

Университет ИТМО
Факультет программной инженерии и компьютерной
техники

Сети ЭВМ и телекоммуникации

Учебно-исследовательская работа №4

Основы администрирования маршрутизируемых
компьютерных сетей

Лабушев Тимофей

Группа Р3302

Санкт-Петербург

2020

Цель

Изучение основных методов настройки маршрутизируемых компьютерных сетей на примере сети, состоящей из компьютеров под управлением ОС Linux.

Задание

В процессе выполнения работы изучается сетевой уровень модели OSI. Производится базовая настройка связности в сети, управление таблицами маршрутизации и правилами трансляции сетевых адресов. При помощи утилиты `tcpdump` выполняются наблюдения за передачей трафика по каналам связи в маршрутизируемой компьютерной сети. Применение утилиты `tcpdump` позволяет непосредственно в терминале (это основной метод управления сетевым оборудованием) наблюдать проходящие через интерфейсы компьютера пакеты и изучить их внутреннюю структуру.

Исходные данные

Вариант выполнения работы $V1 = 1 + (14 \bmod 5) = 5$.

Для общей и вариативной части задания используется следующая топология сети:

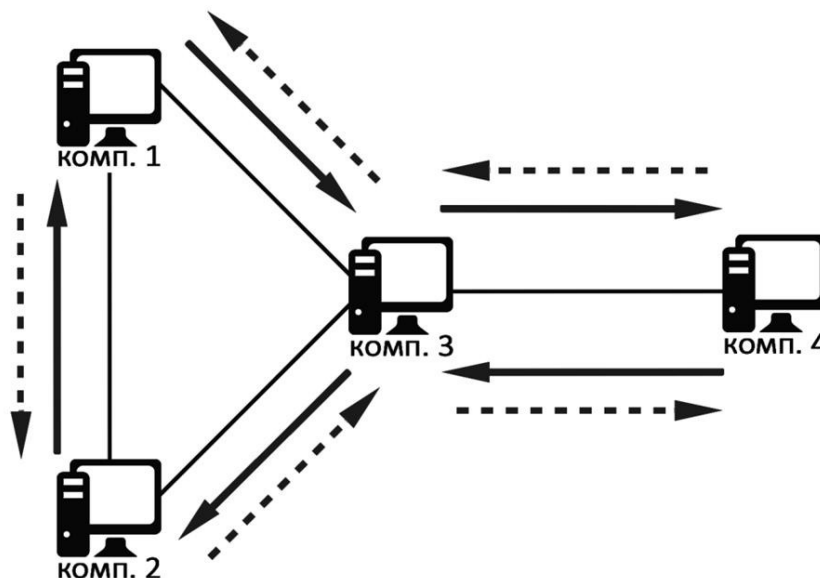


Рис. 1. Топология сети и схема прохождения трафика для варианта 5

Ход работы

Настройка сети

Настроим IPv4 адреса компьютеров А.В.Х.У/М в топологии следующим образом:

- А равно количеству букв в имени студента (7)
- В равно количеству букв в фамилии студента (7)
- Х и У выбирается случайно
- М принимается равной 30, максимальному значению для обеспечения связи двух компьютеров (два адреса из четырех возможных — минимальный и максимальный — зарезервированы)

Назначим следующие адреса подсетей:

- 7.7.12.0/30 для связи компьютеров 1 и 3 (сетевой адаптер s1_s2 в VirtualBox)
- 7.7.13.0/30 для связи компьютеров 1 и 3 (сетевой адаптер s1_s3 в VirtualBox)
- 7.7.23.0/30 для связи компьютеров 2 и 3 (сетевой адаптер s2_s3 в VirtualBox)
- 7.7.34.0/30 для связи компьютеров 3 и 4 (сетевой адаптер s3_s4 в VirtualBox)

Для IPv6 адресов назначим маску /127 (2 адреса) и следующие адреса подсетей:

- fc00::7.7.12.0/127 (fc00:0:0:0:0:0:707:c00/127) для s1_s2
- fc00::7.7.13.0/127 для s1_s3
- fc00::7.7.23.0/127 для s2_s3
- fc00::7.7.34.0/127 для s3_s4

Настройка компьютера s1:

```
ip link set eth0 up
ip link set eth1 up

ip a add 7.7.12.1/30 dev eth0
ip a add 7.7.13.1/30 dev eth1
ip -6 a add fc00::7.7.12.0/127 dev eth0
ip -6 a add fc00::7.7.13.0/127 dev eth1

ip ro add 7.7.34.2 via 7.7.13.2
ip -6 ro add fc00::7.7.34.1 via fc00::7.7.13.1
```

Настройка компьютера s2:

```
ip link set eth0 up
ip link set eth1 up
```

```
ip a add 7.7.12.2/30 dev eth0
ip a add 7.7.23.1/30 dev eth1
ip -6 a add fc00::7.7.12.1/127 dev eth0
ip -6 a add fc00::7.7.23.0/127 dev eth1

ip ro add 7.7.34.2 via 7.7.23.2
```

Настройка компьютера s3:

```
ip link set eth0 up
ip link set eth1 up
ip link set eth2 up

ip a add 7.7.13.2/30 dev eth0
ip a add 7.7.23.2/30 dev eth1
ip a add 7.7.34.1/30 dev eth2
ip -6 a add fc00::7.7.13.1/127 dev eth0
ip -6 a add fc00::7.7.23.1/127 dev eth1
ip -6 a add fc00::7.7.34.0/127 dev eth2

sysctl -w net.ipv4.ip_forward=1
sysctl -w net.ipv4.conf.all.rp_filter=0
```

Настройка компьютера s4:

```
ip link set eth0 up

ip a add 7.7.34.2/30 dev eth0
ip -6 a add fc00::7.7.34.1/127 dev eth0

ip ro add 7.7.13.1 via 7.7.34.1
ip ro add 7.7.23.1 via 7.7.34.1
```

Проверка работоспособности

Для проверки сети возьмем компьютеры #1 и #4, трафик между которыми проходит через шлюз, которым выступает компьютер #3.

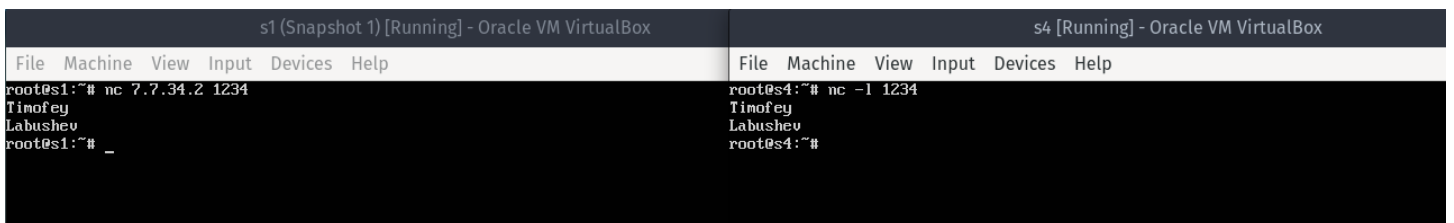


Рис. 2. Вывод утилиты nc

Настройка межсетевого экрана

1. Запретить передачу только тех пакетов, которые отправлены на TCP-порт, заданный в настройках утилиты nc.

Для порта 1234 на компьютере, который отправляет пакеты, создадим следующее правило:

```
iptables -A OUTPUT -p tcp --dport 1234 -j DROP
```

По умолчанию правило помещается в таблицу filter.

Для проверки запустим nc с ключами -z (проверка соединения без отправки данных) и -w 1 (ограничение времени на установку соединения):

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox	s4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help	File Machine View Input Devices Help
<pre>root@s1:~# nc -z -w 1 -v 7.7.34.2 1234 Connection to 7.7.34.2 1234 port [tcp/*] succeeded! root@s1:~# iptables -A OUTPUT -p tcp --dport 1234 -j DROP root@s1:~# nc -z -w 1 -v 7.7.34.2 1234 nc: connect to 7.7.34.2 port 1234 (tcp) timed out: Operation now in progress root@s1:~# nc -z -w 1 -v -u 7.7.34.2 1234 Connection to 7.7.34.2 1234 port [udp/*] succeeded! root@s1:~# _</pre>	<pre>root@s4:~# nc -l -k 1234 & [1] 1365 root@s4:~# nc -l -k -u 1234 & [2] 1366 root@s4:~# XXX</pre>

Рис. 3. Демонстрация работы правила №1

2. Запретить приём только тех пакетов, которые отправлены с UDP-порта утилиты nc.

Для порта 1234 на компьютере, который принимает пакеты, создадим следующее правило:

```
iptables -A INPUT -p udp --sport 1234 -j DROP
```

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox	s4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help	File Machine View Input Devices Help
<pre>root@s1:~# nc -u 7.7.34.2 1234 udp test ^C root@s1:~# nc 7.7.34.2 1234 tcp test root@s1:~# nc -u 7.7.34.2 1234 udp test</pre>	<pre>root@s4:~# nc -l -k -u 1234 udp test ^C root@s4:~# iptables -A INPUT -p udp --sport 1234 -j DROP root@s4:~# nc -l -k 1234 tcp test ^C root@s4:~# nc -l -k -u 1234 _</pre>

Рис. 4. Демонстрация работы правила №2

3. Запретить передачу только тех пакетов, которые отправлены с IP-адреса компьютера А.

На передающей стороне создадим следующее правило:

```
iptables -A OUTPUT -s 7.7.13.1 -j DROP
```

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox	s4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help	File Machine View Input Devices Help
<pre> root@s1:~# ping -c 1 7.7.34.2 PING 7.7.34.2 (7.7.34.2) 56(84) bytes of data. 64 bytes from 7.7.34.2: icmp_seq=1 ttl=63 time=2.00 ms --- 7.7.34.2 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 2.002/2.002/2.002/0.000 ms root@s1:~# iptables -A OUTPUT -s 7.7.13.1 -j DROP root@s1:~# ping -c 1 7.7.34.2 PING 7.7.34.2 (7.7.34.2) 56(84) bytes of data. ping: sendmsg: Operation not permitted --- 7.7.34.2 ping statistics --- 1 packets transmitted, 0 received, 100% packet loss, time 0ms root@s1:~# _ </pre>	<pre> root@s4:~# tcpdump icmp tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes 18:41:22.989212 IP 7.7.13.1 > 7.7.34.2: ICMP echo request, id 2225, seq 1, length 64 18:41:22.989314 IP 7.7.34.2 > 7.7.13.1: ICMP echo reply, id 2225, seq 1, length 64 - </pre>

Рис. 5. Демонстрация работы правила №3

4. Запретить приём только тех пакетов, которые отправлены на IP-адрес компьютера Б.

На принимающей стороне создадим следующее правило:

```
iptables -A INPUT -d 7.7.34.2 -j DROP
```

ICMP Echo Request отображается на принимающей стороне, поскольку tcpdump получает трафик до его фильтрации. ICMP Echo Reply при этом уже не отправляется:

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox	s4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help	File Machine View Input Devices Help
<pre> root@s1:~# ping -c 1 7.7.34.2 PING 7.7.34.2 (7.7.34.2) 56(84) bytes of data. 64 bytes from 7.7.34.2: icmp_seq=1 ttl=63 time=0.965 ms --- 7.7.34.2 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.965/0.965/0.965/0.000 ms root@s1:~# ping -c 1 7.7.34.2 PING 7.7.34.2 (7.7.34.2) 56(84) bytes of data. --- 7.7.34.2 ping statistics --- 1 packets transmitted, 0 received, 100% packet loss, time 0ms root@s1:~# </pre>	<pre> root@s4:~# tcpdump icmp tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes 18:58:39.656664 IP 7.7.13.1 > 7.7.34.2: ICMP echo request, id 2249, seq 1, length 64 18:58:39.656701 IP 7.7.34.2 > 7.7.13.1: ICMP echo reply, id 2249, seq 1, length 64 ^C 2 packets captured 2 packets received by filter 0 packets dropped by kernel root@s4:~# iptables -A INPUT -d 7.7.34.2 -j DROP root@s4:~# tcpdump icmp tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes 18:58:49.900921 IP 7.7.13.1 > 7.7.34.2: ICMP echo request, id 2250, seq 1, length 64 - </pre>

Рис. 6. Демонстрация работы правила №4

5. Запретить приём и передачу ICMP-пакетов, размер которых превышает 1000 байт, а поле TTL при этом меньше 10.

На передающей стороне создадим следующее правило:

```
iptables -A OUTPUT -p icmp -m length --length 1001:65535 -m ttl --ttl-lt 10 -j DROP
```

На принимающей стороне создадим такое же правило, заменив цепочку OUTPUT на INPUT.

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox	s4 [Running] - Oracle VM VirtualBox
<pre>File Machine View Input Devices Help root@s1:~# ping -c 1 -t 9 -s 973 7.7.34.2 PING 7.7.34.2 (7.7.34.2) 973(1001) bytes of data. 981 bytes from 7.7.34.2: icmp_seq=1 ttl=63 time=2.22 ms --- 7.7.34.2 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 2.221/2.221/2.221/0.000 ms root@s1:~# iptables -A OUTPUT -p icmp -m length --length 1001:65535 -m ttl --ttl-lt 10 -j DROP root@s1:~# ping -c 1 -t 9 -s 973 7.7.34.2 PING 7.7.34.2 (7.7.34.2) 973(1001) bytes of data. ping: sendmsg: Operation not permitted --- 7.7.34.2 ping statistics --- 1 packets transmitted, 0 received, 100% packet loss, time 0ms root@s1:~# iptables -D OUTPUT -p icmp -m length --length 1001:65535 -m ttl --ttl-lt 10 -j DROP root@s1:~# ping -c 1 -t 9 -s 973 7.7.34.2 PING 7.7.34.2 (7.7.34.2) 973(1001) bytes of data. --- 7.7.34.2 ping statistics --- 1 packets transmitted, 0 received, 100% packet loss, time 0ms root@s1:~#</pre>	<pre>File Machine View Input Devices Help root@s4:~# tcpdump icmp tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes 19:40:12.119566 IP 7.7.13.1 > 7.7.34.2: ICMP echo request, id 2301, seq 1, length 981 19:40:12.119648 IP 7.7.34.2 > 7.7.13.1: ICMP echo reply, id 2301, seq 1, length 981 ^C 2 packets captured 2 packets received by filter 0 packets dropped by kernel root@s4:~# iptables -A INPUT -p icmp -m length --length 1001:65535 -m ttl --ttl-lt 10 -j DROP root@s4:~# tcpdump icmp tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes 19:41:18.420998 IP 7.7.13.1 > 7.7.34.2: ICMP echo request, id 2305, seq 1, length 981</pre>

Рис. 7. Демонстрация работы правила №5

Задание вариативной части

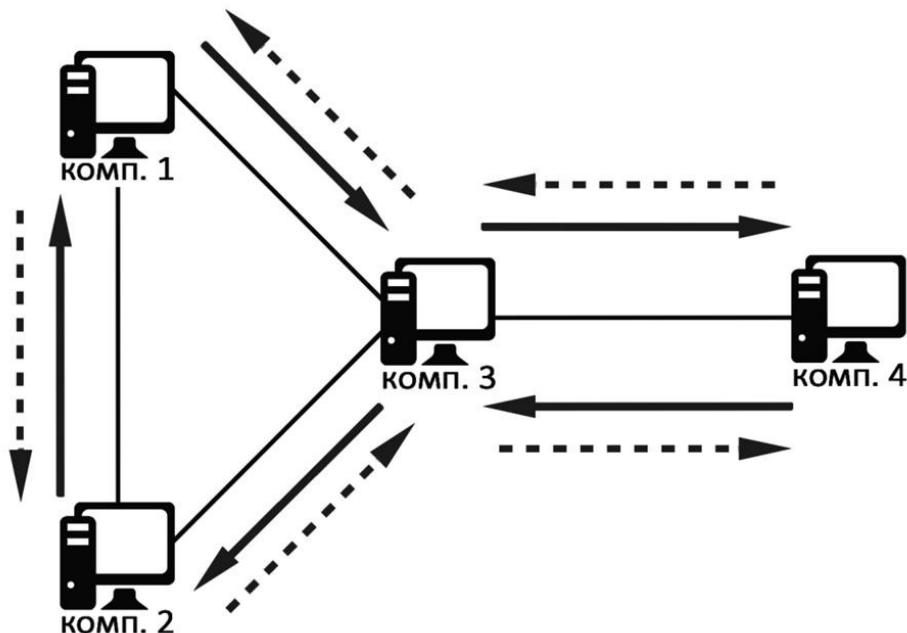


Рис. 8. Топология сети и схема прохождения трафика для варианта 5

На рисунке 8 изображена топология сети и требуемый путь прохождения сетевых пакетов.

С компьютера 4 посылается ICMP Echo Request на адрес, который не существует в данной сети. На компьютерах 1, 2 и 3 должны быть настроены таблицы маршрутизации и правила NAT таким образом, чтобы пакет поочередно прошел через компьютеры 3, 2, 1 и, снова пройдя через компьютер 3, пришел на компьютер 4 (сплошные линии на рисунке 1) с IP заголовком, в котором IP адрес источника и IP адрес назначения будут поменяны местами.

Таким образом, компьютер 4 получит ICMP Echo Request на свой локальный адрес и ответит на него. ICMP Echo Reply должен пройти обратный путь (4->3->1->2->3->4) и прийти на компьютер 4 (штриховые линии на рисунке 1) с поменяными местами адресами источника и назначения.

В результате выполнения команды ping должна быть выведена информация об успешном выполнении. То есть компьютер 4 сам отвечает на собственные ICMP запросы, однако пакет проходит через внешнюю сеть маршрутизаторов.

Выполнение вариативной части (IPv4)

В качестве несуществующего адреса в сети возьмем 7.7.0.1.

На компьютере #4 настроим отправку всех пакетов на выбранный адрес через компьютер #3:

```
ip link set eth0 up

ip a add 7.7.34.2/30 dev eth0

ip ro add 7.7.0.1 via 7.7.34.1

sysctl -w net.ipv4.ip_forward=1
sysctl -w net.ipv4.conf.all.rp_filter=0
sysctl -w net.ipv4.conf.eth0.rp_filter=0
```

Дальнейший маршрут следования пакета определяется компьютером #3.

Поступающий пакет помечается (MARK) правилами, добавленными в цепочку PREROUTING таблицы mangle, соответственно типу ICMP-сообщения: если это echo request (ping), то пакет адресован компьютеру #2, если же это echo reply (pong), то компьютеру #1. На основе метки выбирается отдельная таблица маршрутизации, перенаправляющая пакет на нужный интерфейс:

```
ip link set eth0 up
ip link set eth1 up
ip link set eth2 up

ip a add 7.7.13.2/30 dev eth0
ip a add 7.7.23.2/30 dev eth1
ip a add 7.7.34.1/30 dev eth2

# 4->3->2->1->3->4
iptables -t mangle -A PREROUTING -p icmp --icmp-type ping -d 7.7.0.1
-j MARK --set-mark 0x432134
# 4->3->1->2->3->4
iptables -t mangle -A PREROUTING -p icmp --icmp-type pong -d 7.7.0.1
-j MARK --set-mark 0x431234
```



```
ip ro add table 432134 default via 7.7.23.1 dev eth1
ip rule add fwmark 0x432134 table 432134
```

```
ip ro add table 431234 default via 7.7.13.1 dev eth0
ip rule add fwmark 0x431234 table 431234
```

```
sysctl -w net.ipv4.ip_forward=1
sysctl -w net.ipv4.conf.all.rp_filter=0
sysctl -w net.ipv4.conf.eth0.rp_filter=0
sysctl -w net.ipv4.conf.eth1.rp_filter=0
sysctl -w net.ipv4.conf.eth2.rp_filter=0
```

На компьютере #2 происходит замена IP-адресов получателя и отправителя с помощью правил DNAT и SNAT соответственно. Поскольку поступающие пакеты могут быть адресованы разным компьютерам, необходимо пометить их в зависимости от интерфейса-источника и направить с помощью таблиц маршрутизации в нужный узел:

```
ip link set eth0 up
ip link set eth1 up
```

```
ip a add 7.7.12.2/30 dev eth0
ip a add 7.7.23.1/30 dev eth1
```

```
iptables -t nat -A PREROUTING -p icmp -s 7.7.34.2 -d 7.7.0.1 -j DNAT
--to 7.7.34.2
iptables -t nat -A POSTROUTING -p icmp -s 7.7.34.2 -d 7.7.34.2 -j
SNAT --to 7.7.0.1
```

```
# 4->3->2->1->3->4
iptables -t mangle -A PREROUTING -p icmp -i eth1 -d 7.7.0.1 -j MARK
--set-mark 0x432134
# 4->3->1->2->3->4
iptables -t mangle -A PREROUTING -p icmp -i eth0 -d 7.7.0.1 -j MARK
--set-mark 0x431234
```

```
ip ro add table 432134 default via 7.7.12.1 dev eth0
ip rule add fwmark 0x432134 table 432134
```

```
ip ro add table 431234 default via 7.7.23.2 dev eth1
ip rule add fwmark 0x431234 table 431234
```

```
sysctl -w net.ipv4.ip_forward=1
sysctl -w net.ipv4.conf.all.rp_filter=0
sysctl -w net.ipv4.conf.eth0.rp_filter=0
sysctl -w net.ipv4.conf.eth1.rp_filter=0
```

Компьютер #1 выполняет аналогичное перенаправление трафика, исключая nat правила, поскольку они уже применяются на компьютере #2:

```

ip link set eth0 up
ip link set eth1 up

ip a add 7.7.12.1/30 dev eth0
ip a add 7.7.13.1/30 dev eth1

# 4->3->2->1->3->4
iptables -t mangle -A PREROUTING -p icmp -s 7.7.0.1 -j MARK --set-mark 0x432134
# 4->3->1->2->3->4
iptables -t mangle -A PREROUTING -p icmp -d 7.7.0.1 -j MARK --set-mark 0x431234

ip ro add table 432134 default via 7.7.13.2 dev eth1
ip rule add fwmark 0x432134 table 432134

ip ro add table 431234 default via 7.7.12.2 dev eth0
ip rule add fwmark 0x431234 table 431234

sysctl -w net.ipv4.ip_forward=1
sysctl -w net.ipv4.conf.all.rp_filter=0
sysctl -w net.ipv4.conf.eth0.rp_filter=0
sysctl -w net.ipv4.conf.eth1.rp_filter=0

```

Убедимся в правильном прохождении пакетов, отправив один запрос с помощью `ping -c 1 7.7.0.1` и проверив число пакетов, соответствующих всем mangle правилам, отвечающим за маркировку пакета:

s1 [Snapshot 1] [Running] - Oracle VM VirtualBox										s3 [Running] - Oracle VM VirtualBox									
File	Machine	View	Input	Devices	Help					File	Machine	View	Input	Devices	Help				
root@s1:~# iptables -t mangle -L -v										root@s3:~# iptables -t mangle -L -v									
Chain PREROUTING (policy ACCEPT 16 packets, 4760 bytes)										Chain PREROUTING (policy ACCEPT 9 packets, 1976 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
1	84	MARK	icmp	--	any	any	7.7.0.1	MARK set 0x		1	84	MARK	icmp	--	any	any	anywhere	7.7.0.1	icmp echo-r
432134										request MARK set 0x432134									
1	84	MARK	icmp	--	any	any	anywhere	7.7.0.1	MARK set 0x	1	84	MARK	icmp	--	any	any	anywhere	7.7.0.1	icmp echo-r
431234										reply MARK set 0x431234									
Chain INPUT (policy ACCEPT 14 packets, 4592 bytes)										Chain INPUT (policy ACCEPT 5 packets, 1640 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
Chain FORWARD (policy ACCEPT 2 packets, 168 bytes)										Chain FORWARD (policy ACCEPT 4 packets, 336 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)										Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
Chain POSTROUTING (policy ACCEPT 2 packets, 168 bytes)										Chain POSTROUTING (policy ACCEPT 4 packets, 336 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
s2 [Running] - Oracle VM VirtualBox										s4 [Running] - Oracle VM VirtualBox									
File	Machine	View	Input	Devices	Help					File	Machine	View	Input	Devices	Help				
root@s2:~# iptables -t mangle -L -v										root@s4:~# ping -c 1 7.7.0.1									
Chain PREROUTING (policy ACCEPT 41 packets, 4832 bytes)										PING 7.7.0.1 (7.7.0.1) 56(84) bytes of data.									
pkts	bytes	target	prot	opt	in	out	source	destination		64 bytes from 7.7.0.1: icmp_seq=1 ttl=60 time=8.32 ms									
1	84	MARK	icmp	--	eth1	any	anywhere	7.7.0.1	MARK set 0x	--- 7.7.0.1 ping statistics ---									
432134										MARK set 0x1 packets transmitted, 1 received, 0% packet loss, time 0ms									
1	84	MARK	icmp	--	eth0	any	anywhere	7.7.0.1		rtt min/avg/max/mdev = 8.322/8.322/8.322/0.000 ms									
431234										root@s4:~#									
Chain INPUT (policy ACCEPT 39 packets, 4664 bytes)																			
pkts	bytes	target	prot	opt	in	out	source	destination											
Chain FORWARD (policy ACCEPT 2 packets, 168 bytes)																			
pkts	bytes	target	prot	opt	in	out	source	destination											
Chain OUTPUT (policy ACCEPT 32 packets, 2368 bytes)																			
pkts	bytes	target	prot	opt	in	out	source	destination											
Chain POSTROUTING (policy ACCEPT 34 packets, 2536 bytes)																			
pkts	bytes	target	prot	opt	in	out	source	destination											

Рис. 9. Демонстрация работы вариативной части

Настройки узлов приведены на рисунках 11-13.

Выполнение вариативной части (IPv6)

Адресация узлов соответствует пункту *Настройка сети* представленного отчета.

В качестве несуществующего адреса в сети возьмем fc00::7.7.0.0.

При настройке IPv6 были внесены следующие изменения:

- вместо команд `ip ...` используются команды `ip -6 ...`
- вместо утилиты `iptables` используется `ip6tables`
- вместо утилиты `ping` используется `ping6`

Утилита `ping6` отправляет пакеты ICMPv6, которые отличаются от ICMPv4 измененными типами сообщений (в частности, 128 для `echo request` и 129 для `echo reply` вместо 8 и 0).

Настройка компьютера #4:

```
ip link set eth0 up
ip -6 a add fc00::7.7.34.1/127 dev eth0
ip -6 ro add fc00::7.7.0.0 via fc00::7.7.34.0
sysctl -w net.ipv6.conf.all.forwarding=1
```

Настройка компьютера #3:

```
ip link set eth0 up
ip link set eth1 up
ip link set eth2 up

ip -6 a add fc00::7.7.13.1/127 dev eth0
ip -6 a add fc00::7.7.23.1/127 dev eth1
ip -6 a add fc00::7.7.34.0/127 dev eth2

# 4->3->2->1->3->4
ip6tables -t mangle -A PREROUTING -p icmpv6 --icmpv6-type ping -d fc00::7.7.0.0 -j MARK --set-mark 0x432134
# 4->3->1->2->3->4
ip6tables -t mangle -A PREROUTING -p icmpv6 --icmpv6-type pong -d fc00::7.7.0.0 -j MARK --set-mark 0x431234

ip -6 ro add table 432134 default via fc00::7.7.23.0 dev eth1
ip -6 rule add fwmark 0x432134 table 432134

ip -6 ro add table 431234 default via fc00::7.7.13.0 dev eth0
ip -6 rule add fwmark 0x431234 table 431234

sysctl -w net.ipv6.conf.all.forwarding=1
```

Настройка компьютера #2:

```

ip link set eth0 up
ip link set eth1 up

ip -6 a add fc00::7.7.12.1/127 dev eth0
ip -6 a add fc00::7.7.23.0/127 dev eth1

ip6tables -t nat -A PREROUTING -p icmpv6 -s fc00::7.7.34.1 -d
fc00::7.7.0.0 -j DNAT --to fc00::7.7.34.1
ip6tables -t nat -A POSTROUTING -p icmpv6 -s fc00::7.7.34.1 -d
fc00::7.7.34.1 -j SNAT --to fc00::7.7.0.0

# 4->3->2->1->3->4
ip6tables -t mangle -A PREROUTING -p icmpv6 -i eth1 -d fc00::7.7.0.0
-j MARK --set-mark 0x432134
# 4->3->1->2->3->4
ip6tables -t mangle -A PREROUTING -p icmpv6 -i eth0 -d fc00::7.7.0.0
-j MARK --set-mark 0x431234

ip -6 ro add table 432134 default via fc00::7.7.12.0 dev eth0
ip -6 rule add fwmark 0x432134 table 432134

ip -6 ro add table 431234 default via fc00::7.7.23.1 dev eth1
ip -6 rule add fwmark 0x431234 table 431234

sysctl -w net.ipv6.conf.all.forwarding=1

```

Настройка компьютера #1:

```

ip link set eth0 up
ip link set eth1 up

ip -6 a add fc00::7.7.12.0/127 dev eth0
ip -6 a add fc00::7.7.13.0/127 dev eth1

# 4->3->2->1->3->4
ip6tables -t mangle -A PREROUTING -p icmpv6 -s fc00::7.7.0.0 -j MARK
--set-mark 0x432134
# 4->3->1->2->3->4
ip6tables -t mangle -A PREROUTING -p icmpv6 -d fc00::7.7.0.0 -j MARK
--set-mark 0x431234

ip -6 ro add table 432134 default via fc00::7.7.13.1 dev eth1
ip -6 rule add fwmark 0x432134 table 432134

ip -6 ro add table 431234 default via fc00::7.7.12.1 dev eth0
ip -6 rule add fwmark 0x431234 table 431234

sysctl -w net.ipv6.conf.all.forwarding=1

```

s1 [Snapshot 1] [Running] - Oracle VM VirtualBox										s3 [Running] - Oracle VM VirtualBox									
File	Machine	View	Input	Devices	Help					File	Machine	View	Input	Devices	Help				
root@s1:~# iptables -t mangle -L -v										root@s3:~# iptables -t mangle -L -v									
Chain PREROUTING (policy ACCEPT 16 packets, 768 bytes)										Chain PREROUTING (policy ACCEPT 16 packets, 1248 bytes)									
pkts	bytes	target	prot	opt in	out	source	destination			pkts	bytes	target	prot	opt in	out	source	destination		
1	104	MARK	ipv6-icmp	any	any	fc00::707:0	anywhere	MARK se		1	104	MARK	ipv6-icmp	any	any	anywhere	fc00::707:0	ipv6-ic	
t	0x432134									mp	echo-request	MARK	set	0x432134					
1	104	MARK	ipv6-icmp	any	any	anywhere	fc00::707:0	MARK se		1	104	MARK	ipv6-icmp	any	any	anywhere	fc00::707:0	ipv6-ic	
t	0x431234									mp	echo-reply	MARK	set	0x431234					
Chain INPUT (policy ACCEPT 8 packets, 560 bytes)										Chain INPUT (policy ACCEPT 12 packets, 832 bytes)									
pkts	bytes	target	prot	opt in	out	source	destination			pkts	bytes	target	prot	opt in	out	source	destination		
Chain FORWARD (policy ACCEPT 2 packets, 208 bytes)										Chain FORWARD (policy ACCEPT 4 packets, 416 bytes)									
pkts	bytes	target	prot	opt in	out	source	destination			pkts	bytes	target	prot	opt in	out	source	destination		
Chain OUTPUT (policy ACCEPT 19 packets, 1720 bytes)										Chain OUTPUT (policy ACCEPT 31 packets, 2824 bytes)									
pkts	bytes	target	prot	opt in	out	source	destination			pkts	bytes	target	prot	opt in	out	source	destination		
Chain POSTROUTING (policy ACCEPT 21 packets, 1928 bytes)										Chain POSTROUTING (policy ACCEPT 35 packets, 3240 bytes)									
pkts	bytes	target	prot	opt in	out	source	destination			pkts	bytes	target	prot	opt in	out	source	destination		
s2 [Running] - Oracle VM VirtualBox										s4 [Running] - Oracle VM VirtualBox									
File	Machine	View	Input	Devices	Help					File	Machine	View	Input	Devices	Help				
root@s2:~# iptables -t mangle -L -v										root@s4:~# ping6 -c 1 fc00::7:7:0:0									
Chain PREROUTING (policy ACCEPT 10 packets, 768 bytes)										PING fc00::7:7:0:0(fc00::707:0) 56 data bytes									
pkts	bytes	target	prot	opt in	out	source	destination			64 bytes from fc00::707:0: icmp_seq=1 ttl=60 time=4.56 ms									
1	104	MARK	ipv6-icmp	eth1	any	anywhere	fc00::707:0	MARK se											
t	0x432134									--- fc00::7:7:0:0 ping statistics ---									
1	104	MARK	ipv6-icmp	eth0	any	anywhere	fc00::707:0	MARK se1		packets transmitted, 1 received, 0% packet loss, time 0ms									
t	0x431234									rtt min/avg/max/mdev = 4.560/4.560/4.560/0.000 ms									
										root@s4:~#									
Chain INPUT (policy ACCEPT 8 packets, 560 bytes)																			
pkts	bytes	target	prot	opt in	out	source	destination												
Chain FORWARD (policy ACCEPT 2 packets, 208 bytes)																			
pkts	bytes	target	prot	opt in	out	source	destination												
Chain OUTPUT (policy ACCEPT 19 packets, 1720 bytes)																			
pkts	bytes	target	prot	opt in	out	source	destination												
Chain POSTROUTING (policy ACCEPT 21 packets, 1928 bytes)																			
pkts	bytes	target	prot	opt in	out	source	destination												

Рис. 10. Демонстрация работы вариативной части

Настройки узлов приведены на рисунках 11, 14, 15.

Настройки узлов вариативной части

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox	s3 [Running] - Oracle VM VirtualBox
<pre>File Machine View Input Devices Help root@s1:~# ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:b2:fd:a2 brd ff:ff:ff:ff:ff:ff inet 7.7.12.1/30 scope global eth0 valid_lft forever preferred_lft forever inet6 fc00::707:c00/127 scope global valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:feb2:fd2/64 scope link valid_lft forever preferred_lft forever 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:38:e1:8f brd ff:ff:ff:ff:ff:ff inet 7.7.13.1/30 scope global eth1 valid_lft forever preferred_lft forever inet6 fc00::707:400/127 scope global valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:fe38:e18f/64 scope link valid_lft forever preferred_lft forever root@s1:~#</pre>	<pre>File Machine View Input Devices Help root@s3:~# ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:f4:0c:1a brd ff:ff:ff:ff:ff:ff inet 7.7.13.2/30 scope global eth0 valid_lft forever preferred_lft forever inet6 fc00::707:d01/127 scope global valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:fe4:c1a/64 scope link valid_lft forever preferred_lft forever eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:65:e8:fc brd ff:ff:ff:ff:ff:ff inet 7.7.23.2/30 scope global eth1 valid_lft forever preferred_lft forever inet6 fc00::707:1701/127 scope global valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:fe65:e8fc/64 scope link valid_lft forever preferred_lft forever 4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:f6:f1:af brd ff:ff:ff:ff:ff:ff inet 7.7.34.1/30 scope global eth2 valid_lft forever preferred_lft forever inet6 fc00::707:2200/127 scope global valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:fe6:f1af/64 scope link valid_lft forever preferred_lft forever root@s3:~#</pre>
s2 [Running] - Oracle VM VirtualBox	s4 [Running] - Oracle VM VirtualBox
<pre>File Machine View Input Devices Help root@s2:~# ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:ef:b0:05 brd ff:ff:ff:ff:ff:ff inet 7.7.12.2/30 scope global eth0 valid_lft forever preferred_lft forever inet6 fc00::707:c01/127 scope global valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:feef:b005/64 scope link valid_lft forever preferred_lft forever 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:f8:4a:eb brd ff:ff:ff:ff:ff:ff inet 7.7.23.1/30 scope global eth1 valid_lft forever preferred_lft forever inet6 fc00::707:1700/127 scope global valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:fe8:4aeb/64 scope link valid_lft forever preferred_lft forever root@s2:~#</pre>	<pre>File Machine View Input Devices Help root@s4:~# ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 08:00:27:ef:94:66 brd ff:ff:ff:ff:ff:ff inet 7.7.34.2/30 scope global eth0 valid_lft forever preferred_lft forever inet6 fc00::707:2201/127 scope global valid_lft forever preferred_lft forever inet6 fe80::a00:27ff:feef:9466/64 scope link valid_lft forever preferred_lft forever root@s4:~#</pre>

Рис. 11. Настроїнки адресації (IPv4 у IPv6)

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox										s3 [Running] - Oracle VM VirtualBox									
File	Machine	View	Input	Devices	Help					File	Machine	View	Input	Devices	Help				
root@s1:~# iptables -t mangle -L -v										root@s3:~# iptables -t mangle -L -v									
Chain PREROUTING (policy ACCEPT 56 packets, 9752 bytes)										Chain PREROUTING (policy ACCEPT 13 packets, 3288 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
1	84	MARK	icmp	--	any	any	7.7.0.1			1	84	MARK	icmp	--	any	any	anywhere	7.7.0.1	icmp echo-r
432134																			
1	84	MARK	icmp	--	any	any	anywhere	7.7.0.1	MARK set 0x	1	84	MARK	icmp	--	any	any	anywhere	7.7.0.1	icmp echo-r
432134										reply MARK set 0x432134									
Chain INPUT (policy ACCEPT 54 packets, 9584 bytes)										Chain INPUT (policy ACCEPT 9 packets, 2952 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
Chain FORWARD (policy ACCEPT 2 packets, 168 bytes)										Chain FORWARD (policy ACCEPT 4 packets, 336 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
Chain OUTPUT (policy ACCEPT 32 packets, 2368 bytes)										Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
Chain POSTROUTING (policy ACCEPT 34 packets, 2536 bytes)										Chain POSTROUTING (policy ACCEPT 4 packets, 336 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination		pkts	bytes	target	prot	opt	in	out	source	destination	
s2 [Running] - Oracle VM VirtualBox										s4 [Running] - Oracle VM VirtualBox									
File	Machine	View	Input	Devices	Help					File	Machine	View	Input	Devices	Help				
root@s2:~# iptables -t mangle -L -v										root@s4:~# ping -c 1 7.7.0.1									
Chain PREROUTING (policy ACCEPT 40 packets, 4504 bytes)										PING 7.7.0.1 (7.7.0.1) 56(84) bytes of data.									
pkts	bytes	target	prot	opt	in	out	source	destination		64 bytes from 7.7.0.1: icmp_seq=1 ttl=60 time=3.36 ms									
1	84	MARK	icmp	--	eth1	any	anywhere	7.7.0.1	MARK set 0x	--- 7.7.0.1 ping statistics ---									
432134										0x1 packets transmitted, 1 received, 0% packet loss, time 0ms									
1	84	MARK	icmp	--	eth0	any	anywhere	7.7.0.1	MARK set 0x1	rtt min/avg/max/mdev = 3.367/3.367/3.367/0.000 ms									
432134										root@s4:~# ping6 -c 1 fc00::7.7.0.0									
Chain INPUT (policy ACCEPT 38 packets, 4336 bytes)										PING fc00::7.7.0.0(fc00::707:0) 56 data bytes									
pkts	bytes	target	prot	opt	in	out	source	destination		64 bytes from fc00::707:0: icmp_seq=1 ttl=60 time=11.4 ms									
Chain FORWARD (policy ACCEPT 2 packets, 168 bytes)										--- fc00::7.7.0.0 ping statistics ---									
pkts	bytes	target	prot	opt	in	out	source	destination		1 packets transmitted, 1 received, 0% packet loss, time 0ms									
Chain OUTPUT (policy ACCEPT 32 packets, 2368 bytes)										rtt min/avg/max/mdev = 11.461/11.461/11.461/0.000 ms									
pkts	bytes	target	prot	opt	in	out	source	destination		root@s4:~#									
Chain POSTROUTING (policy ACCEPT 34 packets, 2536 bytes)																			
pkts	bytes	target	prot	opt	in	out	source	destination											
root@s2:~# iptables -t nat -L -v																			
Chain PREROUTING (policy ACCEPT 1 packets, 328 bytes)																			
pkts	bytes	target	prot	opt	in	out	source	destination											
1	84	DNAT	icmp	--	any	any	7.7.34.2	7.7.0.1	to:7.7.34.2										
Chain INPUT (policy ACCEPT 1 packets, 328 bytes)																			
pkts	bytes	target	prot	opt	in	out	source	destination											
Chain OUTPUT (policy ACCEPT 12 packets, 744 bytes)																			
pkts	bytes	target	prot	opt	in	out	source	destination											
Chain POSTROUTING (policy ACCEPT 12 packets, 744 bytes)																			
pkts	bytes	target	prot	opt	in	out	source	destination											
1	84	SNAT	icmp	--	any	any	7.7.34.2	7.7.34.2	to:7.7.0.1										

Рис. 12. Настройка iptables (Ipn4)

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox					s3 [Running] - Oracle VM VirtualBox				
File	Machine	View	Input	Devices	Help	File	Machine	View	Input
<pre> root@s1:~# ip rule list 0: from all lookup local 32764: from all fwmark 0x431234 lookup 431234 32765: from all fwmark 0x432134 lookup 432134 32766: from all lookup main 32767: from all lookup default root@s1:~# ip ro list table 431234 default via 7.7.12.2 dev eth0 root@s1:~# ip ro list table 432134 default via 7.7.13.2 dev eth1 root@s1:~# ip ro list 7.7.12.0/30 dev eth0 proto kernel scope link src 7.7.12.1 7.7.13.0/30 dev eth1 proto kernel scope link src 7.7.13.1 root@s1:~# </pre>					<pre> root@s3:~# ip rule list 0: from all lookup local 32764: from all fwmark 0x431234 lookup 431234 32765: from all fwmark 0x432134 lookup 432134 32766: from all lookup main 32767: from all lookup default root@s3:~# ip ro list table 431234 default via 7.7.13.1 dev eth0 root@s3:~# ip ro list table 432134 default via 7.7.23.1 dev eth1 root@s3:~# ip ro list 7.7.13.0/30 dev eth0 proto kernel scope link src 7.7.13.2 7.7.23.0/30 dev eth1 proto kernel scope link src 7.7.23.2 7.7.34.0/30 dev eth2 proto kernel scope link src 7.7.34.1 root@s3:~# </pre>				
s2 [Running] - Oracle VM VirtualBox					s4 [Running] - Oracle VM VirtualBox				
File	Machine	View	Input	Devices	Help	File	Machine	View	Input
<pre> root@s2:~# ip rule list 0: from all lookup local 32764: from all fwmark 0x431234 lookup 431234 32765: from all fwmark 0x432134 lookup 432134 32766: from all lookup main 32767: from all lookup default root@s2:~# ip ro list table 431234 default via 7.7.23.2 dev eth1 root@s2:~# ip ro list table 432134 default via 7.7.12.1 dev eth0 root@s2:~# ip ro list 7.7.12.0/30 dev eth0 proto kernel scope link src 7.7.12.2 7.7.23.0/30 dev eth1 proto kernel scope link src 7.7.23.1 root@s2:~# </pre>					<pre> root@s4:~# ip rule list 0: from all lookup local 32766: from all lookup main 32767: from all lookup default root@s4:~# ip ro list 7.7.0.1 via 7.7.34.1 dev eth0 7.7.34.0/30 dev eth0 proto kernel scope link src 7.7.34.2 root@s4:~# </pre>				

Рис. 13. Таблицы маршрутизации (IPv4)

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox										s3 [Running] - Oracle VM VirtualBox									
File Machine View Input Devices Help										File Machine View Input Devices Help									
root@s1:~# iptables -t mangle -L -v										root@s3:~# iptables -t mangle -L -v									
Chain PREROUTING (policy ACCEPT 19 packets, 768 bytes)										Chain PREROUTING (policy ACCEPT 17 packets, 1304 bytes)									
pkts bytes target	prot opt in	out	source	destination						pkts bytes target	prot opt in	out	source	destination					
1 104 MARK	ipv6-icmp	any	any	fc00::707:0	anywhere				MARK se	1 104 MARK	ipv6-icmp	any	any	anywhere	fc00::707:0			ipv6-ic	
t 0x432134										mp echo-request	MARK set	0x432134							
t 0x432134										MARK se	1 104 MARK	ipv6-icmp	any	any	anywhere	fc00::707:0			ipv6-ic
t 0x432134										mp echo-reply	MARK set	0x432134							
Chain INPUT (policy ACCEPT 8 packets, 560 bytes)										Chain INPUT (policy ACCEPT 13 packets, 888 bytes)									
pkts bytes target	prot opt in	out	source	destination						pkts bytes target	prot opt in	out	source	destination					
Chain FORWARD (policy ACCEPT 2 packets, 208 bytes)										Chain FORWARD (policy ACCEPT 4 packets, 416 bytes)									
pkts bytes target	prot opt in	out	source	destination						pkts bytes target	prot opt in	out	source	destination					
Chain OUTPUT (policy ACCEPT 14 packets, 1232 bytes)										Chain OUTPUT (policy ACCEPT 21 packets, 1848 bytes)									
pkts bytes target	prot opt in	out	source	destination						pkts bytes target	prot opt in	out	source	destination					
Chain POSTROUTING (policy ACCEPT 16 packets, 1440 bytes)										Chain POSTROUTING (policy ACCEPT 25 packets, 2264 bytes)									
pkts bytes target	prot opt in	out	source	destination						pkts bytes target	prot opt in	out	source	destination					
s2 [Running] - Oracle VM VirtualBox										s4 [Running] - Oracle VM VirtualBox									
File Machine View Input Devices Help										File Machine View Input Devices Help									
root@s2:~# iptables -t mangle -L -v										root@s4:~# ping -c 1 7.7.0.1									
Chain PREROUTING (policy ACCEPT 19 packets, 768 bytes)										PING 7.7.0.1 (7.7.0.1) 56(84) bytes of data.									
pkts bytes target	prot opt in	out	source	destination						64 bytes from 7.7.0.1: icmp_seq=1 ttl=60 time=3.36 ms									
1 104 MARK	ipv6-icmp	eth1	any	anywhere	fc00::707:0				MARK se	--- 7.7.0.1 ping statistics ---									
t 0x432134										1 packets transmitted, 1 received, 0% packet loss, time 0ms									
t 0x432134										rtt min/avg/max/mdev = 3.367/3.367/3.367/0.000 ms									
Chain INPUT (policy ACCEPT 8 packets, 560 bytes)										root@s4:~# ping6 -c 1 fc00::7.7.0.0									
pkts bytes target	prot opt in	out	source	destination						PING fc00::7.7.0.0(fc00::707:0) 56 data bytes									
Chain FORWARD (policy ACCEPT 2 packets, 208 bytes)										64 bytes from fc00::707:0: icmp_seq=1 ttl=60 time=11.4 ms									
pkts bytes target	prot opt in	out	source	destination						--- fc00::7.7.0.0 ping statistics ---									
Chain OUTPUT (policy ACCEPT 14 packets, 1192 bytes)										1 packets transmitted, 1 received, 0% packet loss, time 0ms									
pkts bytes target	prot opt in	out	source	destination						rtt min/avg/max/mdev = 11.461/11.461/11.461/0.000 ms									
Chain POSTROUTING (policy ACCEPT 16 packets, 1400 bytes)										root@s4:~# _									
pkts bytes target	prot opt in	out	source	destination															
root@s2:~# iptables -t nat -L -v																			
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)																			
pkts bytes target	prot opt in	out	source	destination															
1 104 DNAT	ipv6-icmp	any	any	fc00::707:2201	fc00::707:0				to:fc00										
::707:2201																			
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)																			
pkts bytes target	prot opt in	out	source	destination															
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)																			
pkts bytes target	prot opt in	out	source	destination															
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)																			
pkts bytes target	prot opt in	out	source	destination															
1 104 SNAT	ipv6-icmp	any	any	fc00::707:2201	fc00::707:2201				to:fc00										
::707:0																			

Рис. 14. Настройка iptables (Ipv6)

s1 (Snapshot 1) [Running] - Oracle VM VirtualBox	s3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help	File Machine View Input Devices Help
<pre> root@s1:~# ip rule list 0: from all lookup local 32764: from all fwmark 0x431234 lookup 431234 32765: from all fwmark 0x432134 lookup 432134 32766: from all lookup main 32767: from all lookup default root@s1:~# ip ro list table 431234 default via 7.7.12.2 dev eth0 root@s1:~# ip ro list table 432134 default via 7.7.13.2 dev eth1 root@s1:~# ip ro list 7.7.12.0/30 dev eth0 proto kernel scope link src 7.7.12.1 7.7.13.0/30 dev eth1 proto kernel scope link src 7.7.13.1 root@s1:~# </pre>	<pre> root@s3:~# ip -6 rule list 0: from all lookup local 32764: from all fwmark 0x431234 lookup 431234 32765: from all fwmark 0x432134 lookup 432134 32766: from all lookup main root@s3:~# ip -6 ro list table 431234 default via fc00::707:d00 dev eth0 metric 1024 root@s3:~# ip -6 ro list table 432134 default via fc00::707:1700 dev eth1 metric 1024 root@s3:~# ip -6 ro list fc00::707:d00/127 dev eth0 proto kernel metric 256 fc00::707:1700/127 dev eth1 proto kernel metric 256 fc00::707:2200/127 dev eth2 proto kernel metric 256 fe80::/64 dev eth0 proto kernel metric 256 fe80::/64 dev eth1 proto kernel metric 256 fe80::/64 dev eth2 proto kernel metric 256 root@s3:~# </pre>
s2 [Running] - Oracle VM VirtualBox	s4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help	File Machine View Input Devices Help
<pre> root@s2:~# ip -6 rule list 0: from all lookup local 32764: from all fwmark 0x431234 lookup 431234 32765: from all fwmark 0x432134 lookup 432134 32766: from all lookup main root@s2:~# ip -6 ro list table 431234 default via fc00::707:1701 dev eth1 metric 1024 root@s2:~# ip -6 ro list table 432134 default via fc00::707:c00 dev eth0 metric 1024 root@s2:~# ip -6 ro list fc00::707:c00/127 dev eth0 proto kernel metric 256 fc00::707:1700/127 dev eth1 proto kernel metric 256 fe80::/64 dev eth0 proto kernel metric 256 fe80::/64 dev eth1 proto kernel metric 256 root@s2:~# _ </pre>	<pre> root@s4:~# ip -6 rule list 0: from all lookup local 32766: from all lookup main root@s4:~# ip -6 ro list fc00::707:0 via fc00::707:2200 dev eth0 metric 1024 fc00::707:2200/127 dev eth0 proto kernel metric 256 fe80::/64 dev eth0 proto kernel metric 256 root@s4:~# </pre>

Рис. 15. Таблицы маршрутизации (IPv6)