra2: также ничего не выходит. Успех.

```
root@astra2:~# ssh owner@10.10.6.3
```

Посмотрим в MikroTik Log: действия firewall отчётливо видны.

29	Apr/08/2023 11:02:22	memory	system, info	filter rule changed by admin
30	Apr/08/2023 11:05:16	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
31	Apr/08/2023 11:05:17	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
32	Apr/08/2023 11:05:19	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
33	Apr/08/2023 11:05:22	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
34	Apr/08/2023 11:05:23	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
35	Apr/08/2023 11:05:26	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
36	Apr/08/2023 11:05:30	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
37	Apr/08/2023 11:05:38	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
38	Apr/08/2023 11:06:01	memory	system, info	filter rule added by admin
39	Apr/08/2023 11:06:01	memory	system, info	filter rule changed by admin
40	Apr/08/2023 11:06:07	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
41	Apr/08/2023 11:06:08	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
42	Apr/08/2023 11:06:12	memory	firewall, info	forward: in:ether2 out:ether1, connection-state:new src-mac 0
43	Apr/08/2023 11:06:13	memory	firewall, info	forward: in:ether2 out:ether1, connection-state:new src-mac 0

6. Для отклонения всех входящих пакетов (кроме HTTP) создаю 2 правила в Firewall: одно на отклонение всех входящих пакетов, а второе - на принятие (accept) только пакетов HTTP. При этом ставлю второе правило в списке выше первого, чтобы повысить его приоритет => => роутер при получении пакета HTTP выполнит для него самое приоритетное действие.



Список правил в MikroTik Firewall (по приоритету #):

3 items

		#	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Prot...	Src. Port	Dst. Port
- D		0	accept	forward	10.10.6.3	10.10.6.253			6 (tcp)		80
- D		1	drop	forward	10.10.6.3	10.10.6.253					

Проверяю: пингую astra2 с astra1 и пробую получить HTTP-информацию. Первое не выполняется (пакеты ping не доходят), второе выполняется успешно, информация доходит.

```
root@astra1:~# ping 10.10.6.253
PING 10.10.6.253 (10.10.6.253) 56(84) bytes of data.
^C
--- 10.10.6.253 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2041ms

root@astra1:~# curl http://10.10.6.253
this is astra2
```

58	Apr/08/2023 11:13:28	memory	system, info	filter rule moved by admin
59	Apr/08/2023 11:15:34	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
60	Apr/08/2023 11:15:35	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
61	Apr/08/2023 11:15:36	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
62	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 0
63	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src
64	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src
65	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src
66	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src
67	Apr/08/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src

7. Удалил все настройки фильтрации и трансляции адресов.
8. Убедился, что с узла astalinux-01 имеется доступ до узла astralinux-02 по протоколу http.

```
root@astra1:~# curl http://10.10.6.253
this is astra2
```

Удаляю “путь по умолчанию” на astra2: теперь получить HTTP-информацию невозможно, так как astra2 не знает, куда отправлять ответный пакет.

```
root@astra2:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.10.6.129     0.0.0.0         UG    0      0        0 eth0
10.10.6.128     0.0.0.0         255.255.255.128 U     0      0        0 eth0
root@astra2:~# route del default gw 10.10.3.129
root@astra2:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.6.128     0.0.0.0         255.255.255.128 U     0      0        0 eth0
root@astra2:~#
```

```
root@astra1:~# curl http://10.10.6.253
```

9. Настрою правила трансляции адресов (NAT) таким образом, чтобы весь трафик, уходящий с router1 в сеть, где располагается astra2, имел адрес отправителя router1. Для этого в Firewall создам новое правило вкладки NAT: используя цепочку src-nat (пакеты, которые будут отправляться от имени нашего роутера), в адресе отправителя укажем адрес astra1, в поле “To Addresses” - бывший адрес “маршрута по умолчанию” получателя. Таким образом, astra2 будет считать, что пакет приходит от router1 (к которому есть прямое подключение) и отвечать также на него.

Убедился, что появился доступ с astra1 до astra2 по протоколу HTTP.

```
root@astra1:~# curl http://10.10.6.253
this is astra2
```

77	Apr/08/2023 11:25:47	memory	system, info	nat rule added by admin
78	Apr/08/2023 11:25:47	memory	system, info	nat rule changed by admin
79	Apr/08/2023 11:33:25	memory	firewall, info	srcnat: in:ether1 out:ether2, connection-state:new src-mac 08:

Посмотрел пакеты через Wireshark:

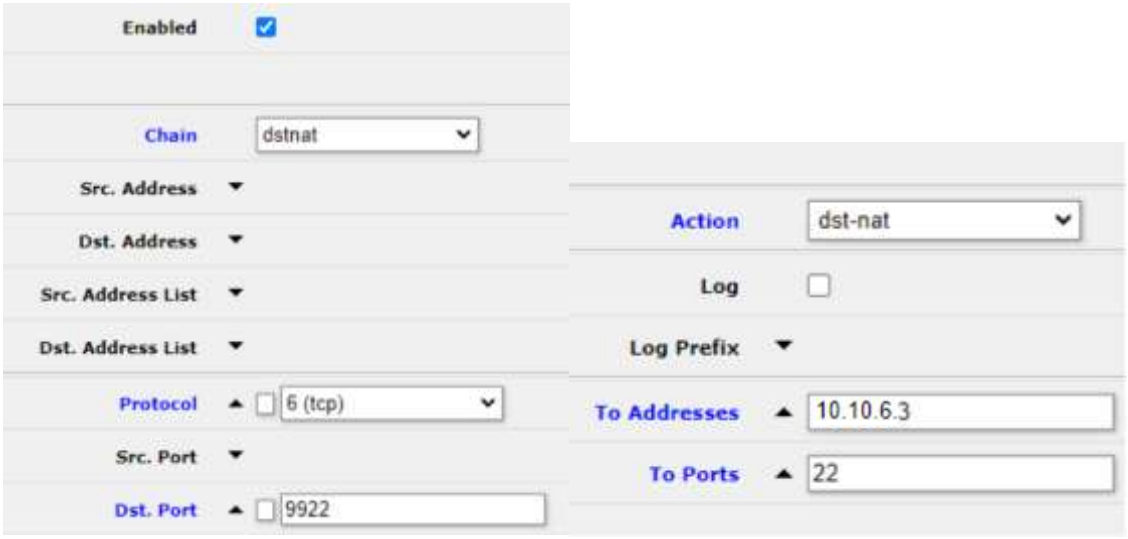
router1 ether1

27125	17227.576894	10.10.6.3	10.10.6.253	HTTP	141 GET / HTTP/1.1
27127	17227.577333	10.10.6.253	10.10.6.3	HTTP	316 HTTP/1.1 200 OK (text/html)

router1 ether2: IP-адрес astra1 заменён на Out. Address, указанный в router1, для astra2.

18837	17227.577008	10.10.6.129	10.10.6.253	HTTP	141 GET / HTTP/1.1
18839	17227.577280	10.10.6.253	10.10.6.129	HTTP	316 HTTP/1.1 200 OK (text/html)

10. Настрою правила трансляции адресов (NAT) таким образом, чтобы при соединении к маршрутизатору MikroTik по протоколу TCP с портом назначения 9922 трафик 11 перенаправлялся на узел astra1 на порт SSH (22). Создам новое правило с цепочкой dst-nat, протоколом TCP и портом 9922, куда будут приходить нужные пакеты. В поле Action указываем dst-nat и перенаправляем наши пакеты на адрес 10.10.3.3, порт 22 (SSH).



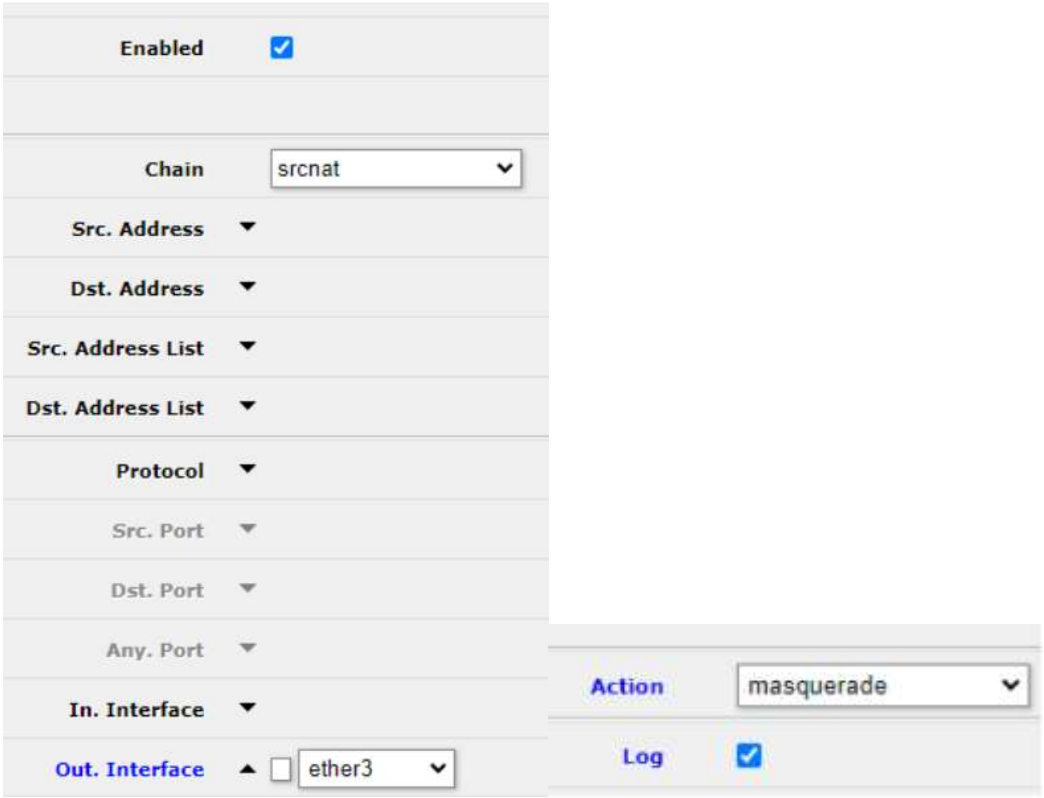
Проверяем: используя команду “ssh”, подключаемся с astra2 к router1 по протоколу TCP (так как SSH использует TCP, дополнительных манипуляций не требуется) и порту 9922.

```
owner@astra2:~$ ssh -p 9922 owner@10.10.6.2
The authenticity of host '[10.10.6.2]:9922 ([10.10.6.2]:9922)' can't be established.
ECDSA key fingerprint is SHA256:zKXHD+3NXKH+cppRy2izr7M1AinIQtfCQn1rS9E3uag.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.6.2]:9922' (ECDSA) to the list of known hosts.
owner@10.10.6.2's password:
You have new mail.
Last login: Sat Apr  8 20:00:33 2023 from 10.10.6.129
owner@astra1:~$ _
```

Отключил добавленные ранее правила Firewall -> NAT, так как они более нам не понадобятся.

11. На router1 настроил правила трансляции адресов (NAT) таким образом, чтобы astra1 получил возможность выхода в сеть Интернет.

    Добавлю новое правило Firewall -> NAT с цепочкой src-nat на выходном интерфейсе ether3 (который подключен к NAT - внешнему Интернету). В Action указываю masquerade, который работает точно так же, как src-nat, но в нём не требуется указывать адрес интерфейса, через который далее пакет пойдёт в сеть (это производится маршрутизатором автоматически - он смотрит адрес на ether3 и указывает его в качестве Out. Address).

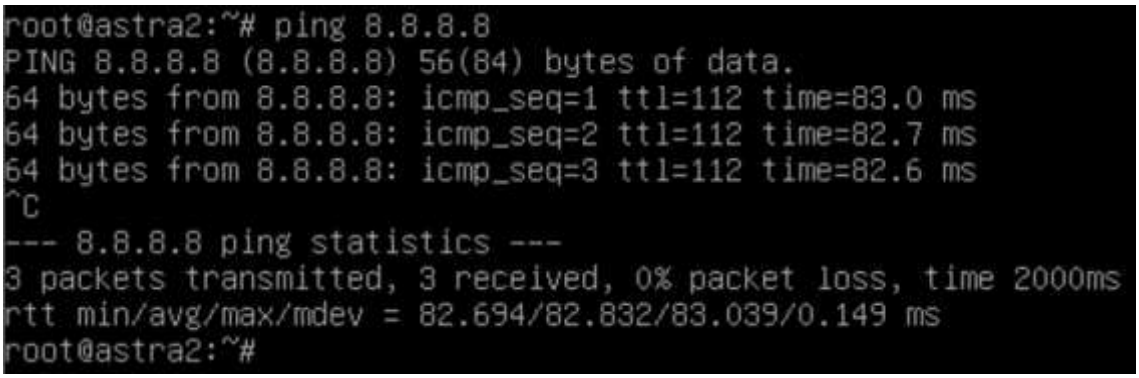


    Проверяю выход astra1 в Интернет пингом адреса 8.8.8.8: успех.

```
root@astra1:~# 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=112 time=82.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=82.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=82.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=82.9 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 82.735/82.797/82.906/0.213 ms
root@astra1:~#
```

    Изменю конфигурацию сети таким образом, чтобы astra2 также получил доступ в сеть Интернет. Для этого необходимо восстановить “маршрут по умолчанию” в

таблице маршрутизации astra2. Чтобы не вводить его вручную, перезапустил интерфейс eth0 на astra2 и DHCP-сервер сам выдаст его.



Все задания выполнены.