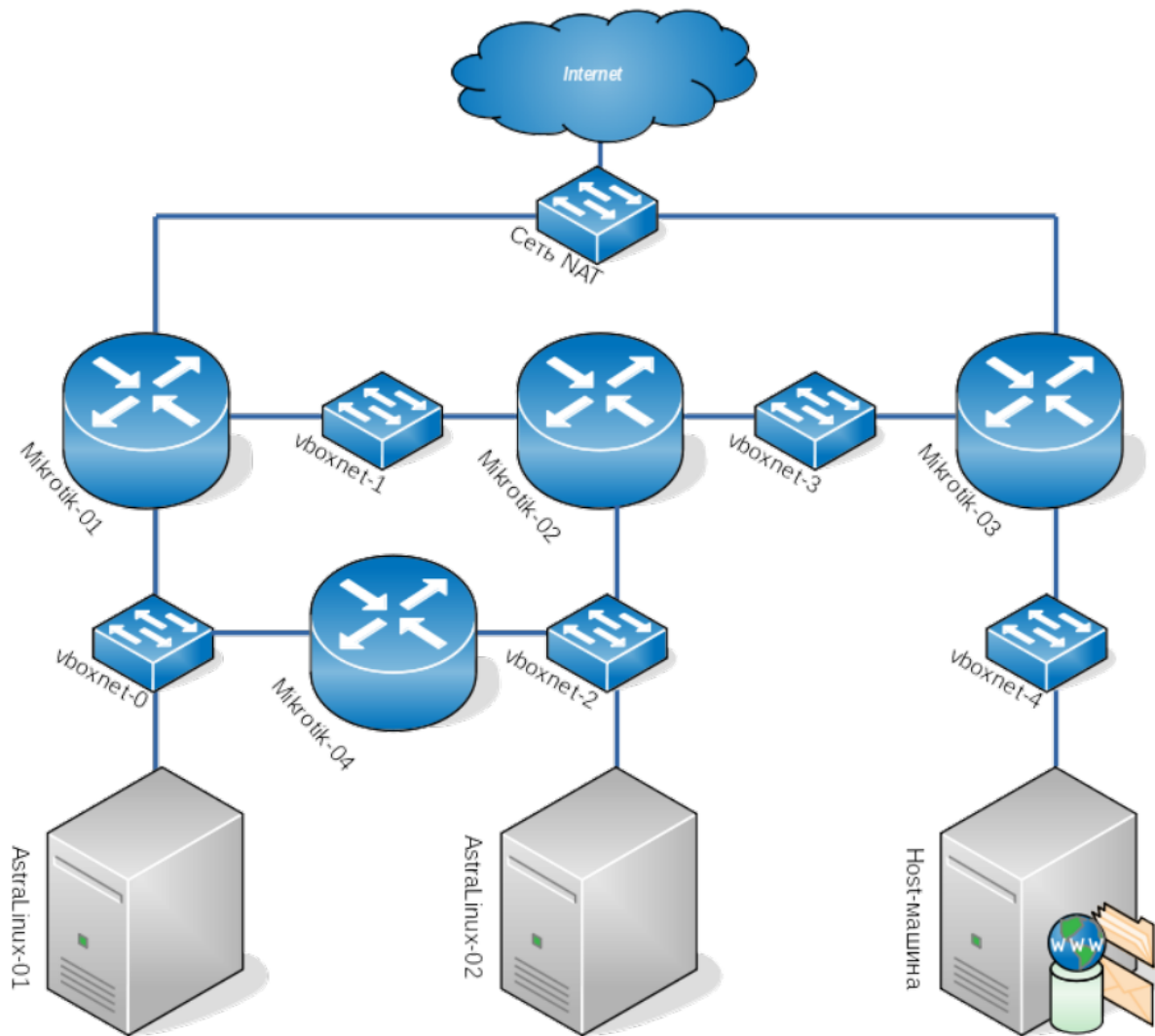


Задание

1. Собрать конфигурацию сети, представленной на рисунке. Доступ в сеть Интернет сконфигурирован для маршрутизаторов Mikrotik-01 и Mikrotik-03 через сеть NAT в VirtualBox. На всех узлах (кроме хоста) последний интерфейс должен быть использован как management интерфейс, остальные "рабочие" интерфейсы используются для передачи данных.



2. Задать уникальные сетевые имена всем узлам (кроме хоста). На management интерфейсах настроить проброс портов (DNAT) с локального интерфейса host-машины до web интерфейса маршрутизатора и до ssh на виртуальных машинах Astra Linux (доступ по ssh должен осуществляться по открытому ключу).
3. Объединить все рабочие порты коммутаторов в сетевые мосты. Настроить работу протокола STP. Показать, в каком состоянии оказались порты маршрутизаторов. Изменить настройки протокола STP так, чтобы корневым коммутатором был Mikrotik-02, а резервным Mikrotik-04.

4. Выделен диапазон IPv4 адресов 10.10.N.0/24 (N - номер в журнале). Разделить полученный диапазон на максимально возможное количество подсетей так, чтобы каждая подсеть могла адресовать до 6 узлов. Выбрать один из полученных диапазонов и сконфигурировать соответствующим образом интерфейсы виртуальных машин и сетевых мостов на маршрутизаторах. Убедиться, что есть связь между всеми указанными сетевыми устройствами. Для доказательства наличия связи использовать захват пакетов с помощью Wireshark.
5. На маршрутизаторах Mikrotik-01, Mikrotik-02, Mikrotik-03 создать VLAN с номером 2, которая будет использоваться для доступа в сеть NAT. Настроить VirtualBox так, чтобы в сети NAT функционировал DHCP сервер и раздавал IPv4 адреса из другого диапазона, чем выбран в пункте 4. На каждом из этих маршрутизаторов настроить dhcp-client так, чтобы автоматически конфигурировались соответствующие интерфейсы и все эти маршрутизаторы получили доступ в сеть Интернет (интерфейс маршрутизатора Mikrotik-2 в сети vboxnet2 пока в эту VLAN не включается). Определить, какие адреса назначены на маршрутизаторах.
6. На всех маршрутизаторах создать VLAN с номером 3, которая будет использоваться для доступа в сеть vboxnet4. Для адресации узлов в этой сети используется ещё один диапазон IPv4 адресов из п.4. Назначить адреса всем сетевым устройствам сети (маршрутизаторам, виртуальным машинам, хост-машине). Какие интерфейсы пингуются между собой? Примечание: на виртуальных машинах должны быть созданы виртуальные интерфейсы для доступа в тегированную VLAN с номером 3.
7. На маршрутизаторе Mikrotik-01 настроить правило трансляции адресов таким образом, чтобы предоставить виртуальной машине AstraLinux-01 доступ в Интернет из нетегированной сети. Изменить конфигурацию Mikrotik-02 таким образом, чтобы обеспечить доступ к тегированной VLAN с номером 2 через интерфейс в сети vboxnet2. На виртуальной машине AstraLinux-02 настроить виртуальный интерфейс таким образом, чтобы он получил настройки конфигурации по DHCP из сети NAT и получил доступ в сеть Интернет.
8. На всех маршрутизаторах настройте протокол динамической маршрутизации OSPF или RIP (тип используемого протокола назначается преподавателем).
9. Выделен диапазон IPv6 адресов FD00:<YEAR>:<MONTH>::/64 (дата рождения). На маршрутизаторе Mikrotik-03 создать DHCP сервер для распределения префиксов IPv6 из этого диапазона.
10. На маршрутизаторе Mikrotik-03 из созданного пула адресов настроить IPv6 адрес на интерфейс в VLAN с номером 3 с трансляцией префикса. Убедиться, что хост сконфигурировал себе адрес из транслируемого диапазона.
11. На маршрутизаторе Mikrotik-01 настроить DHCP клиент так, чтобы он получил префикс для распределения. Из полученного пула IPv6 адресов назначить адрес на интерфейс сетевого моста и настроить распространение префикса. На виртуальных машинах Astra Linux настроить автоматическую конфигурацию IPv6 адресов.

12. Настроить маршрутизацию для IPv6 таким образом, чтобы пинговались виртуальные машины и host-машина.
13. На виртуальной машине AstraLinux-02 проверить настройки DNS клиента. Убедиться, что запросы по умолчанию передаются на DNS с адресом 8.8.8.8.
14. Используя консольные утилиты, с узла AstraLinux-02 найти всю возможную информацию о DNS-зоне csc.sibsutis.ru, IPv4 имени ans.csc.sibsutis.ru, IPv4 адресе домена mail.ru и обо всех IP адресах, найденных для домена mail.ru.

Выполнение работы

1

Чтобы избежать конфликтов, на имеющихся адаптерах vboxnet 0-2 установил IP-адреса по умолчанию:

```
VBoxManage hostonlyif ipconfig vboxnet0 --ip=192.168.56.1 --  
netmask=255.255.255.0
```

```
VBoxManage hostonlyif ipconfig vboxnet1 --ip=192.168.57.1 --  
netmask=255.255.255.0
```

```
VBoxManage hostonlyif ipconfig vboxnet2 --ip=192.168.58.1 --  
netmask=255.255.255.0
```

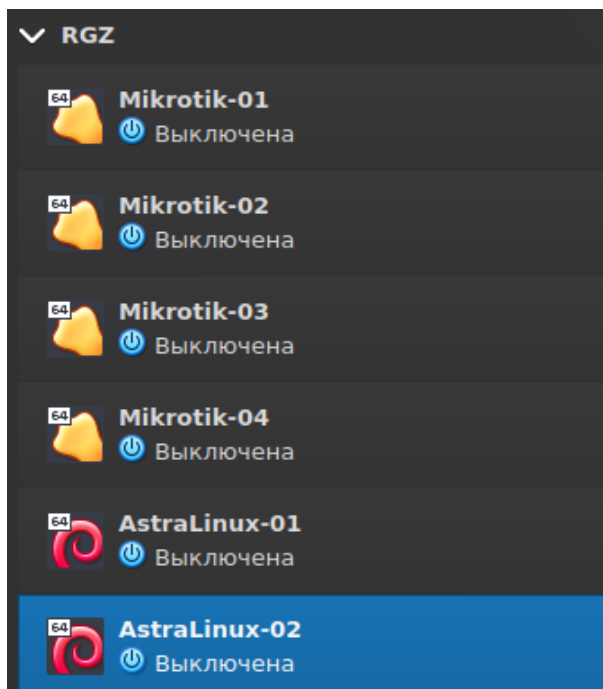
Также создал ещё два адаптера vboxnet3 и vboxnet4:

Имя	IPv4 префикс
vboxnet0	192.168.56.1/24
vboxnet1	192.168.57.1/24
vboxnet2	192.168.58.1/24
vboxnet3	192.168.59.1/24
vboxnet4	192.168.60.1/24

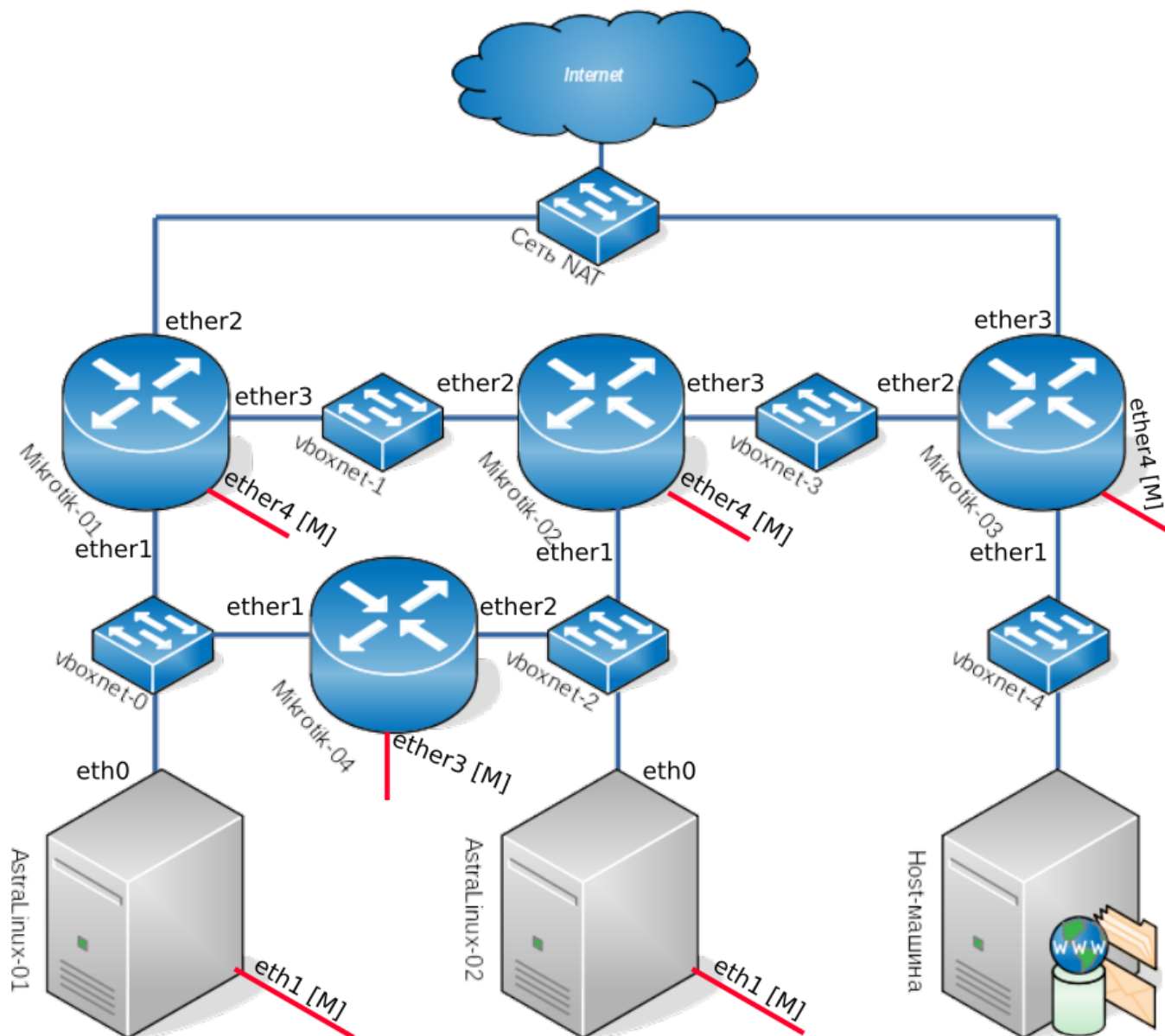
Также создал сеть NAT и отключил ей DHCP-сервер (временно):

Имя	IPv4 префикс
NatNetwork	10.0.2.0/24

Создал 4 новых машины с RouterOS и 2 новых машины с Astra Linux:



Настроил сетевую конфигурацию VirtualBox следующим образом ([M] - management interface):



Адаптеры Mikrotik имеют тип PCnet-FAST III и неразборчивый режим "Разрешить всё".

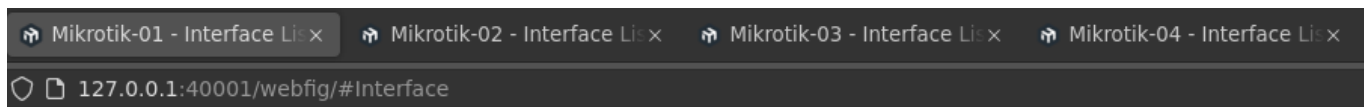
2

Всем узлам сети задал уникальное сетевое имя в соответствии с названиями VM. На Astra Linux менял по стандартной схеме - `hostnamectl` + редактирование `hosts` файла.

В соответствии с номерами VM настроил правила проброса портов по management интерфейсу: для роутеров это порты 40001, 40002, 40003, 40004 соответственно, для машин Astra это порты 40005, 40006.

Mikrotik-03 - Настройки						
Правила проброса портов						
Имя	Протокол	Адрес хоста	Порт хоста	Адрес гостя	Порт гостя	
Rule 1	TCP	127.0.0.1	40003		80	

На всех роутерах выключил DHCP-клиент с номером 0 (`ip dhcp-client disable 0`) и добавил новый клиент для management интерфейса (`ip dhcp-client add interface=etherX add-default-route=no`). Доступ к веб-панелям роутеров из браузера появился:



AstraLinux-01 - Настройки						
Правила проброса портов						
Имя	Протокол	Адрес хоста	Порт хоста	Адрес гостя	Порт гостя	
Rule 1	TCP	127.0.0.1	40005		22	

На обоих астрах на интерфейсе eth1 включил DHCP-клиент. Также на обеих машинах сгенерировал приватный `mng` и публичный `mng.pub` ключи командой `ssh-keygen`, с помощью команд `scp -P 40005 owner@127.0.0.1:mng mngX` загрузил приватные ключи на хост в директорию `~/.ssh`, затем на Astra переместил публичный ключ в директорию `~/.ssh`. Командой `cat ~/.ssh/mng.pub >> ~/.ssh/authorized_keys && chmod 600 ~/.ssh/authorized_keys` добавил публичный ключ в список авторизованных.

После этого SSH-сервер на астре продолжает принимать вход по паролю, необходимо это отключить. В файле конфигурации `/etc/ssh/sshd_config` изменю значение параметра `PasswordAuthentication` на `no` и перезапущу SSH-сервер командой `sudo systemctl restart sshd.service`. На хосте загружу ключи в SSH-агента командой `ssh-add ~/.ssh/mng1 ~/.ssh/mng2`.

Подключение по SSH к астрам теперь работает по ключам:

```
lostie@chasm:~$ ssh owner@127.0.0.1 -p 40005
You have new mail.
Last login: Fri May 12 20:09:01 2023 from 10.0.3.2
[20:12:56 #1] owner@AstraLinux-01:~$ exit
ВЫХОД
Connection to 127.0.0.1 closed.
```

3

На каждом Mikrotik в разделе Bridge создал сетевой мост bridge1 с протоколом по умолчанию RSTP. Во вкладке Ports добавляю к этому мосту рабочие порты (то есть все интерфейсы, кроме management).

На Mikrotik 01-03:

	#	Interface	Bridge	Horiz...	Trust...	Priority (hex)	Path Cost	PVID
- D	0	ether1	bridge1		no	80	10	1
- D	1	ether2	bridge1		no	80	10	1
- D	2	ether3	bridge1		no	80	10	1

На Mikrotik-04:

	#	Interface	Bridge	Horiz...	Trust...	Priority (hex)	Path Cost	PVID
- D	0	ether1	bridge1		no	80	10	1
- D	1	ether2	bridge1		no	80	10	1

Роли портов:

Mikrotik-01: ether1 - root port, ether2 - designated port, ether3 - designated port.

Mikrotik-02: ether1 - root port, ether2 - alternate port, ether3 - designated port.

Mikrotik-03: ether1 - designated port, ether2 - alternate port, ether3 - root port.

Mikrotik-04: ether1 - designated port, ether2 - designated port.

Корневой мост:

Mikrotik-04: root bridge.

Чтобы корневым мостом стал bridge1 на Mikrotik-02, на нём устанавливаю значение Priority 0x7000, а на bridge1 на Mikrotik-04 устанавливаю Priority = 0x7500.

Отлично, теперь bridge1 на Mikrotik-02 стал Root Bridge, а bridge1 на Mikrotik-04 стал его "заместителем":

Root Bridge	<input checked="" type="checkbox"/>
Root Bridge ID	7998.08:00:27:E1:8B:97
Regional Root Bridge ID	0.00:00:00:00:00:00

4

Выделен диапазон 10.10.6.0/24. Чтобы в каждой подсети адресовалось до 6 узлов, в ней должны быть доступны 8 адресов (1 на адрес сети и 1 на broadcast), то есть свободными в маске должны остаться 3 бита. Таким образом, маска становится 29 бит или 255.255.255.248.

Network Address	Usable Host Range	Broadcast Address:
10.10.6.0	10.10.6.1 - 10.10.6.6	10.10.6.7
10.10.6.8	10.10.6.9 - 10.10.6.14	10.10.6.15
10.10.6.16	10.10.6.17 - 10.10.6.22	10.10.6.23
10.10.6.24	10.10.6.25 - 10.10.6.30	10.10.6.31
10.10.6.32	10.10.6.33 - 10.10.6.38	10.10.6.39
10.10.6.40	10.10.6.41 - 10.10.6.46	10.10.6.47
10.10.6.48	10.10.6.49 - 10.10.6.54	10.10.6.55
10.10.6.56	10.10.6.57 - 10.10.6.62	10.10.6.63
10.10.6.64	10.10.6.65 - 10.10.6.70	10.10.6.71
10.10.6.72	10.10.6.73 - 10.10.6.78	10.10.6.79
10.10.6.80	10.10.6.81 - 10.10.6.86	10.10.6.87
10.10.6.88	10.10.6.89 - 10.10.6.94	10.10.6.95
10.10.6.96	10.10.6.97 - 10.10.6.102	10.10.6.103
10.10.6.104	10.10.6.105 - 10.10.6.110	10.10.6.111
10.10.6.112	10.10.6.113 - 10.10.6.118	10.10.6.119
10.10.6.120	10.10.6.121 - 10.10.6.126	10.10.6.127
10.10.6.128	10.10.6.129 - 10.10.6.134	10.10.6.135
10.10.6.136	10.10.6.137 - 10.10.6.142	10.10.6.143
10.10.6.144	10.10.6.145 - 10.10.6.150	10.10.6.151
10.10.6.152	10.10.6.153 - 10.10.6.158	10.10.6.159
10.10.6.160	10.10.6.161 - 10.10.6.166	10.10.6.167
10.10.6.168	10.10.6.169 - 10.10.6.174	10.10.6.175
10.10.6.176	10.10.6.177 - 10.10.6.182	10.10.6.183
10.10.6.184	10.10.6.185 - 10.10.6.190	10.10.6.191
10.10.6.192	10.10.6.193 - 10.10.6.198	10.10.6.199
10.10.6.200	10.10.6.201 - 10.10.6.206	10.10.6.207
10.10.6.208	10.10.6.209 - 10.10.6.214	10.10.6.215
10.10.6.216	10.10.6.217 - 10.10.6.222	10.10.6.223
10.10.6.224	10.10.6.225 - 10.10.6.230	10.10.6.231
10.10.6.232	10.10.6.233 - 10.10.6.238	10.10.6.239
10.10.6.240	10.10.6.241 - 10.10.6.246	10.10.6.247
10.10.6.248	10.10.6.249 - 10.10.6.254	10.10.6.255

Выберу первый диапазон 10.10.6.1 - 10.10.6.6 и присвою их интерфейсам виртуальных машин.

Mikrotik-01: 10.10.6.1 <- bridge1

Mikrotik-02: 10.10.6.2 <- bridge1

Mikrotik-03: 10.10.6.3 <- bridge1

Mikrotik-04: 10.10.6.4 <- bridge1

AstraLinux-01: 10.10.6.5 <- eth0

AstraLinux-02: 10.10.6.6 <- eth0

С каждого устройства проверю пинг до всех остальных:

Mikrotik-01:

```
[admin@Mikrotik-01] > ping count=2 10.10.6.2
```

Columns: SEQ, HOST, SIZE, TTL, TIME

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.2	56	64	932us
1	10.10.6.2	56	64	394us

```
[admin@Mikrotik-01] > ping count=2 10.10.6.3
```

Columns: SEQ, HOST, SIZE, TTL, TIME

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.3	56	64	1ms412us
1	10.10.6.3	56	64	464us

```
[admin@Mikrotik-01] > ping count=2 10.10.6.4
```

Columns: SEQ, HOST, SIZE, TTL, TIME

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.4	56	64	1ms270us
1	10.10.6.4	56	64	590us

```
[admin@Mikrotik-01] > ping count=2 10.10.6.5
```

Columns: SEQ, HOST, SIZE, TTL, TIME

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.5	56	64	1ms10us
1	10.10.6.5	56	64	811us

```
[admin@Mikrotik-01] > ping count=2 10.10.6.6
```

Columns: SEQ, HOST, SIZE, TTL, TIME

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.6	56	64	791us
1	10.10.6.6	56	64	673us

Mikrotik-02:

```
[admin@Mikrotik-02] > ping count=2 10.10.6.1
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.1	56	64	250us
1	10.10.6.1	56	64	372us

```
[admin@Mikrotik-02] > ping count=2 10.10.6.3
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.3	56	64	625us
1	10.10.6.3	56	64	473us

```
[admin@Mikrotik-02] > ping count=2 10.10.6.4
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.4	56	64	662us
1	10.10.6.4	56	64	359us

```
[admin@Mikrotik-02] > ping count=2 10.10.6.5
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.5	56	64	678us
1	10.10.6.5	56	64	719us

```
[admin@Mikrotik-02] > ping count=2 10.10.6.6
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.6	56	64	500us
1	10.10.6.6	56	64	414us

Mikrotik-03:

```
[admin@Mikrotik-03] > ping count=2 10.10.6.1
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.1    56   64  507us
  1  10.10.6.1    56   64  770us
```

```
[admin@Mikrotik-03] > ping count=2 10.10.6.2
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.2    56   64  344us
  1  10.10.6.2    56   64  373us
```

```
[admin@Mikrotik-03] > ping count=2 10.10.6.4
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.4    56   64  1ms114us
  1  10.10.6.4    56   64  534us
```

```
[admin@Mikrotik-03] > ping count=2 10.10.6.5
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.5    56   64  869us
  1  10.10.6.5    56   64  849us
```

```
[admin@Mikrotik-03] > ping count=2 10.10.6.6
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.6    56   64  447us
  1  10.10.6.6    56   64  544us
```

Mikrotik-04:

```
[admin@Mikrotik-04] > ping count=2 10.10.6.1
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.1    56   64  488us
  1  10.10.6.1    56   64  808us

[admin@Mikrotik-04] > ping count=2 10.10.6.2
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.2    56   64  419us
  1  10.10.6.2    56   64  476us

[admin@Mikrotik-04] > ping count=2 10.10.6.3
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.3    56   64  615us
  1  10.10.6.3    56   64  590us

[admin@Mikrotik-04] > ping count=2 10.10.6.5
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.5    56   64  415us
  1  10.10.6.5    56   64  387us

[admin@Mikrotik-04] > ping count=2 10.10.6.6
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.6    56   64  361us
  1  10.10.6.6    56   64  349us
```

AstraLinux-01:

```
[22:52:19 #8] owner@AstraLinux-01:~$ ping -c 2 -q 10.10.6.1
PING 10.10.6.1 (10.10.6.1) 56(84) bytes of data.

--- 10.10.6.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.831/0.909/0.987/0.078 ms
[22:52:33 #9] owner@AstraLinux-01:~$ ping -c 2 -q 10.10.6.2
PING 10.10.6.2 (10.10.6.2) 56(84) bytes of data.

--- 10.10.6.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.409/0.471/0.533/0.062 ms
[22:52:36 #10] owner@AstraLinux-01:~$ ping -c 2 -q 10.10.6.3
PING 10.10.6.3 (10.10.6.3) 56(84) bytes of data.

--- 10.10.6.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.804/0.817/0.830/0.013 ms
[22:52:38 #11] owner@AstraLinux-01:~$ ping -c 2 -q 10.10.6.4
PING 10.10.6.4 (10.10.6.4) 56(84) bytes of data.

--- 10.10.6.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1025ms
rtt min/avg/max/mdev = 0.315/0.346/0.378/0.036 ms
[22:52:39 #12] owner@AstraLinux-01:~$ ping -c 2 -q 10.10.6.6
PING 10.10.6.6 (10.10.6.6) 56(84) bytes of data.

--- 10.10.6.6 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.759/0.802/0.845/0.043 ms
```

AstraLinux-02:

```
[22:51:32 #1] owner@AstraLinux-02:~$ ping -c 2 -q 10.10.6.1
PING 10.10.6.1 (10.10.6.1) 56(84) bytes of data.

--- 10.10.6.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.772/1.329/1.886/0.557 ms
[22:54:33 #2] owner@AstraLinux-02:~$ ping -c 2 -q 10.10.6.2
PING 10.10.6.2 (10.10.6.2) 56(84) bytes of data.

--- 10.10.6.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1021ms
rtt min/avg/max/mdev = 0.353/0.623/0.894/0.271 ms
[22:54:35 #3] owner@AstraLinux-02:~$ ping -c 2 -q 10.10.6.3
PING 10.10.6.3 (10.10.6.3) 56(84) bytes of data.

--- 10.10.6.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.706/0.994/1.283/0.290 ms
[22:54:37 #4] owner@AstraLinux-02:~$ ping -c 2 -q 10.10.6.4
PING 10.10.6.4 (10.10.6.4) 56(84) bytes of data.

--- 10.10.6.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.399/0.572/0.746/0.175 ms
[22:54:39 #5] owner@AstraLinux-02:~$ ping -c 2 -q 10.10.6.5
PING 10.10.6.5 (10.10.6.5) 56(84) bytes of data.

--- 10.10.6.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 0.577/0.626/0.675/0.049 ms
```

Связь между всеми узлами в сети присутствует, как и ожидалось.

5

В VirtualBox для **сети** NAT задал адрес сети 10.10.6.8/29 (второй диапазон) и включил DHCP-сервер:

```
VBoxManage natnetwork modify --dhcp=on --netname=NatNetwork --
network=10.10.6.8/29
```

На всех роутерах Mikrotik в разделе Bridge включил VLAN Filtering для bridge1. Таким образом во вкладке VLANs явно стала видна сеть VLAN с PVID 1. Сеть VLAN 2, которую я создам, будет использоваться для доступа в сеть NAT.

На Mikrotik-01 во вкладке Bridge -> Ports у порта ether2 сменю PVID на 2 (т.к. он относится только к одной сети VLAN).

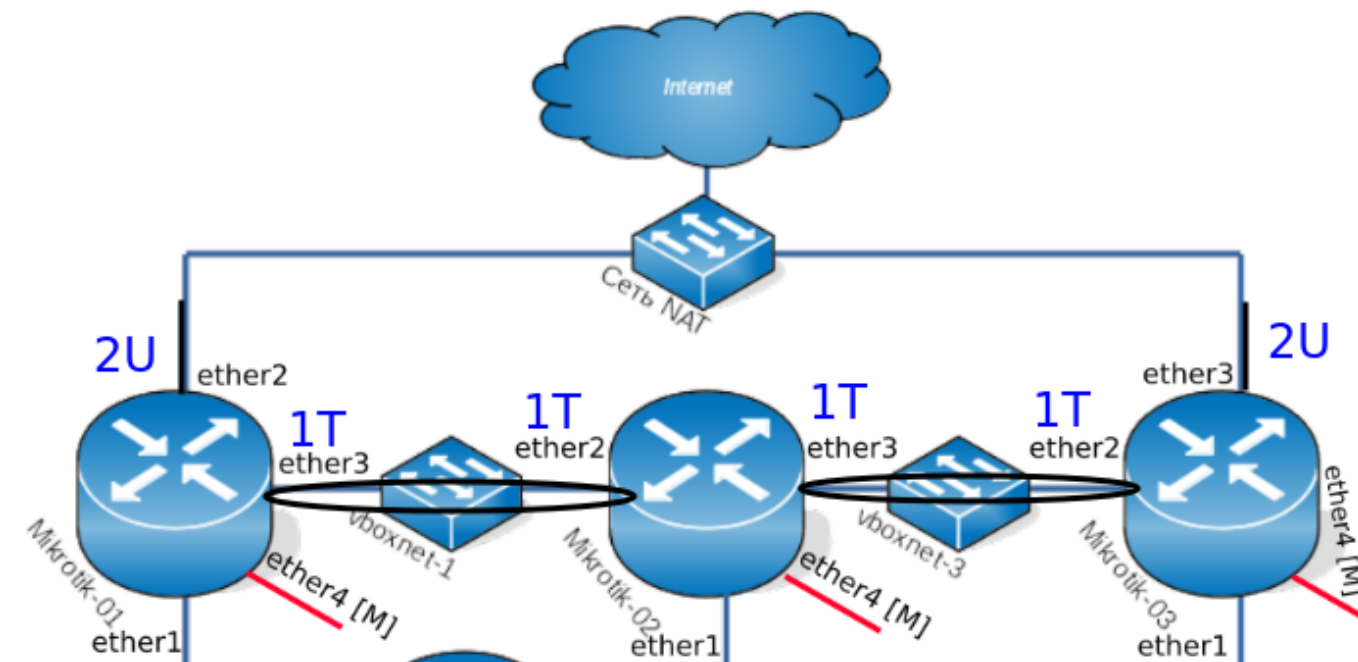
Затем во вкладке Bridge -> VLANs сделаю bridge1, ether3 тегированными, ether2 нетегированным.

На Mikrotik-02 во вкладке Bridge -> VLANs создам VLAN с ID=2 и сделаю bridge1, ether2, ether3 тегированными.

На Mikrotik-03 во вкладке Bridge -> Ports у порта ether3 сменю PVID на 2 (т.к. он относится только к одной сети VLAN).

Затем во вкладке Bridge -> VLANs сделаю bridge1, ether2 тегированными, ether3 нетегированным.

Получается такая схема ([T]agged / [U]ntagged):



Mikrotik-01:

#	Interface	Bridge	Horiz...	Trust...	Priority (hex)	Path Cost	PVID
0	ether1	bridge1		no	80	10	1
1	ether2	bridge1		no	80	10	2
2	ether3	bridge1		no	80	10	1


▲ Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	2	bridge1, ether3	ether2
bridge1	1		bridge1, ether1, ether3

Mikrotik-02:

#	Interface	Bridge	Horiz...	Trust...	Priority (hex)	Path Cost	PVID
0	 ether1	bridge1		no	80	10	1
1	 ether2	bridge1		no	80	10	1
2	 ether3	bridge1		no	80	10	1

▲ Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	2	bridge1, ether2, ether3	
bridge1	1		bridge1, ether1, ether2, ether3

Mikrotik-03:

#	Interface	Bridge	Horiz...	Trust...	Priority (hex)	Path Cost	PVID
0	 ether1	bridge1		no	80	10	1
1	 ether2	bridge1		no	80	10	1
2	 ether3	bridge1		no	80	10	2

▲ Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	2	bridge1, ether2	ether3
bridge1	1		bridge1, ether1, ether2

Чтобы получать IP-адрес из другого диапазона, на каждом Mikrotik-01, Mikrotik-02, Mikrotik-03 нужно настроить виртуальный интерфейс для моста:

Enabled	<input checked="" type="checkbox"/>
Name	<input type="text" value="vlan2"/>
Type	VLAN
MTU	<input type="text" value="1500"/>
Actual MTU	
L2 MTU	
MAC Address	
ARP	<input type="text" value="enabled"/>
ARP Timeout	▼
VLAN ID	<input type="text" value="2"/>
Interface	<input type="text" value="bridge1"/>
Use Service Tag	<input type="checkbox"/>

Затем создать DHCP-клиент для этого интерфейса:

Status: stopped	
Enabled	<input checked="" type="checkbox"/>
Interface	<input type="text" value="vlan2"/>
Use Peer DNS	<input checked="" type="checkbox"/>
Use Peer NTP	<input checked="" type="checkbox"/>
Add Default Route	<input type="text" value="yes"/>
DHCP Options	<div> <div>▼</div> <div>hostname</div> <div>▼</div> </div> <div> <div>▼</div> <div>clientid</div> <div>▼</div> </div> <div>▲</div>
Default Route Distance	<input type="text" value="1"/>

Полученные адреса (успешно пингуются между собой, пакеты содержат тег):

Mikrotik-01: 10.10.6.13/29

Mikrotik-02: 10.10.6.14/29

Mikrotik-03: 10.10.6.12/29

6

Для адресации узлов в VLAN 3 использую третий диапазон IPv4 адресов из п.4, то есть 10.10.6.17/29 - 10.10.6.22/29. Так как виртуальных машин 6 и доступных адресов тоже 6, адаптеру vboxnet4 на хосте придётся назначить адрес сети, то есть 10.10.6.16/29. В теории это не должно привести к проблемам.

```
VBoxManage hostonlyif ipconfig vboxnet4 --ip=10.10.6.16 --  
netmask=255.255.255.248
```

На Mikrotik-01 ether1 и ether3 в созданной VLAN 3 будут тегированными:

▲ Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	3	bridge1, ether1, ether3	
bridge1	2	bridge1, ether3	ether2
bridge1	1		bridge1, ether1, ether3

На Mikrotik-02 ether1, ether2 и ether3 в созданной VLAN 3 будут тегированными:

▲ Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	3	bridge1, ether1, ether2, ether3	
bridge1	2	bridge1, ether2, ether3	
bridge1	1		bridge1, ether1, ether2, ether3

На Mikrotik-03 ether2 в созданной VLAN 3 будет тегированным, а ether1 нетегированным, т.к. соединяется с хостом:

▲ Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	3	bridge1, ether2	ether1
bridge1	2	bridge1, ether2	ether3
bridge1	1		bridge1, ether1, ether2

Также на Mikrotik-03 нужно сменить PVID порта ether1 на 3. Он "смотрит" только в сеть с хостом, значит не будет получать тегированный трафик.

На Mikrotik-04 ether1 и ether2 в созданной VLAN 3 будут тегированными:

▲ Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	3	bridge1, ether1, ether2	
bridge1	1		bridge1, ether1, ether2

На каждом роутере создам интерфейс vlan3 (виртуальный интерфейс для bridge1) и задам ему соответствующий статический адрес:

Mikrotik-01: 10.10.6.17/29

Enabled	<input checked="" type="checkbox"/>
Address	<input type="text" value="10.10.6.17/29"/>
Network	▼
Interface	<input type="text" value="vlan3"/>

Mikrotik-02: 10.10.6.18/29

Mikrotik-03: 10.10.6.19/29

Mikrotik-04: 10.10.6.20/29

На машинах Astra создам виртуальный интерфейс для обработки тегированного трафика в VLAN3. Этим интерфейсам назначу адреса 10.10.6.21/29 (AstraLinux-01) и 10.10.6.22/29 (AstraLinux-02). Весь направляемый в eth0.3 трафик будет проходить через главный интерфейс eth0, но с тегом VLAN.

На AstraLinux-01:

```

sudo vi /etc/network/interfaces.d/eth0:
...
auto eth0.3
iface eth0.3 inet static
    address 10.10.6.21
    netmask 255.255.255.248

sudo ifup eth0.3

```

На AstraLinux-02 то же самое, но с адресом .22.

Проверю пинг с каждой машины до всех остальных:

Mikrotik-01:

```
[admin@Mikrotik-01] > ping count=2 10.10.6.16
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.16     56   64   945us
  1  10.10.6.16     56   64   776us

[admin@Mikrotik-01] > ping count=2 10.10.6.18
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.18     56   64   427us
  1  10.10.6.18     56   64   328us

[admin@Mikrotik-01] > ping count=2 10.10.6.19
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.19     56   64   977us
  1  10.10.6.19     56   64   607us

[admin@Mikrotik-01] > ping count=2 10.10.6.20
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.20     56   64   712us
  1  10.10.6.20     56   64   621us

[admin@Mikrotik-01] > ping count=2 10.10.6.21
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.21     56   64   1ms121us
  1  10.10.6.21     56   64   1ms121us

[admin@Mikrotik-01] > ping count=2 10.10.6.22
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.22     56   64   830us
  1  10.10.6.22     56   64   756us
```

Mikrotik-02:

```
[admin@Mikrotik-02] > ping count=2 10.10.6.16
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.16      56    64  1ms374us
  1  10.10.6.16      56    64  666us

[admin@Mikrotik-02] > ping count=2 10.10.6.17
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.17      56    64  433us
  1  10.10.6.17      56    64  556us

[admin@Mikrotik-02] > ping count=2 10.10.6.19
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.19      56    64  952us
  1  10.10.6.19      56    64  356us

[admin@Mikrotik-02] > ping count=2 10.10.6.20
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.20      56    64  486us
  1  10.10.6.20      56    64  295us

[admin@Mikrotik-02] > ping count=2 10.10.6.21
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.21      56    64  682us
  1  10.10.6.21      56    64  644us

[admin@Mikrotik-02] > ping count=2 10.10.6.22
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST          SIZE  TTL  TIME
  0  10.10.6.22      56    64  314us
  1  10.10.6.22      56    64  229us
```

Mikrotik-03:

```
[admin@Mikrotik-03] > ping count=2 10.10.6.16
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.16	56	64	290us
1	10.10.6.16	56	64	368us

```
[admin@Mikrotik-03] > ping count=2 10.10.6.17
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.17	56	64	676us
1	10.10.6.17	56	64	709us

```
[admin@Mikrotik-03] > ping count=2 10.10.6.18
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.18	56	64	454us
1	10.10.6.18	56	64	305us

```
[admin@Mikrotik-03] > ping count=2 10.10.6.20
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.20	56	64	1ms154us
1	10.10.6.20	56	64	617us

```
[admin@Mikrotik-03] > ping count=2 10.10.6.21
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.21	56	64	893us
1	10.10.6.21	56	64	794us

```
[admin@Mikrotik-03] > ping count=2 10.10.6.22
```

```
Columns: SEQ, HOST, SIZE, TTL, TIME
```

SEQ	HOST	SIZE	TTL	TIME
0	10.10.6.22	56	64	880us
1	10.10.6.22	56	64	735us

Mikrotik-04:

```
[admin@Mikrotik-04] > ping count=2 10.10.6.16
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.16   56   64  957us
  1  10.10.6.16   56   64  856us

[admin@Mikrotik-04] > ping count=2 10.10.6.17
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.17   56   64  856us
  1  10.10.6.17   56   64  739us

[admin@Mikrotik-04] > ping count=2 10.10.6.18
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.18   56   64  360us
  1  10.10.6.18   56   64  449us

[admin@Mikrotik-04] > ping count=2 10.10.6.19
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.19   56   64  772us
  1  10.10.6.19   56   64  566us

[admin@Mikrotik-04] > ping count=2 10.10.6.21
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.21   56   64  428us
  1  10.10.6.21   56   64  356us

[admin@Mikrotik-04] > ping count=2 10.10.6.22
Columns: SEQ, HOST, SIZE, TTL, TIME
SEQ  HOST      SIZE  TTL  TIME
  0  10.10.6.22   56   64  369us
  1  10.10.6.22   56   64  316us
```

AstraLinux-01:

```
[17:13:49 #21] owner@AstraLinux-01:~$ ping -q -c 2 10.10.6.16
PING 10.10.6.16 (10.10.6.16) 56(84) bytes of data.

--- 10.10.6.16 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.990/1.057/1.124/0.067 ms
[17:14:01 #22] owner@AstraLinux-01:~$ ping -q -c 2 10.10.6.17
PING 10.10.6.17 (10.10.6.17) 56(84) bytes of data.

--- 10.10.6.17 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.614/0.776/0.939/0.164 ms
[17:14:03 #23] owner@AstraLinux-01:~$ ping -q -c 2 10.10.6.18
PING 10.10.6.18 (10.10.6.18) 56(84) bytes of data.

--- 10.10.6.18 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1030ms
rtt min/avg/max/mdev = 0.479/0.535/0.592/0.061 ms
[17:14:05 #24] owner@AstraLinux-01:~$ ping -q -c 2 10.10.6.19
PING 10.10.6.19 (10.10.6.19) 56(84) bytes of data.

--- 10.10.6.19 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.866/0.923/0.980/0.057 ms
[17:14:08 #25] owner@AstraLinux-01:~$ ping -q -c 2 10.10.6.20
PING 10.10.6.20 (10.10.6.20) 56(84) bytes of data.

--- 10.10.6.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.390/0.449/0.509/0.063 ms
[17:14:10 #26] owner@AstraLinux-01:~$ ping -q -c 2 10.10.6.22
PING 10.10.6.22 (10.10.6.22) 56(84) bytes of data.

--- 10.10.6.22 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1024ms
rtt min/avg/max/mdev = 0.687/0.732/0.777/0.045 ms
[17:14:13 #27] owner@AstraLinux-01:~$ |
```

AstraLinux-02:


```
[17:14:27 #24] owner@AstraLinux-02:~$ ping -q -c 2 10.10.6.16
PING 10.10.6.16 (10.10.6.16) 56(84) bytes of data.

--- 10.10.6.16 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.738/0.773/0.808/0.035 ms
[17:14:35 #25] owner@AstraLinux-02:~$ ping -q -c 2 10.10.6.17
PING 10.10.6.17 (10.10.6.17) 56(84) bytes of data.

--- 10.10.6.17 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.656/0.710/0.765/0.060 ms
[17:14:37 #26] owner@AstraLinux-02:~$ ping -q -c 2 10.10.6.18
PING 10.10.6.18 (10.10.6.18) 56(84) bytes of data.

--- 10.10.6.18 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1018ms
rtt min/avg/max/mdev = 0.379/0.395/0.412/0.025 ms
[17:14:39 #27] owner@AstraLinux-02:~$ ping -q -c 2 10.10.6.19
PING 10.10.6.19 (10.10.6.19) 56(84) bytes of data.

--- 10.10.6.19 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.583/0.621/0.659/0.038 ms
[17:14:41 #28] owner@AstraLinux-02:~$ ping -q -c 2 10.10.6.20
PING 10.10.6.20 (10.10.6.20) 56(84) bytes of data.

--- 10.10.6.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1025ms
rtt min/avg/max/mdev = 0.429/0.454/0.480/0.033 ms
[17:14:44 #29] owner@AstraLinux-02:~$ ping -q -c 2 10.10.6.21
PING 10.10.6.21 (10.10.6.21) 56(84) bytes of data.

--- 10.10.6.21 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1032ms
rtt min/avg/max/mdev = 0.652/0.654/0.657/0.025 ms
```

Все адреса успешно пингуются между собой, значит всё настроено правильно. Пакеты в сети vboxnet3 (для примера) действительно имеют тег с PVID 3, в сети vboxnet4 этот тег снимается.

```

25 18:11:58,... 10.10.6.17      10.10.6.16      ICMP    Echo (ping) request  i
26 18:11:58,... 10.10.6.17      10.10.6.16      ICMP    Echo (ping) request  i
27 18:11:58,... 10.10.6.16      10.10.6.17      ICMP    Echo (ping) reply    i
28 18:11:58,... PcsCompu_b2:7e:6a  Spinning_topo_450c:25  STP     DST: 01:00:5e:00:00:00  RST: 00000000

```

```

▶ Frame 27: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface vboxnet3, id 0
▶ Ethernet II, Src: 0a:00:27:00:00:04 (0a:00:27:00:00:04), Dst: PcsCompu_b2:7e:6a (08:00:27:b2:7e:6a)
▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3
    000. .... = Priority: Best Effort (default) (0)
    ...0 .... = DEI: Ineligible
    .... 0000 0000 0011 = ID: 3
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.10.6.16, Dst: 10.10.6.17
▶ Internet Control Message Protocol

```

Сейчас доступа в Интернет у AstraLinux-01 нет, это можно проверить пингом до адреса 8.8.8.8 через eth0:

```
[02:08:01 #6] owner@AstraLinux-01:~$ ping -I eth0 8.8.8.8 -q -c 6
PING 8.8.8.8 (8.8.8.8) from 10.10.6.5 eth0: 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5115ms
```

Нужно сделать так, чтобы Mikrotik-01 транслировал адреса для AstraLinux-01 из нетегируемой сети. Для этого на Mikrotik-01 в разделе IP -> Firewall -> NAT создам новое правило:

Enabled	<input checked="" type="checkbox"/>
Chain	srcnat
Src. Address	<input type="checkbox"/> 10.10.6.5
Dst. Address	▼
Src. Address List	▼
Dst. Address List	▼
Protocol	▼
Src. Port	▼
Dst. Port	▼
Any. Port	▼
In. Interface	▼
Out. Interface	<input type="checkbox"/> vlan2

Цепочка srcnat, правило действует только для узла 10.10.6.5 (AstraLinux-01 в VLAN 1), перенаправляет на интерфейс vlan2, который имеет доступ в Интернет.

Action	masquerade
Log	<input checked="" type="checkbox"/>
Log Prefix	▼
To Ports	▼

Firewall NAT *action=masquerade* is a unique subversion of *action=srcnat*, it was designed for specific use in situations when public IP can randomly change, for example, DHCP server change assigned IP or PPPoE tunnel after disconnect gets different IP, in short - **when public IP is dynamic**.

Правило создано, но для AstraLinux-01 оно пока не работает из-за её настроек default route. Дополню файл `/etc/network/interfaces.d/eth1` строками переназначения маршрута по умолчанию:

```
iface eth1 inet dhcp
    up ip route del default
    up ip route add default via 10.10.6.1 dev eth0
```

После перезапуска машины можно пробовать пинговать 8.8.8.8:

```
[02:56:47 #8] owner@AstraLinux-01:~$ ip r
default via 10.10.6.1 dev eth0
10.0.3.0/24 dev eth1 proto kernel scope link src 10.0.3.15
10.10.6.0/29 dev eth0 proto kernel scope link src 10.10.6.5
10.10.6.16/29 dev eth0.3 proto kernel scope link src 10.10.6.21
[02:56:49 #9] owner@AstraLinux-01:~$ 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=100 time=63.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=100 time=61.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=100 time=60.6 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 60.668/62.096/63.690/1.255 ms
```

Google DNS пингуется успешно. Можно даже "дёргать" сайты curl'ом:

```
[02:58:33 #13] owner@AstraLinux-01:~$ curl https://ipwho.de
5. [REDACTED].222
RU / Russia / Novosibirsk
AS34757 / Sibirskie Seti Ltd.

curl/7.52.1

--- help ---
curl 4.ipwho.de/ip --> 1.2.3.4
curl 6.ipwho.de/ip --> 2001:1234:1234::1234
curl ipwho.de/json

ipwho.de proudly presented by adminForge.de. GeoLite2 data created by MaxMind.com.
```

Теперь нужно обеспечить доступ к VLAN 2 через интерфейс в сети vboxnet2. Для этого на Mikrotik-02 в разделе Bridge -> VLANs -> 2 добавлю порт ether1 в тегированные:

Enabled	<input checked="" type="checkbox"/>
Bridge	bridge1 ▾
VLAN IDs	▾ 2 ▴
Tagged	▾ bridge1 ▴
	▾ ether2 ▴
	▾ ether3 ▴
	▾ ether1 ▴
Untagged	▾
Current Tagged	bridge1 ether2 ether3

Теперь на AstraLinux-02 создам виртуальный интерфейс eth0.2 для доступа в сеть NAT:

```

sudo vi /etc/network/interfaces.d/eth0:
...

auto eth0.2
    iface eth0.2 inet dhcp

...

sudo ifup eth0.2

```

В данной ситуации интерфейс не сможет получить адрес, потому что DHCP-сервер с адресом .11 в сети NAT раздал адреса .12, .13, .14 микротикам, а сама сеть NAT заняла адрес .9 под маршрут по умолчанию и .10 адрес. Свободных адресов не осталось "физически":

```

home ▶ lostie ▶ .config ▶ VirtualBox ▶ NatNetwork-Dhcpd.config
1  <?xml version="1.0"?>
2  <DHCPServer networkName="NatNetwork" trunkType="whatever" IPAddress="10.10.6.11"
4  lowerIP="10.10.6.12" upperIP="10.10.6.14" leasesFilename="/home/lostie/.config/VirtualBox/
4  NatNetwork-Dhcpd.leases" networkMask="255.255.255.248">
3    <Options>
4    <Option name="1" encoding="0" value="255.255.255.248"/>
5    <Option name="3" encoding="0" value="10.10.6.9"/>
6    <Option name="6" encoding="0" value="192.168.1.1"/>
7    <Option name="15" encoding="0" value="lan"/>
8    </Options>
9  </DHCPServer>

```

Если сделать Release адреса на Mikrotik-03, то AstraLinux-02 получает адрес по DHCP, но тогда его не получает Mikrotik-03.

На всех роутерах создам такой OSPFv2 Instance:

Enabled	<input checked="" type="checkbox"/>
Name	ospf-instance-v2
Version	2 ▾
VRF	main ▾
Router ID	main ▾
Routing Table	▾
Originate Default	▾
Redistribute	<div> <input checked="" type="checkbox"/> connected <input checked="" type="checkbox"/> static </div> <div> <input type="checkbox"/> rip <input checked="" type="checkbox"/> ospf </div> <div> <input type="checkbox"/> bgp <input type="checkbox"/> vpn </div> <div> <input type="checkbox"/> dhcp <input type="checkbox"/> fantasy </div> <div> <input type="checkbox"/> modem <input type="checkbox"/> copy </div>

Чтобы они заработали, нужно также создать на всех роутерах зону с ID 6.6.6.6 и такой Interface Template (на Mikrotik-04 без vlan2):








Enabled	<input checked="" type="checkbox"/>
Name	ospf-area-v2
Instance	ospf-instance-v2 ▾
Area ID	6.6.6.6
Type	default ▾

Enabled	<input checked="" type="checkbox"/>
Interfaces	<div> <div>▾</div> <div>bridge1 ▾</div> <div>▲</div> </div> <div> <div>▾</div> <div>vlan2 ▾</div> <div>▲</div> </div> <div> <div>▾</div> <div>vlan3 ▾</div> <div>▲</div> </div>
Area	▾
Networks	▾
Network Type	broadcast ▾

Всё заработало, для примера таблица маршрутов с Mikrotik-01:

	▲ Dst. Address	Gateway	Distance
DAd	0.0.0.0/0	10.10.6.9	1
DAo+	10.0.4.0/24	10.10.6.4%bridge1	110
DAo+	10.0.4.0/24	10.10.6.20%vlan3	110
DAC	10.0.5.0/24	%ether4	
Do	10.0.5.0/24	10.10.6.18%vlan3	110
Do	10.0.5.0/24	10.10.6.13%vlan2	110
Do	10.0.5.0/24	10.10.6.2%bridge1	110
Do	10.0.5.0/24	10.10.6.19%vlan3	110
Do	10.0.5.0/24	10.10.6.3%bridge1	110
DAC	10.10.6.0/29	%bridge1	
DAC	10.10.6.8/29	%vlan2	
DAC	10.10.6.16/29	%vlan3	

Таблица соседей для Mikrotik-02:

▲ Instance	Area	Address	State	State Changes
 ospf-instance-v2	ospf-area-v2	10.10.6.12	Full	6
 ospf-instance-v2	ospf-area-v2	10.10.6.4	Full	5
 ospf-instance-v2	ospf-area-v2	10.10.6.3	Full	5
 ospf-instance-v2	ospf-area-v2	10.10.6.1	TwoWay	2
 ospf-instance-v2	ospf-area-v2	10.10.6.20	Full	6
 ospf-instance-v2	ospf-area-v2	10.10.6.19	Full	5
 ospf-instance-v2	ospf-area-v2	10.10.6.17	TwoWay	2

9

Выделен диапазон IPv6 адресов fd00:2003:3::/48. На Mikrotik-03 требуется создать DHCP-сервер, который будет распределять префиксы из данного диапазона. Сервер будет раздавать префиксы с маской 64.

В разделе IPv6 -> Pool создал новый пул адресов fd00:2003:3::/48:

Name	<input type="text" value="pool1"/>
Prefix	<input type="text" value="fd00:2003:3::/48"/>
Prefix Length	<input type="text" value="64"/>

В IPv6 -> DHCP Server на интерфейсе bridge1 создал новый сервер, который будет использовать данный пул адресов:

Enabled	<input checked="" type="checkbox"/>
Name	server1
Interface	bridge1 v
Address Pool6	pool1 v
Lease Time	3d 00:00:00
DHCP Options	v
Use RADIUS	<input type="checkbox"/>

10

На Mikrotik-03 в IPv6 -> Addresses добавлю статический адрес из пула pool1 (скриншот старый). Он будет находиться в сети vlan3 и "предлагать" префикс остальным участникам сети.

Enabled	<input checked="" type="checkbox"/>
Address	::/64
From Pool	ipv6-server-bdpool v
Interface	vlan3 v
EUI64	<input checked="" type="checkbox"/>
Advertise	<input checked="" type="checkbox"/>

Ожидается, что теперь хост получит site-local IPv6 адрес на адаптере vboxnet4. Проверю, так ли это:

```
7: vboxnet4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:00:27:00:00:04 brd ff:ff:ff:ff:ff:ff
    inet 10.10.6.16/29 brd 10.10.6.23 scope global vboxnet4
        valid_lft forever preferred_lft forever
    inet6 fd00:2003:3:0:da63:ae4e:4d89:8dab/64 scope global temporary dynamic
        valid_lft 599930sec preferred_lft 81264sec
    inet6 fd00:2003:3:0:800:27ff:fe00:4/64 scope global dynamic mngtmpaddr
        valid_lft 2591573sec preferred_lft 604373sec
    inet6 fe80::800:27ff:fe00:4/64 scope link
        valid_lft forever preferred_lft forever
```

Да, хост теперь имеет IPv6 адрес в сети VLAN 3. Один EUI64 (внутренний) и один сгенерированный временно (внешний). Пинг до Mikrotik-03 проходит:

```
lostie@chasm:~$ ping fd00:2003:3:0:a00:27ff:fe85:ffae -q -c 3
PING fd00:2003:3:0:a00:27ff:fe85:ffae(fd00:2003:3:0:a00:27ff:fe85:ffae)

--- fd00:2003:3:0:a00:27ff:fe85:ffae ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.154/0.268/0.468/0.141 ms
```

11

На Mikrotik-01 в разделе IPv6 -> DHCP Client создам новый клиент, который будет получать **префикс** от сервера:

Enabled	<input checked="" type="checkbox"/>
Interface	bridge1 ▾
Request	<input type="checkbox"/> info <input type="checkbox"/> address <input checked="" type="checkbox"/> prefix
Pool Name	dpool1
Pool Prefix Length	64
Prefix Hint	▲ ::/0
Use Peer DNS	<input checked="" type="checkbox"/>
Use Interface DUID	<input type="checkbox"/>
Rapid Commit	<input checked="" type="checkbox"/>
Add Default Route	<input type="checkbox"/>

После нажатия Apply префикс получен:

Prefix	fd00:2003:3:1::/64
Prefix Expires After	2d 23:49:43

В разделе IPv6 -> Addresses добавлю адрес из этого пула, который будет распространяться остальным участникам сети:

Enabled	<input checked="" type="checkbox"/>
Address	::/64
From Pool	dpool1
Interface	bridge1
EUI64	<input checked="" type="checkbox"/>
Advertise	<input checked="" type="checkbox"/>

<Здесь я перезапустил все машины, потому что сломался VirtualBox DHCPv4 Server. Теперь он снова работает>

Полученный адрес:

	▲ Address	From Pool	Interface	Advertise
LD	⬇ fe80::a00:27ff:feb2:7e6a/64		vlan2	no
LD	⬇ fe80::a00:27ff:feb2:7e6a/64		bridge1	no
LD	⬇ fe80::a00:27ff:fe0c:4dfb/64		ether4	no
LD	⬇ fe80::a00:27ff:feb2:7e6a/64		vlan3	no
	⬇ fd00:2003:3:1:a00:27ff:feb2:7e6a/64	dpool1	bridge1	yes

Машина AstraLinux-01 получила IPv6 адрес на eth0 автоматически:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc pfifo_fast state UP
    link/ether 08:00:27:21:df:17 brd ff:ff:ff:ff:ff:ff
    inet 10.10.6.5/29 brd 10.10.6.7 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fd00:2003:3:1:a00:27ff:fe21:df17/64 scope global mngtmpaddr dynamic
        valid_lft 2591883sec preferred_lft 604683sec
    inet6 fe80::a00:27ff:fe21:df17/64 scope link
        valid_lft forever preferred_lft forever
```

Машина AstraLinux-02 получила IPv6 адрес на eth0 автоматически:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc pfifo_fast state UP
    link/ether 08:00:27:86:42:cf brd ff:ff:ff:ff:ff:ff
    inet 10.10.6.6/29 brd 10.10.6.7 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fd00:2003:3:1:a00:27ff:fe86:42cf/64 scope global mngtmpaddr dynamic
        valid_lft 2591881sec preferred_lft 604681sec
    inet6 fe80::a00:27ff:fe86:42cf/64 scope link
        valid_lft forever preferred_lft forever
```

Машины и роутер пингуются между собой, пункт выполнен.

Если сейчас попробовать с хоста пропинговать адрес AstraLinux-01 на eth0 (или обратно), то ничего не выйдет:

```
lostie@chase:~$ ping fd00:2003:3:1:a00:27ff:fe21:df17 -I vboxnet4 -q -c 3
PING fd00:2003:3:1:a00:27ff:fe21:df17(fd00:2003:3:1:a00:27ff:fe21:df17) from fd00:2003:3:0:da63:ae4e:4d89:8dab vboxnet4
: 56 data bytes

--- fd00:2003:3:1:a00:27ff:fe21:df17 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2030ms
```

Чтобы решить данную проблему, нужно настроить такой OSPFv3 Instance на каждом маршрутизаторе:

Enabled	<input checked="" type="checkbox"/>
Name	<input type="text" value="ospf-instance-v3"/>
Version	<input type="text" value="3"/>
VRF	<input type="text" value="main"/>
Router ID	<input type="text" value="main"/>
Routing Table	<input type="text" value=""/>
Originate Default	<input type="text" value=""/>
Redistribute	<div><div><input checked="" type="checkbox"/> connected</div><div><input type="checkbox"/> rip</div><div><input type="checkbox"/> bgp</div><div><input type="checkbox"/> dhcp</div><div><input type="checkbox"/> modem</div></div> <div><div><input checked="" type="checkbox"/> static</div><div><input checked="" type="checkbox"/> ospf</div><div><input type="checkbox"/> vpn</div><div><input type="checkbox"/> fantasy</div><div><input type="checkbox"/> copy</div></div>







Area:

Enabled	<input checked="" type="checkbox"/>
Name	<input type="text" value="ospf-area-v3"/>
Instance	<input type="text" value="ospf-instance-v3"/>
Area ID	<input type="text" value="6.6.6.6"/>
Type	<input type="text" value="default"/>

Interface Template:

Enabled	<input checked="" type="checkbox"/>
Interfaces	<div>bridge1 ▼ ▲</div> <div>vlan3 ▼ ▲</div>
Area	ospf-area-v3 ▼
Networks	▼
Network Type	broadcast ▼
Prefix List	▼
Instance ID	0

Теперь таблица соседей для Mikrotik-03 дополнилась данными записями:

D	 ospf-instance-v3	ospf-area-v3	fe80::a00:27ff:fe74:5714%bridge1	ExStart	3
D	 ospf-instance-v3	ospf-area-v3	fe80::a00:27ff:fee1:8b97%bridge1	TwoWay	2
D	 ospf-instance-v3	ospf-area-v3	fe80::a00:27ff:feb2:7e6a%bridge1	TwoWay	2
D	 ospf-instance-v3	ospf-area-v3	fe80::a00:27ff:fe74:5714%vlan3	ExStart	3
D	 ospf-instance-v3	ospf-area-v3	fe80::a00:27ff:fee1:8b97%vlan3	TwoWay	2
D	 ospf-instance-v3	ospf-area-v3	fe80::a00:27ff:feb2:7e6a%vlan3	TwoWay	2

Попробую пропинговать адрес хоста с AstraLinux-01:

```
[19:57:15 #10] owner@AstraLinux-01:~$ ping fd00:2003:3:4:a944:b19b:473f:932e -q -c 3
PING fd00:2003:3:4:a944:b19b:473f:932e(fd00:2003:3:4:a944:b19b:473f:932e) 56 data byt
--- fd00:2003:3:4:a944:b19b:473f:932e ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.930/1.424/2.119/0.507 ms
```

Пинг хоста с AstraLinux-02:

```
[19:56:35 #8] owner@AstraLinux-02:~$ ping -q -c 2 fd00:2003:3:4:a944:b19b:473f:932e
PING fd00:2003:3:4:a944:b19b:473f:932e(fd00:2003:3:4:a944:b19b:473f:932e) 56 data by
--- fd00:2003:3:4:a944:b19b:473f:932e ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.543/0.919/1.296/0.377 ms
```

Попытка ещё раз пропинговать AstraLinux-01 с хоста - успешно:

```
testlab@hass:~$ ping -I vboxnet4 -q -c 3 fd00:2003:3:1:a00:27ff:fe21:df17
PING fd00:2003:3:1:a00:27ff:fe21:df17(fd00:2003:3:1:a00:27ff:fe21:df17) from fd00:2003:3:4:a944:b19b:473f:932e vboxnet4
: 56 data bytes
--- fd00:2003:3:1:a00:27ff:fe21:df17 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.428/1.481/1.518/0.038 ms
```

Ожидаемое поведение достигнуто, пункт выполнен.

13

Проверю текущий DNS сервер, который используется на AstraLinux-02:

```
[20:07:05 #9] owner@AstraLinux-02:~$ systemd-resolve --status
Global
DNS Servers: 192.168.1.1
DNS Domain: lan
DNSSEC NTA: 10.in-addr.arpa
```

По умолчанию установлен DNS домашнего роутера, в файле **/etc/resolv.conf** поменяю его на Google DNS:

```
domain lan
search lan
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Затем перезапущу демон:

```
sudo systemctl restart systemd-resolved.service
```

Проверю DNS сервер теперь:

```
[20:16:06 #15] owner@AstraLinux-02:~$ systemd-resolve --status
Global
DNS Servers: 8.8.8.8
             8.8.4.4
DNS Domain: lan
DNSSEC NTA: 10.in-addr.arpa
```

14

Используя консольные утилиты, с узла AstraLinux-02 найти всю возможную информацию о DNS-зоне **csc.sibsutis.ru**, IPv4 имени **ans.csc.sibsutis.ru**, IPv4 адресе домена **mail.ru** и обо всех IP адресах, найденных для домена **mail.ru**.

На AstraLinux-02 установлю пакет **dnsutils**, затем запрошу всю доступную информацию о DNS-зонах домена **csc.sibsutis.ru**:

```
$ nslookup -q=any csc.sibsutis.ru 8.8.8.8
```

```
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
csc.sibsutis.ru
    origin = ns.csc.sibsutis.ru
    mail addr = root.csc.sibsutis.ru
    serial = 20
    refresh = 10800
    retry = 900
    expire = 604800
    minimum = 86400
csc.sibsutis.ru nameserver = ns.csc.sibsutis.ru.
csc.sibsutis.ru mail exchanger = 10 mx.yandex.net.
csc.sibsutis.ru text = "MS=ms84877494"
csc.sibsutis.ru text = "v=spf1 redirect=_spf.yandex.net"
csc.sibsutis.ru text = "yandex-verification: fd2cfd5e61ab13a5"
Name:   csc.sibsutis.ru
Address: 91.196.245.193
```

Нашлись NS, MX, A записи, а также некоторая текстовая информация.

Информация о IPv4 имени `ans.csc.sibsutis.ru`:

```
$ nslookup -q=A ans.csc.sibsutis.ru 8.8.8.8

Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   ans.csc.sibsutis.ru
Address: 1.1.1.1
```

IPv4 адрес: 1.1.1.1 (кстати, совпадает с DNS сервером Cloudflare).

Информация об IPv4 адресе домена **mail.ru**:

```
$ nslookup -q=A mail.ru 8.8.8.8

Server:      8.8.8.8
Address:     8.8.8.8#53
```

```
Non-authoritative answer:
Name:   mail.ru
Address: 217.69.139.200
Name:   mail.ru
Address: 94.100.180.201
Name:   mail.ru
Address: 94.100.180.200
Name:   mail.ru
Address: 217.69.139.202
```

Возвращается несколько адресов, это нормальное явление для балансировки нагрузки.

Также у этого домена есть IPv6 адрес:

```
$ nslookup -q=AAAA mail.ru 8.8.8.8

Server:           8.8.8.8
Address:          8.8.8.8#53

Non-authoritative answer:
Name:   mail.ru
Address: 2a00:1148:db00:0:b0b0::1
```

Вся нужная информация получена, пункт выполнен.

Все задания расчётно-графической работы успешно выполнены.