

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ
КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

КАФЕДРА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

ПРАКТИЧЕСКАЯ РАБОТА №5

по дисциплине «Сети ЭВМ и телекоммуникации»

Тема: «Фильтрация пакетов и трансляция сетевых адресов»

Выполнил: студент группы ИС-142

Наумов А.А.

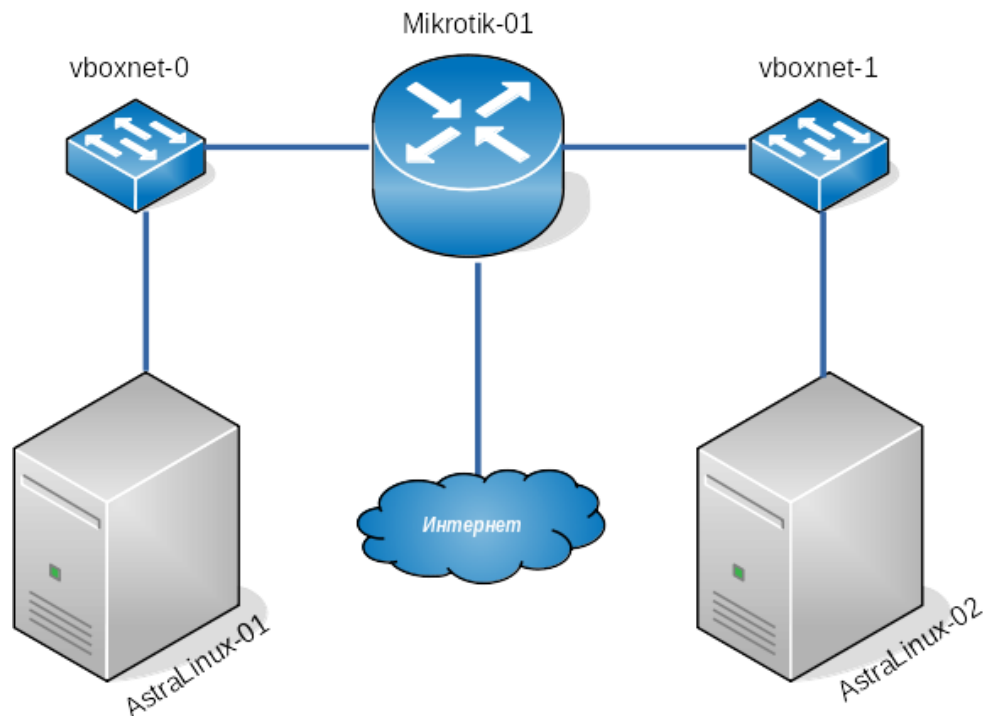
Проверил: доцент

кафедры ВС Перышкова Е.Н.

Новосибирск 2023

Задание

- 1 Собрать конфигурацию сети, представленную на рисунке (Интернет-подключение VirtualBox NAT).

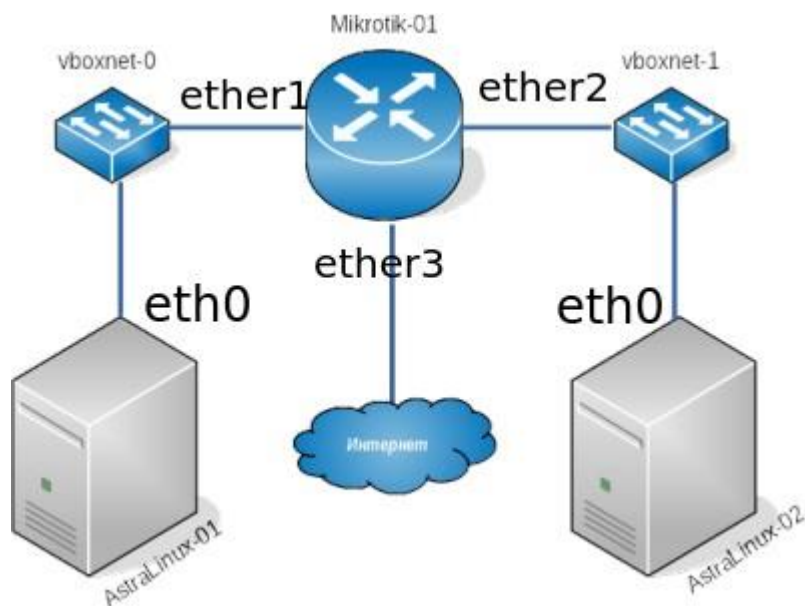


- 2 Сконфигурировать Mikrotik следующим образом: на интерфейсе, подключенном в режиме NAT должен быть настроен DHCP-клиент; на двух других интерфейсах должны быть настроены DHCP-сервера. Для выполнения практического задания выделен диапазон IPv4 адресов: 10.10.N.0/24, где N – номер в журнале. В настройках DHCP серверов должна передаваться опция "маршрут по умолчанию".
- 3 На узлах astra-01 и astra-02 задать соответствующие сетевые имена.
- 4 На узлах astra-01 и astra-02 установить curl и nginx-light. Изменить содержимое файла, отдаваемого nginx по HTTP так, чтобы в нем содержалось имя соответствующего узла. На каждом узле astra с помощью curl запросить файл по умолчанию с другого узла astra. На каждом узле astra получить доступ по SSH к другому узлу astra.
- 5 На маршрутизаторе Mikrotik настроить правила фильтрации так, чтобы с astra-01 было запрещён доступ до astra-02 по протоколу HTTP, а с узла astra-02 был запрещен доступ до узла astra-01 по протоколу SSH.
- 6 Изменить настройки фильтрации на маршрутизаторе Mikrotik так, чтобы с узла astra-01 был доступ до узла astra-02 только по протоколу HTTP.
- 7 Удалить все настройки фильтрации и трансляции адресов.

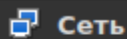
- 8 Убедиться, что с узла astra-01 имеется доступ до узла astra-02 по протоколу HTTP. Удалить на узле astra-02 маршрут "по умолчанию".
- 9 Настроить правила трансляции адресов таким образом, чтобы весь трафик, уходящий с узла Mikrotik в сеть, где располагается astra-02 имел адрес отправителя Mikrotik. Убедиться, что появился доступ с узла astra-01 до узла astra-02 по протоколу HTTP.
- 10 Настроить правила трансляции адресов таким образом, чтобы при соединении к маршрутизатору Mikrotik по протоколу TCP с портом назначения 9922 трафик перенаправлялся на узел astra-01 на порт SSH.
- 11 На узле Mikrotik настроить правила трансляции адресов таким образом, чтобы узел astra-01 получил возможность выхода в сеть Интернет (проверка пингом до 8.8.8.8). Изменить конфигурацию сети таким образом, чтобы astra-02 также получил доступ в сеть Интернет.

Выполнение работы

1. После сброса настроек на mt-01, astra-01, astra-02 конфигурация сети стала выглядеть так:



mt-01:



Сеть

Адаптер 1: Intel PRO/1000 MT Desktop (Виртуальный адаптер хоста, 'vboxnet0')
Адаптер 2: Intel PRO/1000 MT Desktop (Виртуальный адаптер хоста, 'vboxnet1')
Адаптер 3: Intel PRO/1000 MT Desktop (NAT)

2. Выделен диапазон адресов 10.10.10.0/24. Чтобы разделить его на 2 подсети, фиксирую дополнительно 1 бит, таким образом пул **допустимых** адресов для узлов:

vboxnet0: 10.10.10.1 - 10.10.10.126

vboxnet1: 10.10.10.129 -

10.10.10.254

Маска: 255.255.255.128 или /25

```
VBxManage hostonlyif ipconfig vboxnet0 --ip=10.10.10.1 -  
-netmask=255.255.255.128
```

```
VBxManage hostonlyif ipconfig vboxnet1 --ip=10.10.10.129 -  
-netmask=255.255.255.128
```

На Mikrotik назначил статические адреса 10.10.10.2/25 и 10.10.10.129/25 для vboxnet0 и vboxnet1 соответственно.

Настройки роутера:

DHCP

Networks

Leases

Options

Option Sets

Option Matcher

Alerts

Add New

DHCP Config

DHCP Setup

2 items

		<div>▲ Name</div>	Interface	Relay	Lease Time	Address Pool	Add ARP For Leases	
<div>-</div>	<div>D</div>	server1	ether1		00:10:00	subnet1	no	
<div>-</div>	<div>D</div>	server2	ether2		00:10:00	subnet2	no	

DHCP

Networks

Leases

Options

Option Sets

Option Matcher

Alerts

Add New

2 items

		▲ Address	Gateway	DNS Servers	Domain	WINS Servers	Next Server	
-		10.10.10.0/25	10.10.10.2					
-		10.10.10.128/25	10.10.10.130					

Пулы подсетей:

Pools

Used Addresses

Add New

2 items

		<div>▲ Name</div>	Addresses	Next Pool	
<div>-</div>		<div><div></div>subnet1</div>	10.10.10.3-10.10.10.127	none	
<div>-</div>		<div><div></div>subnet2</div>	10.10.10.131-10.10.10.254	none	

```

root@astra:~# ifdown eth1
ifdown: unknown interface eth1
root@astra:~# ifup eth0
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:68:cb:e0
Sending on   LPF/eth0/08:00:27:68:cb:e0
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPREQUEST of 10.10.10.127 on eth0 to 255.255.255.255 port 67
DHCPOFFER of 10.10.10.127 from 10.10.10.2
DHCPACK of 10.10.10.127 from 10.10.10.2
bound to 10.10.10.127 -- renewal in 288 seconds.
root@astra:~#

owner@astra2:~$ sudo ifdown eth0
[sudo] пароль для owner:
Killed old client process
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:7b:6e:34
Sending on   LPF/eth0/08:00:27:7b:6e:34
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 10.10.10.130 port 67
owner@astra2:~$ sudo ifup eth0
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:7b:6e:34
Sending on   LPF/eth0/08:00:27:7b:6e:34
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPREQUEST of 10.10.10.254 on eth0 to 255.255.255.255 port 67
DHCPOFFER of 10.10.10.254 from 10.10.10.130
DHCPACK of 10.10.10.254 from 10.10.10.130
bound to 10.10.10.254 -- renewal in 256 seconds.
owner@astra2:~$

```

Машины astra пингуются между собой, значит настройка выполнена верно.

3.Имя первой астры уже настроено, задам для второй:

Sudo hostnamectl set-hostname astra2

для MikroTik-роутера командой :

system identity set name=...

Также меняю имя в/etc/hosts.

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**):

```
root@astra1:~# cat /var/www/html/index.nginx-debian.html
this is astra1
root@astra2:~# cat /var/www/html/index.nginx-debian.html
this is astra2
```

Попробуем запросить содержимое этих файлов по протоколу HTTP с помощью curl:

```
root@astra1:~# curl http://10.10.10.253
this is astra2
root@astra2:~# curl http://10.10.10.3
this is astra1
```

Попробуем подключиться к машинам по протоколу SSH:

```
root@astra2:~# ssh owner@10.10.10.3
owner@10.10.10.3's password:
You have new mail.
Last login: Sat Apr  8 13:48:53 2023
owner@astra1:~$

root@astra1:~# ssh owner@10.10.10.253
owner@10.10.10.253's password:
You have new mail.
Last login: Sat Apr  8 14:53:46 2023 from 10.10.10.3
owner@astra2:~$
```

5. Настроим 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 настроим 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. Создаём ещё одно правило Firewall для пакетов по протоколу SSH от astra2 до astra1. Порт в данном случае - 22.

Enabled ☒

Chain

Src. Address

Dst. Address

Src. Address List

Dst. Address List

Protocol

Src. Port

Dst. Port

Enabled ☒

Chain

Src. Address

Dst. Address

Src. Address List

Dst. Address List

Protocol

Src. Port

Dst. Port

Action

Log ☒

Log Prefix

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

```
root@astra1:~# curl http://10.10.10.253
```

Пробуем подключиться к astra1 с astra2: также ничего не выходит.

```
root@astra2:~# ssh owner@10.10.10.3
```

Смотрим в MikroTik Log: действия firewall (дропы пакетов) отчётливо видны.

29	Apr/18/2023 11:02:22	memory	system, info	filter rule changed by admin
30	Apr/18/2023 11:05:16	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
31	Apr/18/2023 11:05:17	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
32	Apr/18/2023 11:05:19	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
33	Apr/18/2023 11:05:22	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
34	Apr/18/2023 11:05:23	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
35	Apr/18/2023 11:05:26	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
36	Apr/18/2023 11:05:30	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
37	Apr/18/2023 11:05:38	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
38	Apr/18/2023 11:06:01	memory	system, info	filter rule added by admin
39	Apr/18/2023 11:06:01	memory	system, info	filter rule changed by admin
40	Apr/18/2023 11:06:07	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
41	Apr/18/2023 11:06:08	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00

6. Для отклонения всех входящих пакетов (кроме HTTP) создаю 2 правила в Firewall: одно на отклонение всех входящих пакетов, а второе - на принятие (ассепт) 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.

Enabled ☒

Chain

Src. Address

Dst. Address

Src. Address List

Dst. Address List

Protocol

Src. Port

Dst. Port

Action

Log ☒

Log Prefix

Enabled ☒

Chain

Src. Address

Dst. Address

Src. Address List

Dst. Address List

Protocol

Src. Port

Dst. Port

Action

Log ☒

Log Prefix

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	
<input type="checkbox"/> D	0	accept	forward	10.10.10.3	10.10.10.253			6 (tcp)		80	
<input type="checkbox"/> D	1	drop	forward	10.10.10.3	10.10.10.253						

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 10.10.10.253
PING 10.10.10.253 (10.10.10.253) 56(84) bytes of data.
^C
--- 10.10.10.253 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2041ms

root@astra1:~# curl http://10.10.10.253
this is astra2
```


58	Apr/18/2023 11:13:28	memory	system, info	filter rule moved by admin
59	Apr/18/2023 11:15:34	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
60	Apr/18/2023 11:15:35	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
61	Apr/18/2023 11:15:36	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
62	Apr/18/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:new src-mac 08:00:27:00:00:00
63	Apr/18/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src-mac 08:00:27:00:00:00
64	Apr/18/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src-mac 08:00:27:00:00:00
65	Apr/18/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src-mac 08:00:27:00:00:00
66	Apr/18/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src-mac 08:00:27:00:00:00
67	Apr/18/2023 11:15:39	memory	firewall, info	forward: in:ether1 out:ether2, connection-state:established src-mac 08:00:27:00:00:00

7. Удаляю все правила фильтрации пакетов, в дальнейшем они не понадобятся.

8. С astra1 до astra2 по прежнему можно получить HTTP-информацию используя curl.

```
root@astra1:~# curl http://10.10.10.253
this is astra2
```

Удаляем "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          10.10.10.129   0.0.0.0         UG      0      0      0 eth0
10.10.10.128     0.0.0.0        255.255.255.128 U        0      0      0 eth0
root@astra2:~# route del default gw 10.10.10.129
root@astra2:~# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.10.128     0.0.0.0        255.255.255.128 U        0      0      0 eth0
root@astra2:~#
```

```
root@astra1:~# curl http://10.10.10.253
```

9. Настроим 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 создадим новое правило вкладки NAT: используя цепочку src-nat (пакеты, которые будут отправляться от имени нашего роутера), в адресе отправителя укажем адреса 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.

Enabled <input checked="" type="checkbox"/>	Action <input type="text" value="src-nat"/>
Chain <input type="text" value="srcnat"/>	Log <input checked="" type="checkbox"/>
Src. Address <input type="text" value="10.10.10.3"/>	Log Prefix <input type="text" value=""/>
	To Addresses <input type="text" value="10.10.10.129"/>

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

```

root@astra1:~# curl http://10.10.10.253
^C
root@astra1:~# curl http://10.10.10.253
this is astra2

```

77	Apr/18/2023 11:25:47	memory	system, info	nat rule added by admin
78	Apr/18/2023 11:25:47	memory	system, info	nat rule changed by admin
79	Apr/18/2023 11:33:25	memory	firewall, info	srcnat: in:ether1 out:ether2, connection-state:new src-mac 08:

Посмотрим пакеты через Wireshark:
router1 ether1

27125	17227.576894	10.10.10.3	10.10.10.253	HTTP	141 GET / HTTP/1.1
27127	17227.577333	10.10.10.253	10.10.10.3	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	10.10.10.129	10.10.10.253	HTTP	141 GET / HTTP/1.1
18839	17227.577280	10.10.10.253	10.10.10.129	HTTP	316 HTTP/1.1 200 OK (text/html)

10. Настроим правила трансляции адресов (NAT) таким образом, чтобы при соединении к маршрутизатору MikroTik по протоколу TCP с портом назначения 9922 трафик перенаправлялся на узел astra1 на порт SSH (22). Создаём 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).

Enabled <input checked="" type="checkbox"/>	
Chain	dstnat
Src. Address	
Dst. Address	
Src. Address List	
Dst. Address List	
Protocol	6 (tcp)
Src. Port	
Dst. Port	9922
Action	dst-nat
Log	<input type="checkbox"/>
Log Prefix	
To Addresses	10.10.10.3
To Ports	22

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

```

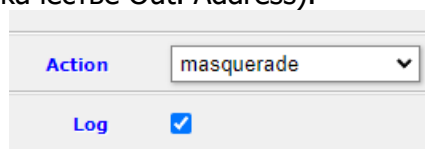
owner@astra2:~$ ssh -p 9922 owner@10.10.10.2
The authenticity of host '[10.10.10.2]:9922 ([10.10.10.2]:9922)' can't be established.
ECDSA key fingerprint is SHA256:zKXHD+3NXXKH+cppRy2izr7M1AinIQtfCQn1rS9E3uag.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.10.2]:9922' (ECDSA) to the list of known hosts.
owner@10.10.10.2's password:
You have new mail.
Last login: Sat Apr  8 20:00:33 2023 from 10.10.10.129
owner@astra1:~$ _

```

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

Enabled <input checked="" type="checkbox"/>	
Chain	srcnat
Src. Address	
Dst. Address	
Src. Address List	

11. На router1 настроим правила трансляции адресов (NAT) таким образом, чтобы astra1 получил возможность выхода в сеть Интернет. Добавим новое правило Firewall -> NAT с цепочкой src-nat на выходном интерфейсе ether3 (который подключен к NAT - внешнему Интернету). В Action укажем 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).



Action	masquerade
Log	<input checked="" type="checkbox"/>

Проверим 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:~#
```

Изменим 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, перезапустим интерфейс eth0 на astra2 и DHCP-сервер сам выдаст его.

```
root@astra2:~# 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=83.0 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=82.6 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 82.694/82.832/83.039/0.149 ms
root@astra2:~#
```

Все задания практической работы выполнены успешно.

