

Топология сети

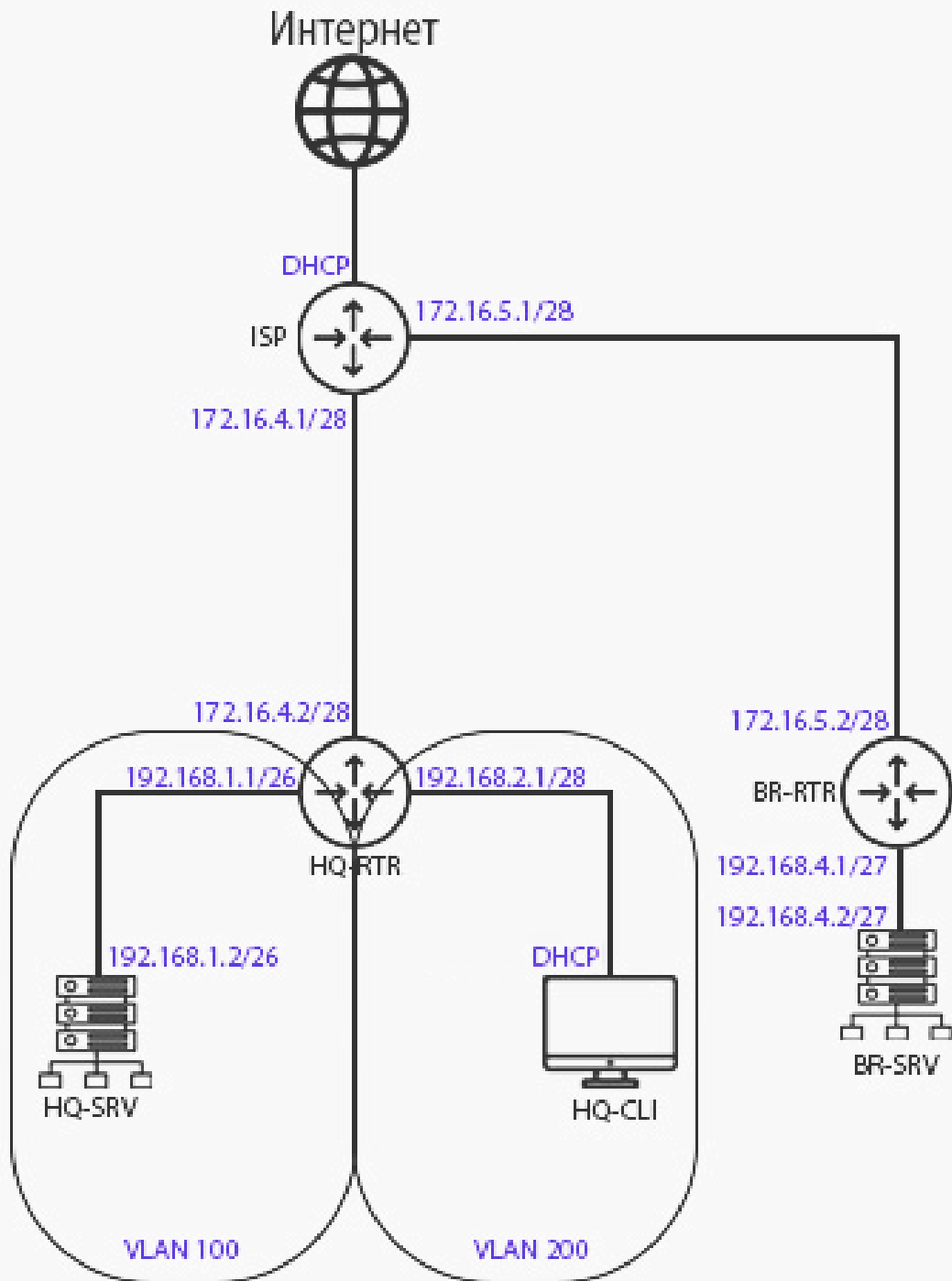


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска	VLAN	Подсеть	Шлюз
ISP	eth0 (к интернету)	DHCP	DHCP	-	DHCP	DHCP
	eth1 (к HQ-RTR)	172.16.4.1	255.255.255.240	-	172.16.4.0/28	-
	eth2 (к BR-RTR)	172.16.5.1	255.255.255.240	-	172.16.5.0/28	-
HQ-RTR	eth0 (к ISP)	172.16.4.2	255.255.255.240	-	172.16.4.0/28	172.16.4.1
	eth1 (Trunk)	-	-	Trunk	-	-
	eth1.100	192.168.1.1	255.255.255.192	100	192.168.1.0/26	-
	eth1.200	192.168.2.1	255.255.255.240	200	192.168.2.0/28	-
	eth1.999	192.168.3.1	255.255.255.248	999	192.168.3.0/29	-
	gre1 (IP туннель)	10.10.10.1	255.255.255.252	-	10.10.10.0/30	-
	enp0s3 (Trunk)	-	-	Trunk	-	-
HQ-SRV	enp0s3.100	192.168.1.2	255.255.255.192	100	192.168.1.0/26	192.168.1.1
HQ-CLI	enp0s3.200	192.168.2.2	255.255.255.240	200	192.168.2.0/28	192.168.2.1
BR-RTR	eth0 (к ISP)	172.16.5.2	255.255.255.240	-	172.16.5.0/28	172.16.5.1
	eth1 (к BR-SRV)	192.168.4.1	255.255.255.224	-	192.168.4.0/27	-
	gre1 (IP туннель)	10.10.10.2	255.255.255.252	-	10.10.10.0/30	-
BR-SRV	enp0s3 (к BR-RTR)	192.168.4.2	255.255.255.224	-	192.168.4.0/27	192.168.4.1

Версии дистрибутивов к соответствующим устройствам (ссылки):

ISP, HQ-RTR, BR-RTR –

https://dl.astralinux.ru/astra/stable/2.12_x86-64/iso/alce-2.12.46.6-17.04.2023_15.09.iso

HQ-SRV, BR-SRV –

https://download.basealt.ru/pub/distributions/ALTLinux/p10/images/server/x86_64/alt-server-10.2-x86_64.iso

HQ-CLI –

https://download.basealt.ru/pub/distributions/ALTLinux/p10/images/workstation/x86_64/alt-workstation-10.1-x86_64.iso

Таблица масок

Маска подсети	CIDR префикс	Всего IP адресов	Используемых IP адресов
255.255.255.255	/32	1	1
255.255.255.254	/31	2	0
255.255.255.252	/30	4	2
255.255.255.248	/29	8	6
255.255.255.240	/28	16	14
255.255.255.224	/27	32	30
255.255.255.192	/26	64	62
255.255.255.128	/25	128	126
255.255.255.0	/24	256	254
255.255.254.0	/23	512	510
255.255.252.0	/22	1024	1022
255.255.248.0	/21	2048	2046
255.255.240.0	/20	4096	4094
255.255.224.0	/19	8192	8190
255.255.192.0	/18	16384	16382
255.255.128.0	/17	32768	32766
255.255.0.0	/16	65536	65534
255.254.0.0	/15	131072	131070
255.252.0.0	/14	262144	262142
255.248.0.0	/13	524288	524286
255.240.0.0	/12	1048576	1048574
255.224.0.0	/11	2097152	2097150
255.192.0.0	/10	4194304	4194302
255.128.0.0	/9	8388608	8388606
255.0.0.0	/8	16777216	16777214
254.0.0.0	/7	33554432	33554430
252.0.0.0	/6	67108864	67108862
248.0.0.0	/5	134217728	134217726
240.0.0.0	/4	268435456	268435454
224.0.0.0	/3	536870912	536870910
192.0.0.0	/2	1073741824	1073741822
128.0.0.0	/1	2147483648	2147483646
0.0.0.0	/0	4294967296	4294967294

МОДУЛЬ №1

1. Произведите базовую настройку устройств

ВСЕ СЛЕДУЮЩИЕ НАСТРОЙКИ ПРОИЗВОДЯТСЯ ОТ root!!!

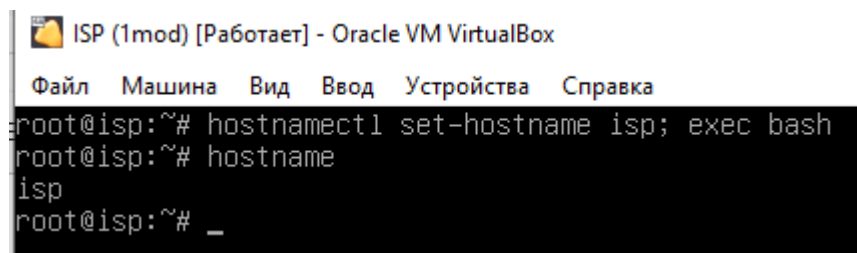
Команда для перехода в режим суперпользователя:

su - (ALT Linux)

sudo -i (ASTRA Linux)

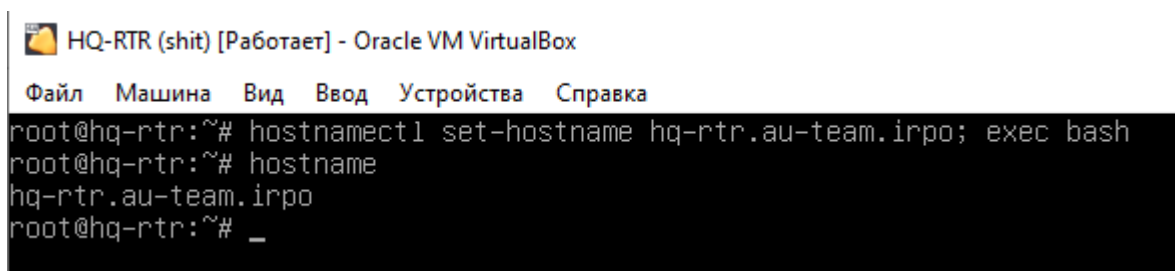
а) Настройте имена устройств согласно топологии. Используйте полное доменное имя.

Настроим имя на **ISP**:



```
ISP (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@isp:~# hostnamectl set-hostname isp; exec bash
root@isp:~# hostname
isp
root@isp:~# _
```

Настроим им на **HQ-RTR**:



```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@hq-rtr:~# hostnamectl set-hostname hq-rtr.au-team.irpo; exec bash
root@hq-rtr:~# hostname
hq-rtr.au-team.irpo
root@hq-rtr:~# _
```

АНАЛОГИЧНО НА ДРУГИХ УСТРОЙСТВАХ!

б) На всех устройствах необходимо сконфигурировать IPv4

Адресация на ISP:

Настраивать будем через следующую команду:

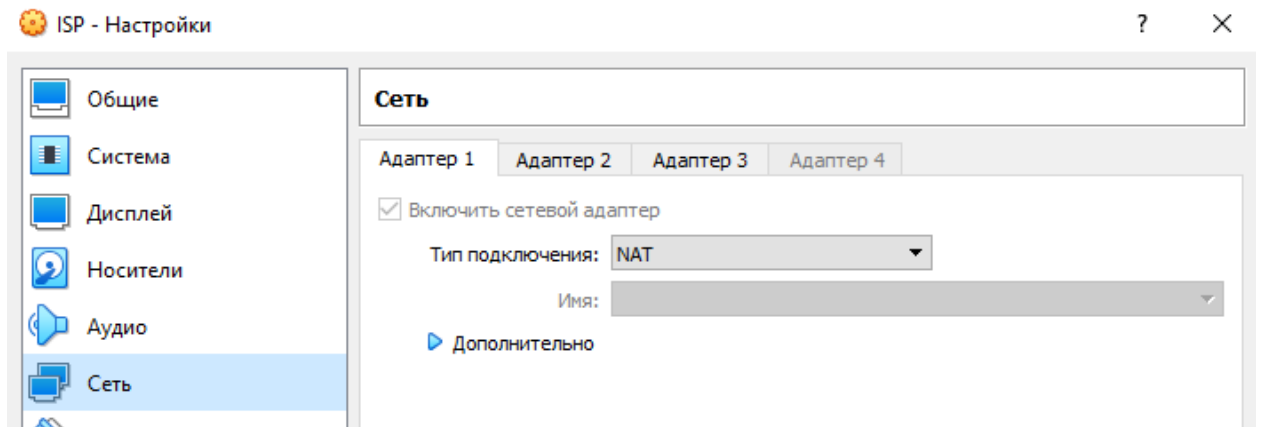
mcedit /etc/network/interfaces

```
alhome.zapto.org:7015 QEMU (ISP) - noVNC
/etc/network/interfaces [---] 25 L:[ 1+15 16/ 16] *(400 / 400b) <EOF>
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

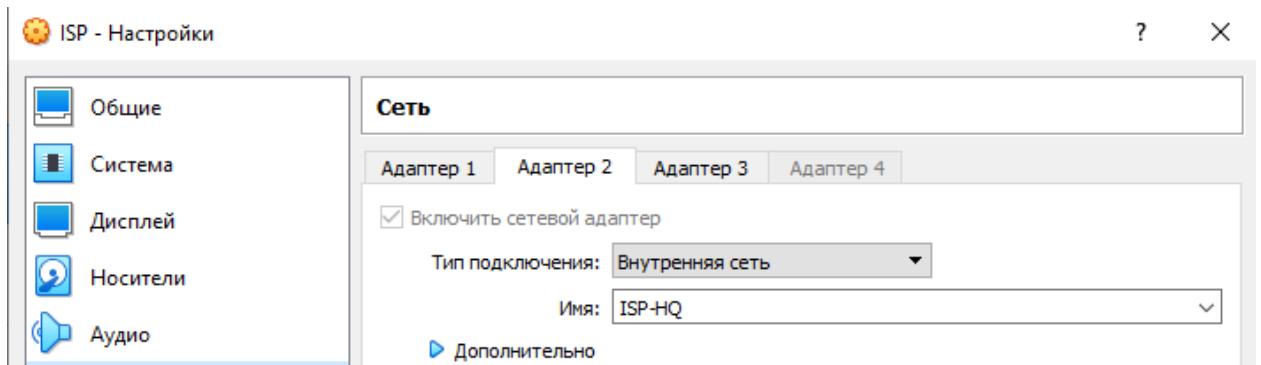
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
    iface eth0 inet dhcp
auto eth1
    iface eth1 inet static
    address 172.16.4.1/28
auto eth2
    iface eth2 inet static
    address 172.16.5.1/28_
```

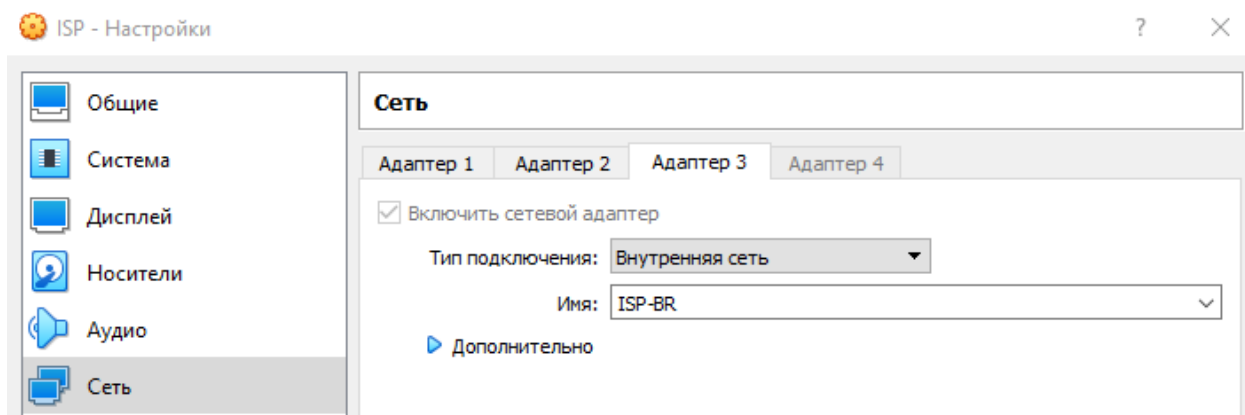
eth0 – интерфейс, подключенный к провайдеру (Интернет), должен быть по dhcp



eth1 – интерфейс, подключенный к ISP-HQ, должна быть настроена static (см. [Таблица адресации](#))



eth2 – интерфейс, подключенный к ISP-BR, должна быть настроена static (см. [Таблица адресации](#)).



Маска 255.255.255.240 (/28) была выбрана с условием, что сеть должна вмещать не более 32 хостов (см. [Таблица масок](#))

Из **mcedit** выходим нажатием **F2** для сохранения изменений и **F10** для выхода из него.

systemctl restart networking (перезапуск службы сети для применения изменений на Astra Linux)

systemctl restart network (тоже самое, только на Alt Linux)

Адресация на HQ-RTR:

Настраивать будем через следующую команду:

mcedit /etc/network/interfaces

```
QEMU (HQ-RTR2) - noVNC — Firefox Developer Edition
https://demo.peacedeath.su:7015/?console=kvm&novnc=1&vmid=10001&vmname=H
/etc/network/interfaces [-M--] 0 L:[ 1+35 36/ 36] *(680 / 680b) <EOF>
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# Example configuration
# auto eth0
# iface eth0 inet dhcp

auto eth0
<----->iface eth0 inet static
<----->address 172.16.4.2/28
<----->gateway 172.16.4.1

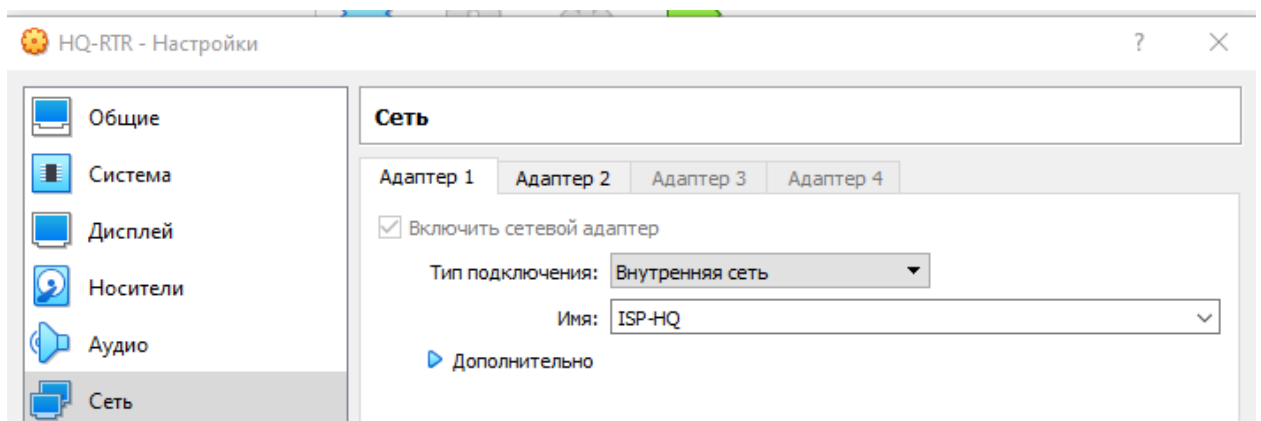
auto eth1
<----->iface eth1 inet manual

auto eth1.100
<----->iface eth1.100 inet static
<----->address 192.168.1.1/26
<----->vlan-raw-device eth1

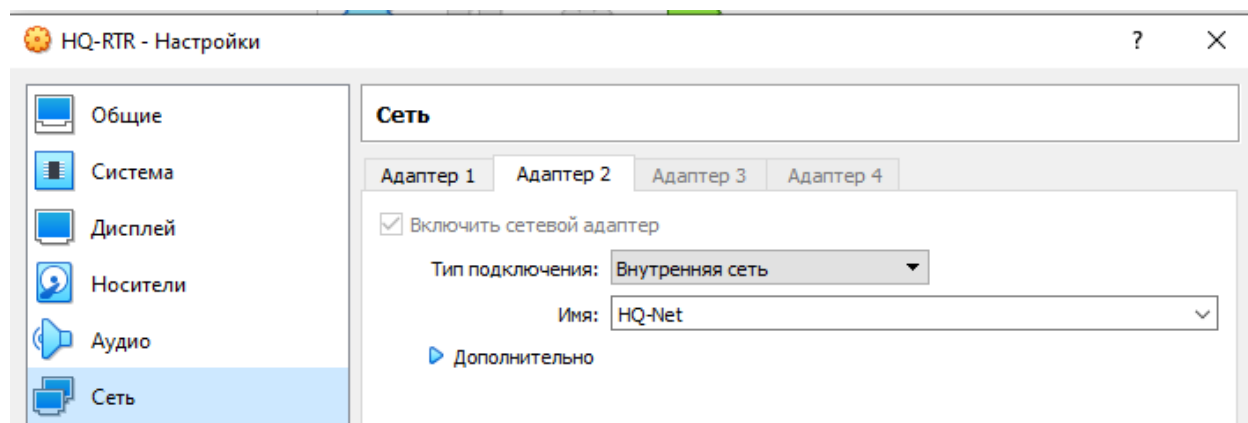
auto eth1.200
<----->iface eth1.200 inet static
<----->address 192.168.2.1/28
<----->vlan-raw-device eth1

auto eth1.999
<----->iface eth1.999 inet static
<----->address 192.168.3.1/29
<----->vlan-raw-device eth1
```

eth0 – интерфейс, подключенный к ISP-HQ, должна быть настроена static (см. [Таблица адресации](#)).



eth1 – интерфейс, подключенный к HQ-Net, должен быть настроен на manual, так как далее мы на нём будем настраивать VLAN`ы.



eth1.100 – интерфейс, подключенный к HQ-Net, должен быть настроен на static и настроен на VLAN 100 с маской /26. Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов.

eth1.200 – интерфейс, подключенный к HQ-Net, должен быть настроен на static и настроен на VLAN 200 с маской /28. Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 16 адресов.

eth1.999 – интерфейс, подключенный к HQ-Net, должен быть настроен на static и настроен на VLAN 999 с маской /29. Локальная сеть для управления(VLAN999) должна вмещать не более 8 адресов.

systemctl restart networking (перезапуск службы сети для применения изменений)

Адресация на BR-RTR:

Настраивать будем через следующую команду:

mcedit /etc/network/interfaces

```
alhome.zapto.org:7015 QEMU (BR-RTR) - noVNC
/etc/network/interfaces [-M--] 26 L:[ 1+14 15/ 15] *(389 / 389b) <EOF>
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
    iface eth0 inet static
    address 172.16.5.2/28
    gateway 172.16.5.1
auto eth1
    iface eth1 inet static
    address 192.168.4.1/27_
```


eth0 - интерфейс, подключенный к ISP-BR, должна быть настроена static (см. [Таблица адресации](#)).

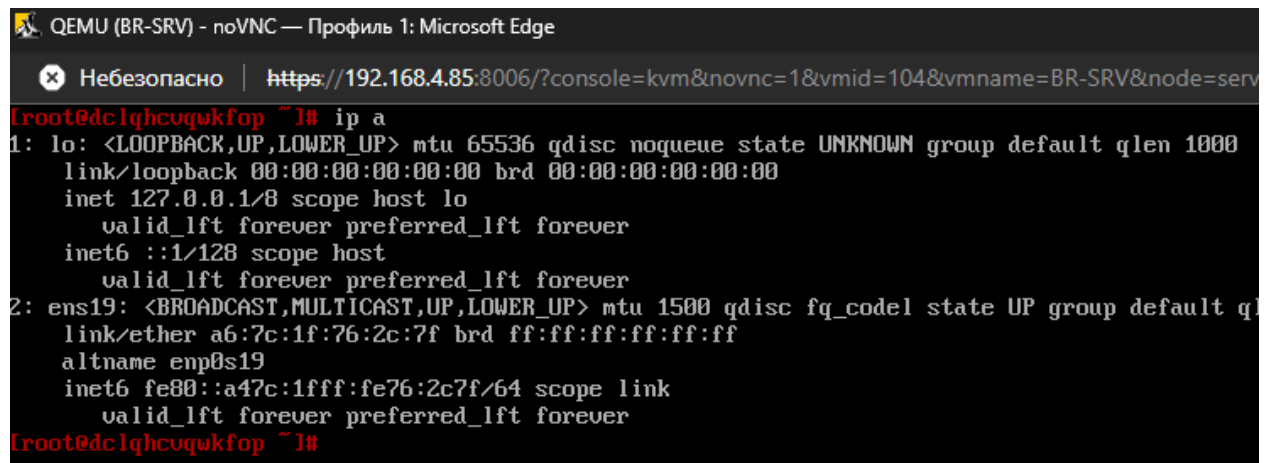
eth1 - интерфейс, подключенный к BR-Net, должна быть настроена static (см. [Таблица адресации](#)). Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов.

systemctl restart networking (перезапуск службы сети для применения изменений)!

Адресация на BR-SRV:

Альт отличается настройкой, как минимум тем, что в нём для настройки интерфейса нужно использовать отдельный каталог и внутри ещё каталоги, сейчас всё увидите, перейдём в каталог нужного нам интерфейса, но для начала посмотрим наши интерфейсы через команду:

ip a



```
QEMU (BR-SRV) - noVNC — Профиль 1: Microsoft Edge
https://192.168.4.85:8006/?console=kvm&tnovnc=1&vmid=104&vmname=BR-SRV&node=serv
[root@dc1qhcuvqwkfop ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether a6:7c:1f:76:2c:7f brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet6 fe80::a47c:1fff:fe76:2c7f/64 scope link
        valid_lft forever preferred_lft forever
[root@dc1qhcuvqwkfop ~]#
```

Видим, что нужный нам интерфейс имеет название **ens19** (У вас может отличаться, смотрите внимательно)

Переходим в каталог этого интерфейса:

cd /etc/net/ifaces/ens19

ls (выводим содержимое этого каталога)

```
QEMU (BR-SRV) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=104&vmname=BR-SRV&node=server&resize=off&
[root@dclqhcvgwkfop ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether a6:7c:1f:76:2c:7f brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet6 fe80::a47c:1fff:fe76:2c7f/64 scope link
        valid_lft forever preferred_lft forever
[root@dclqhcvgwkfop ~]# cd /etc/net/ifaces/ens19/
[root@dclqhcvgwkfop ens19]# ls
options
[root@dclqhcvgwkfop ens19]# _
```

Теперь будем настраивать файл, который здесь лежит, остальные создадим сами, приступаем.

Первым делом настраивать будем options через следующую команду:

mcedit /etc/net/ifaces/ens19/options

Если вы уже в каталоге, и делали всё по нашим шагам, то просто:

mcedit options

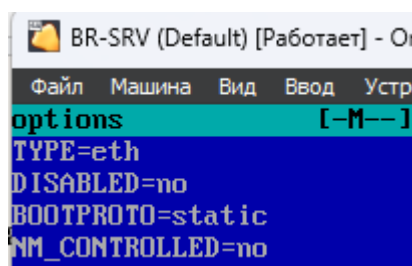
Приведём строки в файле к следующему виду:

TYPE=eth

DISABLED=no

BOOTPROTO=static

NM_CONTROLLED=no



СОХРАНЯЕМ ИЗМЕНЕНИЯ НАЖАТИЕМ КЛАВИШИ F2 И ЗАКРОЕМ КЛАВИШЕЙ F10, ЗАПОМНИТЕ, РЕБЯТИШКИ!!!

Далее настроим файл ipv4address (если его нет, то он создастся):

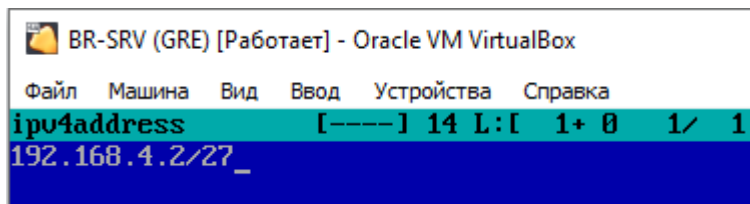
mcedit /etc/net/ifaces/ens19/ipv4address

Если вы уже в каталоге, и делали всё по нашим шагам, то просто:

mcedit ipv4address

Внесём туда следующую строку:

192.168.4.2/27 (см. [Таблица адресации](#))



Далее настроим файл `ipv4route`:

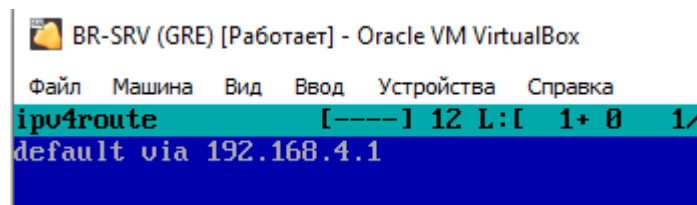
`mcedit /etc/net/iface/ens19/ipv4route`

Если вы уже в каталоге, и делали всё по нашим шагам, то просто:

`mcedit ipv4route`

Внесём туда следующую строку:

`default via 192.168.4.1` (см. [Таблица адресации](#))



Настройка адресации на **BR-SRV** завершена!

Перезапускаем службу `network` командой:

`systemctl restart network`

И смотрим ещё раз данные об интерфейсах командой:

`ip a`

```
[root@dclghcuqwkfop ens19]# mcedit ip4address
[root@dclghcuqwkfop ens19]# mcedit ip4route
[root@dclghcuqwkfop ens19]# systemctl restart network
[root@dclghcuqwkfop ens19]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether a6:7c:1f:76:2c:7f brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.4.2/27 brd 192.168.4.31 scope global ens19
        valid_lft forever preferred_lft forever
    inet6 fe80::a47c:1fff:fe76:2c7f/64 scope link tentative
        valid_lft forever preferred_lft forever
[root@dclghcuqwkfop ens19]#
```

Всё успешно! Но если у вас на Альт установлена служба **systemd-networkd**, то придётся вносить запись о перезагрузке службы **network** в **crontab**, как у нас. В Альт существует по умолчанию своя служба управлению сетью – это

Etcnet (никто не знает зачем, из-за неё как раз и приходится создавать отдельный каталог для интерфейсов), а вместе **Etcnet** и **systemd-networkd** работать не могут, поэтому вы можете просто отключить службу **systemd-networkd** командой:

systemctl disable --now systemd-networkd

!ВАЖНО! Это касается ТОЛЬКО СЕРВЕРОВ!!!

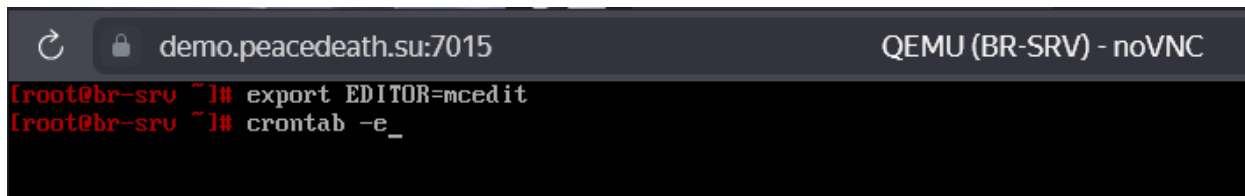
В ином случае, когда обе службы работают, нужно будет взаимодействовать с **crontab**, как это сделано далее, чтобы адрес не пропадал с интерфейса.

Делаем это следующим образом, пишем команду:

export EDITOR=mcedit

А затем:

crontab -e



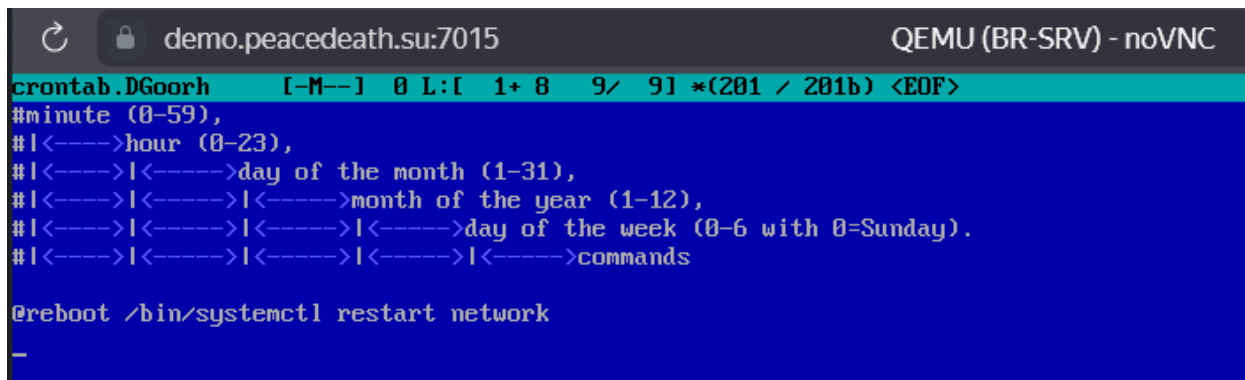
```
demo.peacedeath.su:7015 QEMU (BR-SRV) - noVNC
[root@br-srv ~]# export EDITOR=mcedit
[root@br-srv ~]# crontab -e_
```

Мы попадаем в конфиг, где указываются различные задачи, которые выполняются в назначенное время. В нашем случае нужно перезагружать службу **network** каждый раз после перезапуска системы.

Для этого мы в конце файла пишем следующее:

@reboot /bin/systemctl restart network

!ВАЖНО! Оставляем пустую строку после введенной строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу ПУСТУЮ СТРОКУ!



```
demo.peacedeath.su:7015 QEMU (BR-SRV) - noVNC
crontab.DGoorh [-M--] 0 L:[ 1+ 8 9/ 9] *(201 / 201b) <EOF>
#minute (0-59),
#|<---->hour (0-23),
#|<---->|<---->day of the month (1-31),
#|<---->|<---->|<---->month of the year (1-12),
#|<---->|<---->|<---->|<---->day of the week (0-6 with 0=Sunday).
#|<---->|<---->|<---->|<---->|<---->commands

@reboot /bin/systemctl restart network
-
```

Если всё сделано успешно, то появится следующее сообщение в консоли:

```
crontab: installing new crontab
[root@br-srv ~]#
```

И теперь вы можете перезагружать спокойно машину, не боясь, что адрес с интерфейса может пропасть. (ПО РФ 😊)

Настройка HQ-SRV и HQ-CLI производится по заданию позже!

2. Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.

Настройка производится встроенной службой, настроим зону на **HQ-SRV** следующей командой:

timedatectl set-timezone Asia/Barnaul

```
set-timezone set-timezone
[root@hq-srv ~]# timedatectl set-timezone Asia/Barnaul
```

И проверим правильность настройки:

timedatectl status

```
[root@hq-srv ~]# timedatectl set-timezone Asia/Barnaul
[root@hq-srv ~]# timedatectl status
          Local time: Thu 2024-09-12 21:20:56 +07
          Universal time: Thu 2024-09-12 14:20:56 UTC
             RTC time: Thu 2024-09-12 14:20:56
            Time zone: Asia/Barnaul (+07, +0700)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
[root@hq-srv ~]# _
```

Аналогично на других устройствах

Настройка часового пояса завершена завершена.

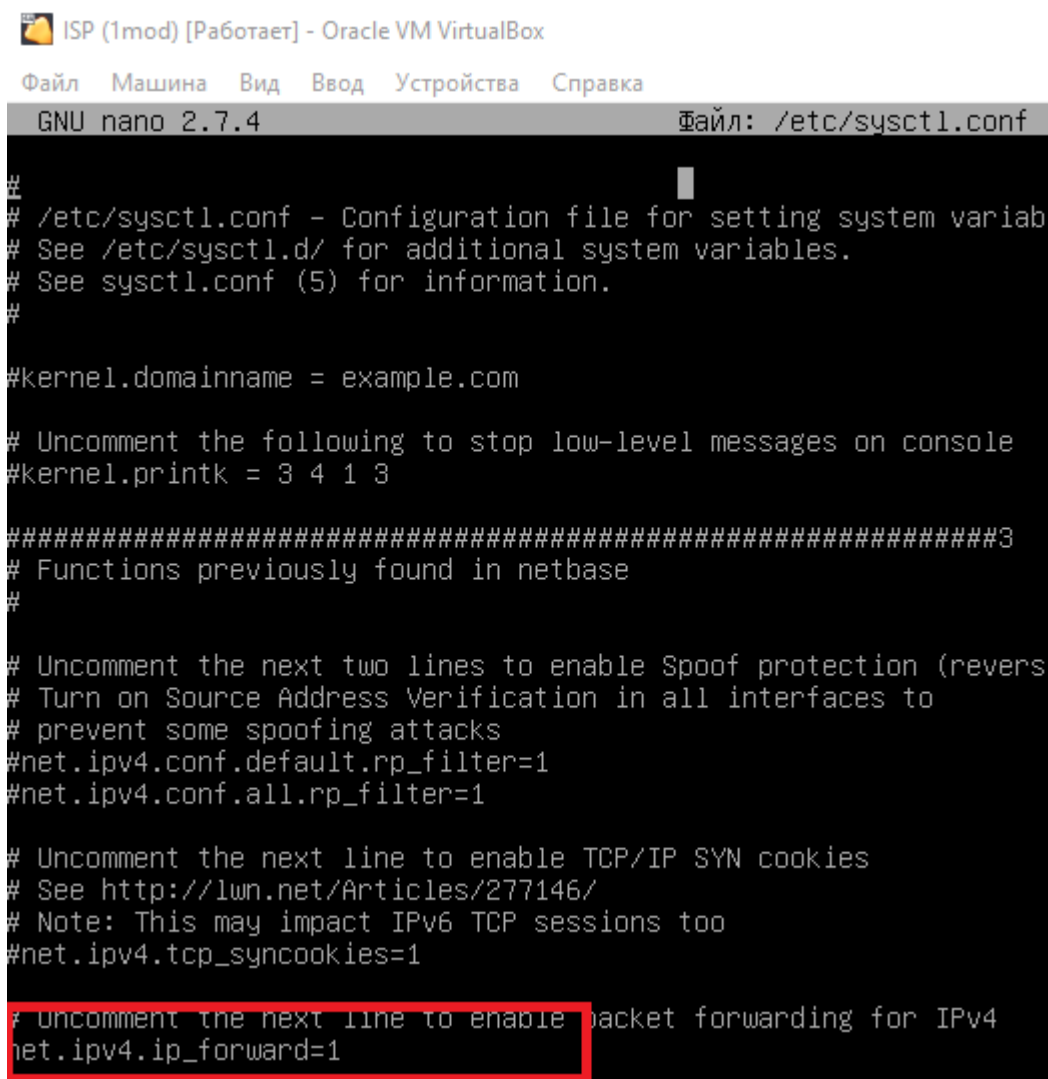
3. Настройка forward пакетов:

ISP:

mcedit /etc/sysctl.conf

Убрать знак комментария на этой строке:

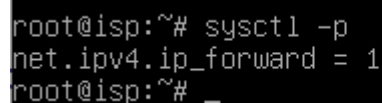
net.ipv4.ip_forward=1



```
ISP (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 2.7.4                               Файл: /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variab
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####3
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (revers
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

И применить изменения:

sysctl -p



```
root@isp:~# sysctl -p
net.ipv4.ip_forward = 1
root@isp:~# _
```

АНАЛОГИЧНО НА ДРУГИХ РОУТЕРАХ!

4. Настройка NAT:

ISP:

Пишем в консоль следующие команды:

iptables -t nat -A POSTROUTING -s 172.16.4.0/28 -o eth0 -j

MASQUERADE (Правило для доступа в интернет для устройств сети HQ)

iptables -t nat -A POSTROUTING -s 172.16.5.0/28 -o eth0 -j

MASQUERADE (Правило для доступа в интернет для устройств сети BR)

iptables -t nat -L (Вывод прописанных правил для nat)

```
root@isp:~# iptables -t nat -A POSTROUTING -s 172.16.4.0/28 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -A POSTROUTING -s 172.16.5.0/28 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE  all  --  172.16.4.0/28          anywhere
MASQUERADE  all  --  172.16.5.0/28          anywhere
root@isp:~# _
```

Сохраним наши правила, пишем в консоль следующую команду:

iptables-save > /root/rules

```
root@isp:~# iptables-save > /root/rules
root@isp:~# _
```

Запишем в **crontab** одну команду, чтобы при старте системы, правила загружались из файла, в котором они хранятся.

Пишем в консоль следующие команды:

export EDITOR=mcedit (Команда одноразовая, для комфортной работы с crontab её нужно писать каждый раз)

crontab -e

Добавляем в конец файла следующие строки:

@reboot /sbin/iptables-restore < /root/rules

!ВАЖНО! Оставляем пустую строку после введенной строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу **ПУСТУЮ СТРОКУ!**

```

/tmp/crontab.sA3xop/crontab [----] 0 L:[ 1+24 25/ 25] *(934 / 934
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#.
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
@reboot /sbin/iptables-restore < /root/rules
-

```

Перезагружаем машину и смотрим список правил, применяются ли они при запуске системы:

iptables -t nat -L

```

root@isp:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  172.16.4.0/28          anywhere
MASQUERADE all  --  172.16.5.0/28          anywhere
root@isp:~#

```


HQ-RTR:

Пишем в консоль следующие команды:

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/26 -o eth0 -j MASQUERADE
```

```
iptables -t nat -A POSTROUTING -s 192.168.2.0/28 -o eth0 -j MASQUERADE
```

```
iptables -t nat -A POSTROUTING -s 192.168.3.0/29 -o eth0 -j MASQUERADE
```

```
iptables -t nat -L
```

```
root@isp:~# iptables -t nat -A POSTROUTING -s 192.168.1.0/26 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -A POSTROUTING -s 192.168.2.0/28 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -A POSTROUTING -s 192.168.3.0/29 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  192.168.1.0/26       anywhere
MASQUERADE  all  --  192.168.2.0/28       anywhere
MASQUERADE  all  --  192.168.3.0/29       anywhere
root@isp:~#
```

Сохраним наши правила, пишем в консоль следующую команду:

```
iptables-save > /root/rules
```

```
root@hq-rtr:~# iptables-save > /root/rules
root@hq-rtr:~#
```

Запишем в **crontab** одну команду, чтобы при старте системы, правила загружались из файла, в котором они хранятся.

Пишем в консоль следующие команды:

```
export EDITOR=mcedit
```

```
crontab -e
```

Добавляем в конец файла следующие строки:

```
@reboot /sbin/iptables-restore < /root/rules
```

!ВАЖНО! Оставляем пустую строку после введённой строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу **ПУСТУЮ СТРОКУ!**

```
/tmp/crontab.sA3xop/crontab  [----]  0 L:[ 1+24 25/ 25] *(934 / 934
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
@reboot /sbin/iptables-restore < /root/rules
-
```

Перезагружаем машину и смотрим список правил, применяются ли они при запуске системы:

iptables -t nat -L

```

root@hq-rtr:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target      prot opt source                destination

Chain INPUT (policy ACCEPT)
target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target      prot opt source                destination
MASQUERADE  all  --  192.168.1.0/26         anywhere
MASQUERADE  all  --  192.168.2.0/28         anywhere
MASQUERADE  all  --  192.168.3.0/29         anywhere
root@hq-rtr:~# _

```

BR-RTR:

Пишем в консоль следующие команды:

```

iptables -t nat -A POSTROUTING -s 192.168.4.0/27 -o eth0 -j
MASQUERADE

```

```

iptables -t nat -L

```

```

root@br-rtr:~# iptables -t nat -A POSTROUTING -s 192.168.4.0/27 -o eth0 -j MASQUERADE
root@br-rtr:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target      prot opt source                destination

Chain INPUT (policy ACCEPT)
target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target      prot opt source                destination
MASQUERADE  all  --  192.168.4.0/27         anywhere
root@br-rtr:~#

```

Сохраним наши правила, пишем в консоль следующую команду:

```

iptables-save > /root/rules

```

```

root@br-rtr:~# iptables-save > /root/rules
root@br-rtr:~#

```

Запишем в **crontab** одну команду, чтобы при старте системы, правила загрузались из файла, в котором они хранятся.

Ппишем в консоль следующие команды:

```
export EDITOR=mcedit
```

```
crontab -e
```

Добавляем в конец файла следующие строки:

```
@reboot /sbin/iptables-restore < /root/rules
```

!ВАЖНО! Оставляем пустую строку после введённой строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу **ПУСТУЮ СТРОКУ!**

```
/tmp/crontab.sA3xop/crontab  [----]  0 L:[ 1+24 25/ 25] *(934 / 934
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
@reboot /sbin/iptables-restore < /root/rules
-
```

Перезагружаем машину и смотрим список правил, применяются ли они при запуске системы:

```
iptables -t nat -L
```

```

root@br-rtr:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  192.168.4.0/27        anywhere
root@br-rtr:~# _

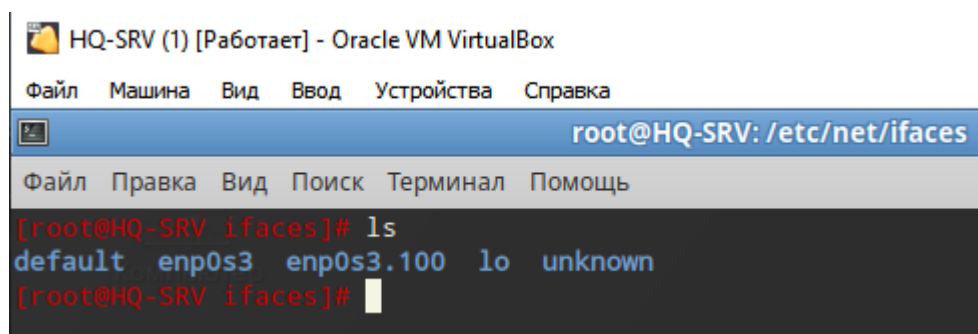
```

5. Настройка VLAN для HQ-SRV и HQ-CLI:

HQ-SRV:

Каталог **enp0s3** (у вас может быть своё название интерфейса, будьте внимательны) оставлять без изменений и перейти к настройке VLAN:

mkdir /etc/net/ifaces/enp0s3.100 (создание каталога под VLAN интерфейс)



```

HQ-SRV (1) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@HQ-SRV: /etc/net/ifaces
Файл  Правка  Вид  Поиск  Терминал  Помощь
[root@HQ-SRV ifaces]# ls
default enp0s3 enp0s3.100 lo unknown
[root@HQ-SRV ifaces]#

```

Создадим файл options и откроем его командой

mcedit /etc/net/ifaces/enp0s3.100/options

Запишем в него следующее содержимое:

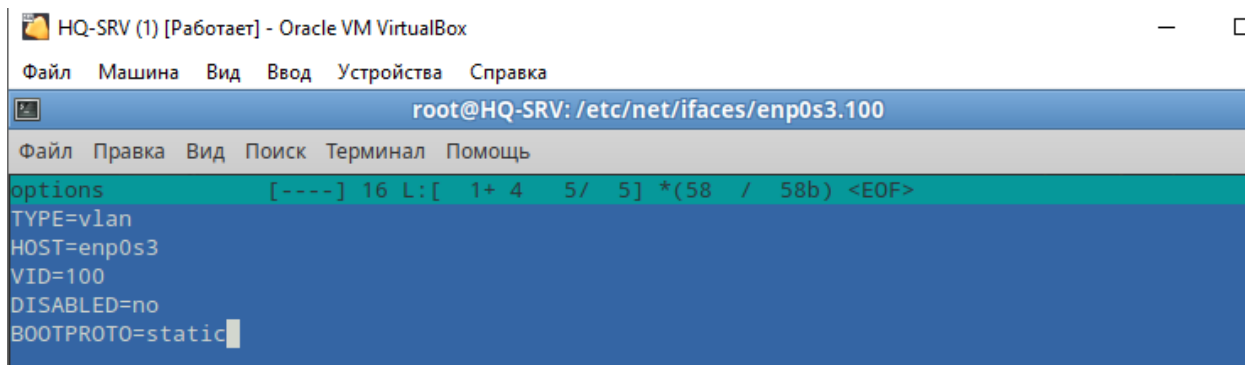
TYPE=vlan

HOST= enp0s3 (основной интерфейс, но у вас может быть иное название)

VID=100 (id VLAN'a)

DISABLED=no

BOOTPROTO=static



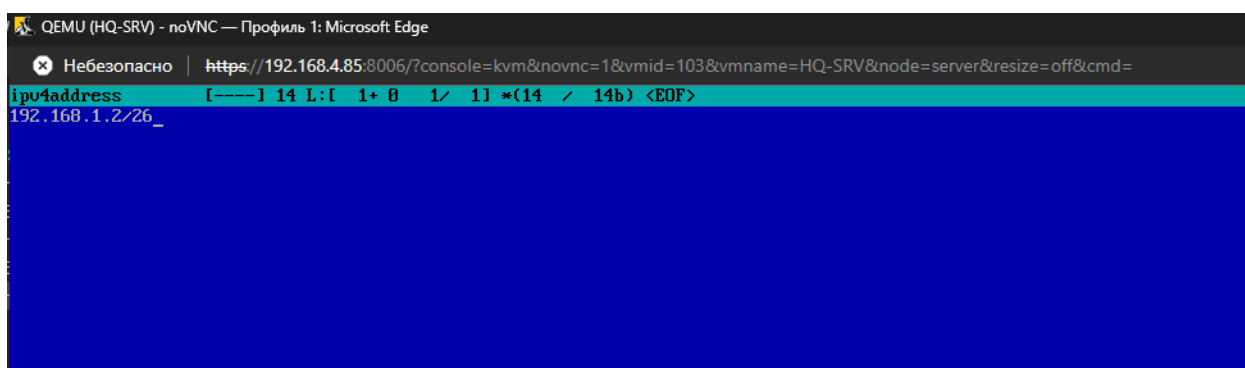
```
HQ-SRV (1) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@HQ-SRV: /etc/net/ifaces/enp0s3.100
Файл  Правка  Вид  Поиск  Терминал  Помощь
options [----] 16 L:[ 1+ 4 5/ 5] *(58 / 58b) <EOF>
TYPE=vlan
HOST=enp0s3
VID=100
DISABLED=no
BOOTPROTO=static
```

Создадим файлы **ipv4address** и **ipv4route** и откроем их командой:

mcedit /etc/net/ifaces/enp0s3.100/ipv4address

Записать туда следующую строку:

192.168.1.2/26

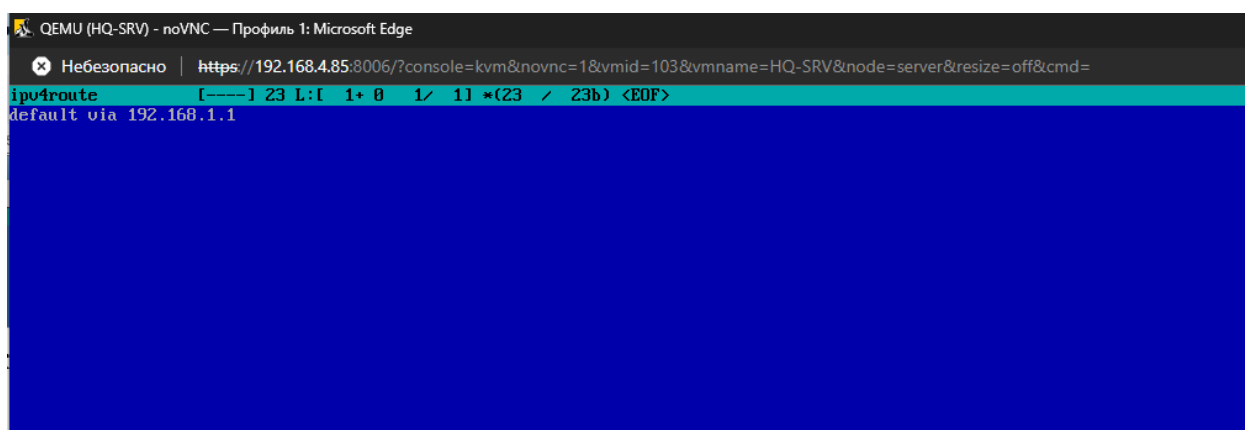


```
QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=103&vmname=HQ-SRV&node=server&resize=off&cmd=
root@HQ-SRV: /etc/net/ipv4address
192.168.1.2/26
```

mcedit /etc/net/ifaces/enp0s3.100/ipv4route

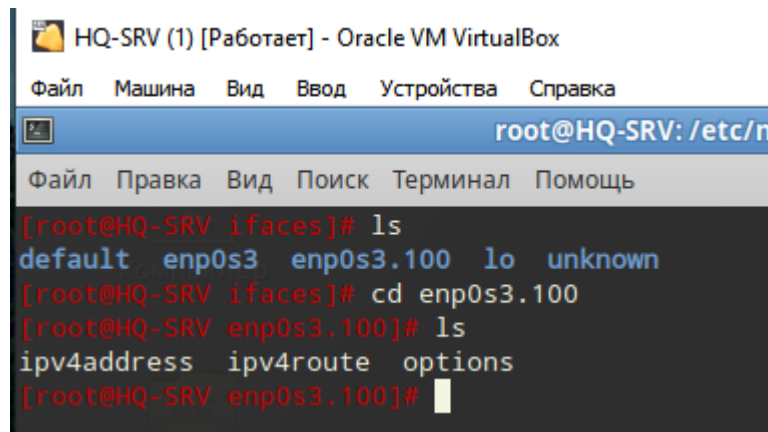
Записать туда следующую строку:

default via 192.168.1.1



```
QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=103&vmname=HQ-SRV&node=server&resize=off&cmd=
root@HQ-SRV: /etc/net/ipv4route
default via 192.168.1.1
```

В итоге должен получится такой набор файлов в каталоге интерфейса:



```
HQ-SRV (1) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@HQ-SRV: /etc/network/interfaces
Файл  Правка  Вид  Поиск  Терминал  Помощь
[root@HQ-SRV interfaces]# ls
default  enp0s3  enp0s3.100  lo  unknown
[root@HQ-SRV interfaces]# cd enp0s3.100
[root@HQ-SRV enp0s3.100]# ls
ipv4address  ipv4route  options
[root@HQ-SRV enp0s3.100]#
```

Обязательно после всех настроек интерфейсов ввести:

systemctl restart network

Также добавим запись о перезагрузке службы **network** в **crontab**.

Делаем это следующим образом, пишем команду:

export EDITOR=mcedit

А затем:

crontab -e

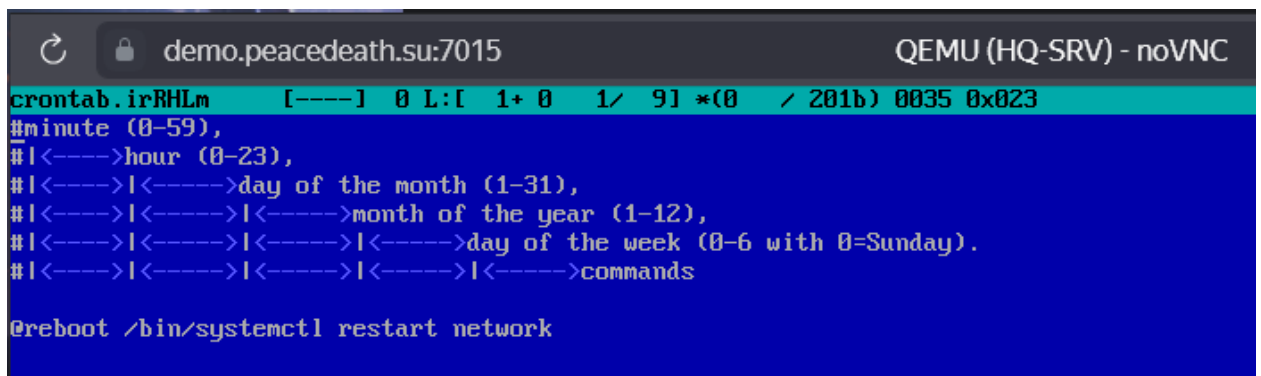


```
demo.peacedeath.su:7015 QEMU (HQ-SRV) - noVNC
[root@hq-srv ~]# export EDITOR=mcedit
[root@hq-srv ~]# crontab -e
```

И в конце файла пишем следующее:

@reboot /bin/systemctl restart network

!ВАЖНО! Оставляем пустую строку после введенной строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу **ПУСТУЮ СТРОКУ!**

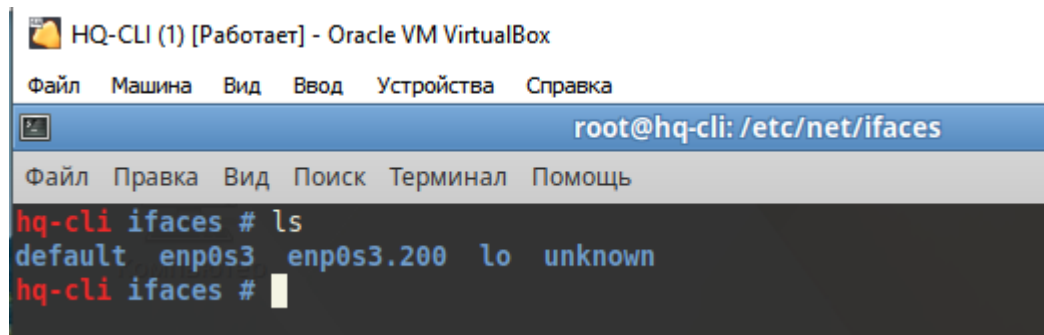


```
demo.peacedeath.su:7015 QEMU (HQ-SRV) - noVNC
crontab.irRHLm  [----] 0 L: 1+ 0 1/ 91 *(0 / 201b) 0035 0x023
#minute (0-59),
#|<---->hour (0-23),
#|<---->|<---->day of the month (1-31),
#|<---->|<---->|<---->month of the year (1-12),
#|<---->|<---->|<---->|<---->day of the week (0-6 with 0=Sunday).
#|<---->|<---->|<---->|<---->|<---->commands
@reboot /bin/systemctl restart network
```

HQ-CLI:

Каталог `enp0s3` оставлять без изменений и перейти к настройке VLAN:

mkdir /etc/net/ifaces/enp0s3.200 (создание каталога под VLAN интерфейс)



```
HQ-CLI (1) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@hq-cli: /etc/net/ifaces
Файл  Правка  Вид  Поиск  Терминал  Помощь
hq-cli ifaces # ls
default enp0s3 enp0s3.200 lo unknown
hq-cli ifaces #
```

Создадим файл `options` и откроем его командой:

mcedit /etc/net/ifaces/enp0s3.200/options

Запишем в него следующее содержимое:

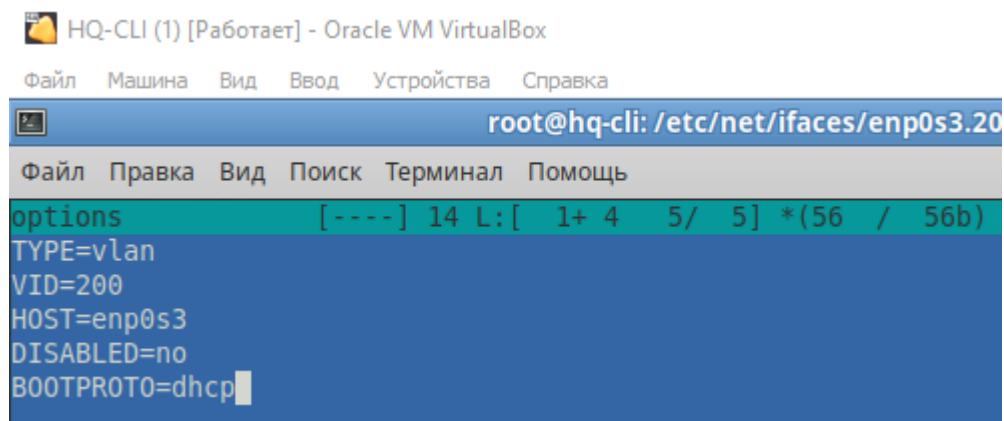
TYPE=vlan

VID=200 (id VLAN'a)

HOST= enp0s3 (основной интерфейс)

DISABLED=no

BOOTPROTO=dhcp



```
HQ-CLI (1) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@hq-cli: /etc/net/ifaces/enp0s3.200
Файл  Правка  Вид  Поиск  Терминал  Помощь
options [-----] 14 L:[ 1+ 4 5/ 5] *(56 / 56b)
TYPE=vlan
VID=200
HOST=enp0s3
DISABLED=no
BOOTPROTO=dhcp
```

Создавать файлы **ipv4address** и **ipv4route** не нужно, т.к. мы получаем на **HQ-CLI** настройки по **DHCP**, который далее будет настроен на роутере.

Обязательно после всех настроек интерфейсов ввести:

systemctl restart network (АЛЬТ)

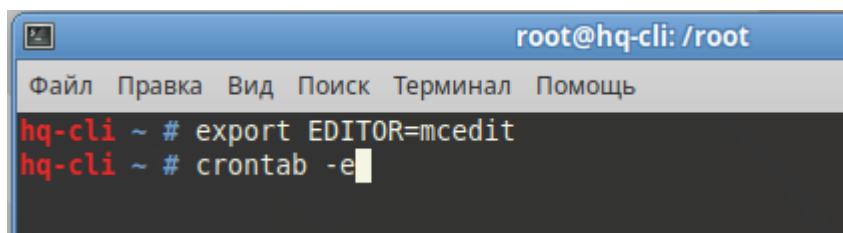
Также добавим запись о перезагрузке службы **network** в **crontab**.

Делаем это следующим образом, пишем команду:

export EDITOR=mcedit

А затем:

crontab -e

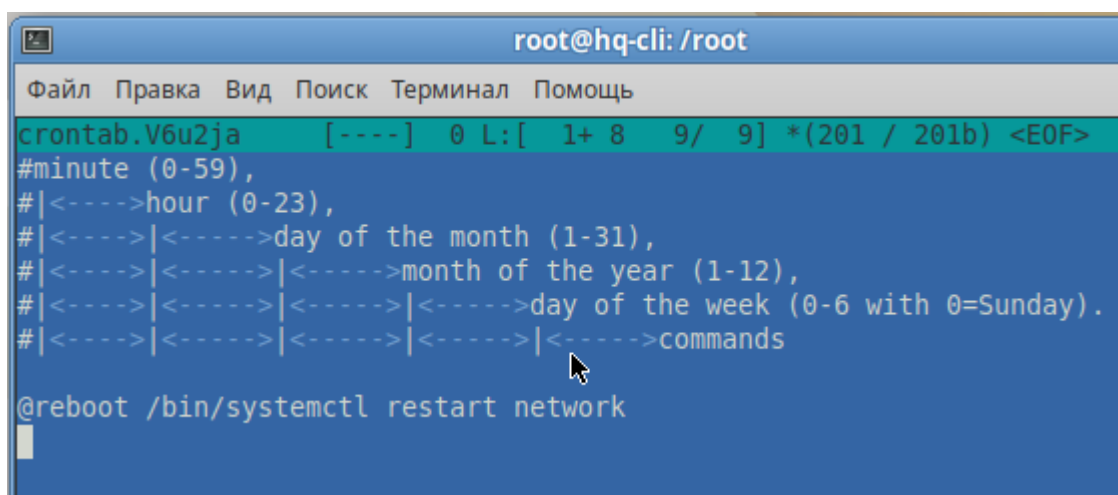


```
root@hq-cli: /root
Файл Правка Вид Поиск Терминал Помощь
hq-cli ~ # export EDITOR=mcedit
hq-cli ~ # crontab -e
```

И в конце файла пишем следующее:

@reboot /bin/systemctl restart network

!ВАЖНО! Оставляем пустую строку после введенной строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу **ПУСТУЮ СТРОКУ!**



```
root@hq-cli: /root
Файл Правка Вид Поиск Терминал Помощь
crontab.V6u2ja  [----] 0 L: [ 1+ 8 9/ 9] *(201 / 201b) <EOF>
#minute (0-59),
#|<---->hour (0-23),
#|<---->|<---->day of the month (1-31),
#|<---->|<---->|<---->month of the year (1-12),
#|<---->|<---->|<---->|<---->day of the week (0-6 with 0=Sunday).
#|<---->|<---->|<---->|<---->|<---->commands
@reboot /bin/systemctl restart network
```

6. Настройка IP-туннеля между офисами HQ и BR:

Создание туннеля производится на маршрутизаторах **HQ-RTR** и **BR-RTR**.

HQ-RTR:

Для создания туннеля необходимо добавить новый интерфейс в файл **/etc/network/interfaces**

Откроем этот файл текстовым редактором следующей командой:

mcedit /etc/network/interfaces

Добавляем в конец файла то, что выделено на скриншоте:

The screenshot shows a terminal window titled "HQ-RTR (1) [Работает] - Oracle VM VirtualBox". Inside, the GNU nano 2.7.4 editor is open, editing the file /etc/network/interfaces. The file contains configurations for three interfaces: eth1.100, eth1.200, and eth1.999, all using static IP addresses and connected to eth1 via vlan-raw-device. A fourth interface, gre1, is being added and highlighted with a red box. It is configured as a tunnel interface with IP 10.10.10.1, netmask 255.255.255.252, mode gre, local endpoint 172.16.4.2, remote endpoint 172.16.5.2, and ttl 255. The nano editor's status bar at the bottom shows various keyboard shortcuts in Russian, such as "Помощь", "Записать", "Поиск", etc.

```
GNU nano 2.7.4 Файл: /etc/network/interfaces

iface eth1.100 inet static
address 192.168.1.1
netmask 255.255.255.192
vlan-raw-device eth1
auto eth1.200
iface eth1.200 inet static
address 192.168.2.1
netmask 255.255.255.240
vlan-raw-device eth1
auto eth1.999
iface eth1.999 inet static
address 192.168.3.1
netmask 255.255.255.248
vlan-raw-device eth1
auto gre1
iface gre1 inet tunnel
address 10.10.10.1
netmask 255.255.255.252
mode gre
local 172.16.4.2
endpoint 172.16.5.2
ttl 255
_
```

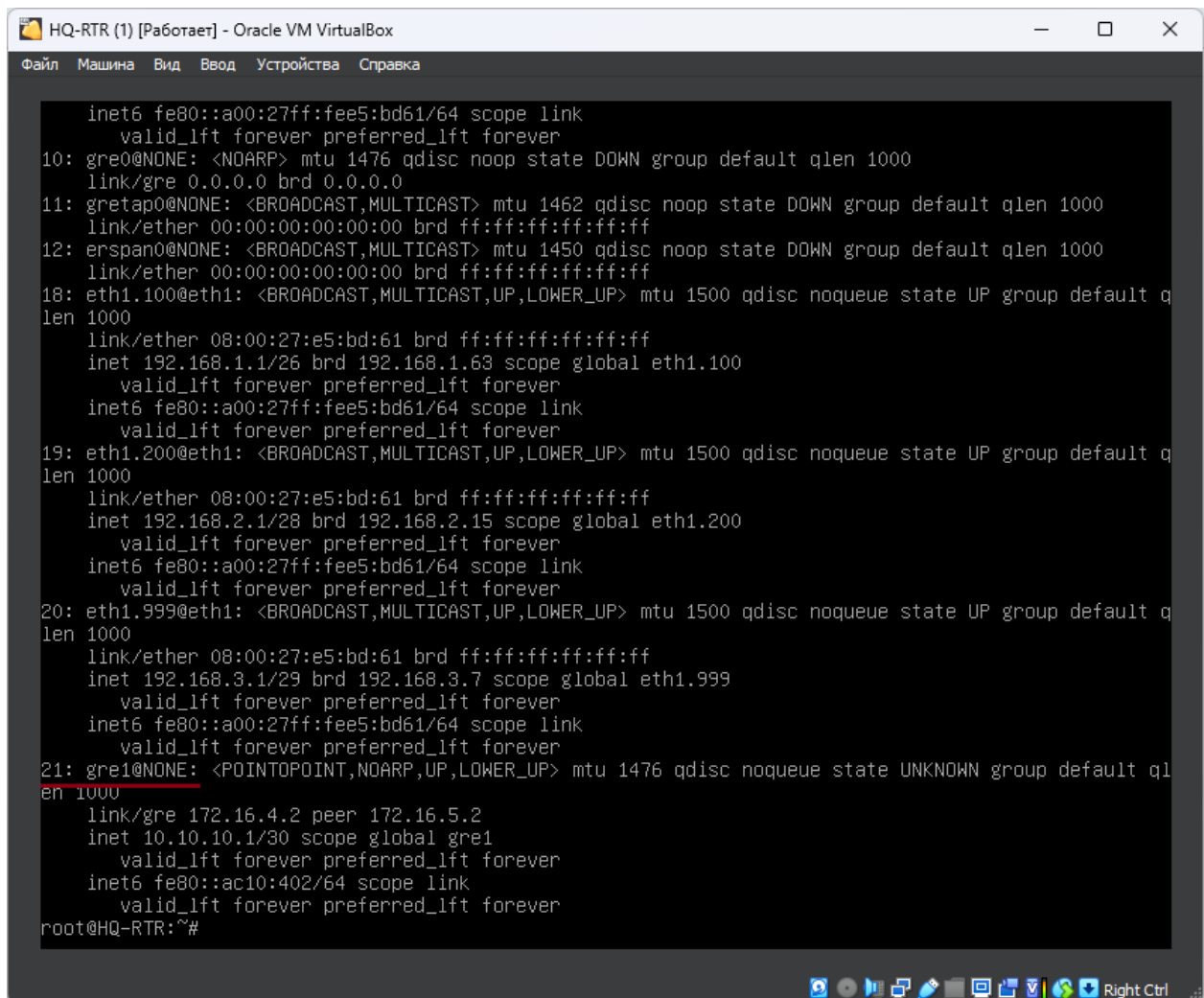
Сохраняем файл, выходим из редактора.

Перезапускаем службу networking для применения изменений:

systemctl restart networking

Проверяем наличие IP-туннеля:

ip a



```
inet6 fe80::a00:27ff:fee5:bd61/64 scope link
    valid_lft forever preferred_lft forever
10: gre0@NONE: <NOARP> mtu 1476 qdisc noop state DOWN group default qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
11: gretap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
12: erspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
18: eth1.100@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:e5:bd:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/26 brd 192.168.1.63 scope global eth1.100
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee5:bd61/64 scope link
        valid_lft forever preferred_lft forever
19: eth1.200@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:e5:bd:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.1/28 brd 192.168.2.15 scope global eth1.200
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee5:bd61/64 scope link
        valid_lft forever preferred_lft forever
20: eth1.999@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:e5:bd:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.1/29 brd 192.168.3.7 scope global eth1.999
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee5:bd61/64 scope link
        valid_lft forever preferred_lft forever
21: gre1@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default qlen 1000
    link/gre 172.16.4.2 peer 172.16.5.2
    inet 10.10.10.1/30 scope global gre1
        valid_lft forever preferred_lft forever
    inet6 fe80::ac10:402/64 scope link
        valid_lft forever preferred_lft forever
root@HQ-RTR:~#
```

Туннель появился.

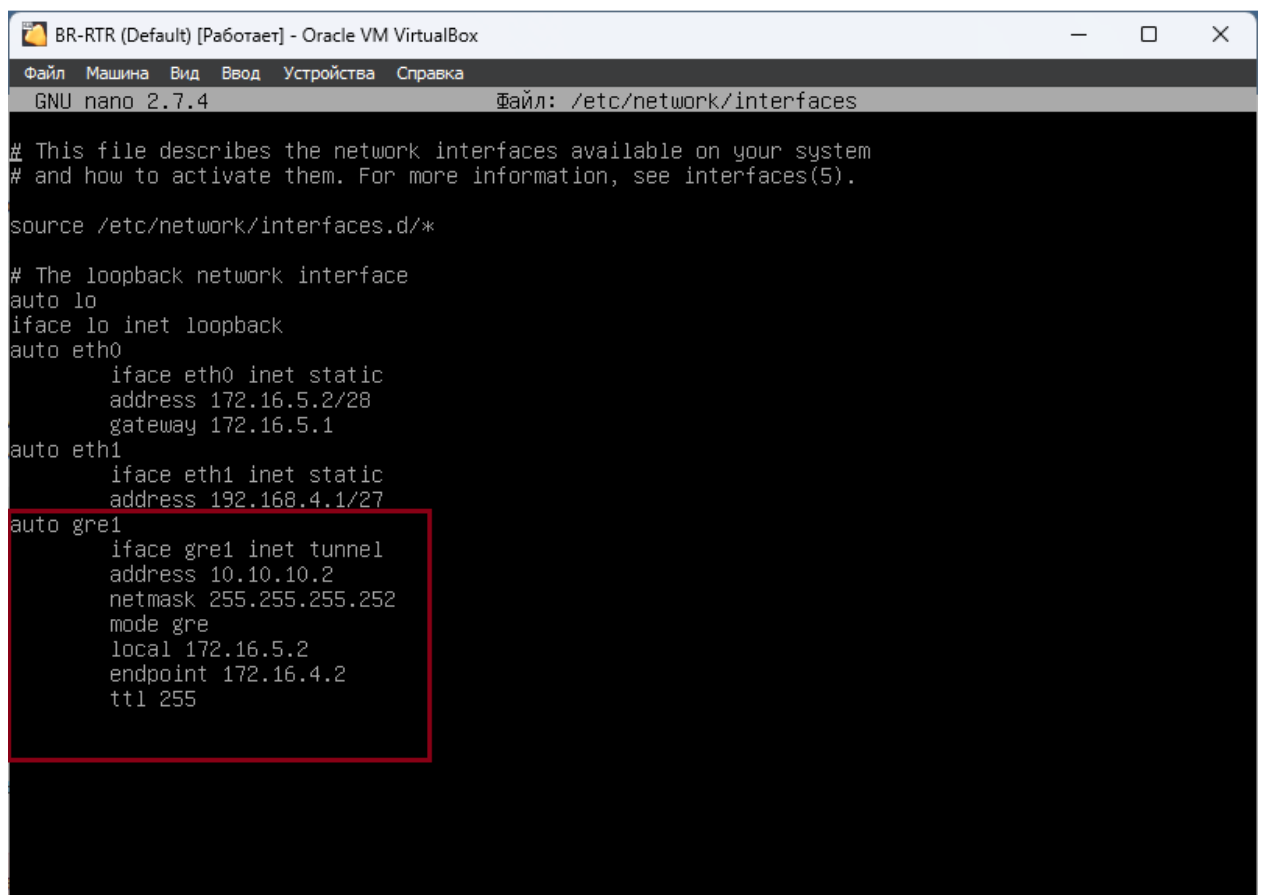
BR-RTR:

На этом роутере тоже самое, только нужно поменять IP-адрес туннеля и IP-адреса local и endpoint.

Открываем файл текстовым редактором **mcedit** следующей командой:

mcedit /etc/network/interfaces

Прописываем в конец файла следующее содержимое:

A screenshot of a virtual machine window titled "BR-RTR (Default) [Работает] - Oracle VM VirtualBox". Inside the window, a terminal window shows the GNU nano 2.7.4 text editor editing the file /etc/network/interfaces. The file content includes configuration for loopback, eth0, eth1, and gre1 interfaces. The gre1 configuration is highlighted with a red box. The configuration for gre1 is as follows:

```
auto gre1
    iface gre1 inet tunnel
    address 10.10.10.2
    netmask 255.255.255.252
    mode gre
    local 172.16.5.2
    endpoint 172.16.4.2
    ttl 255
```

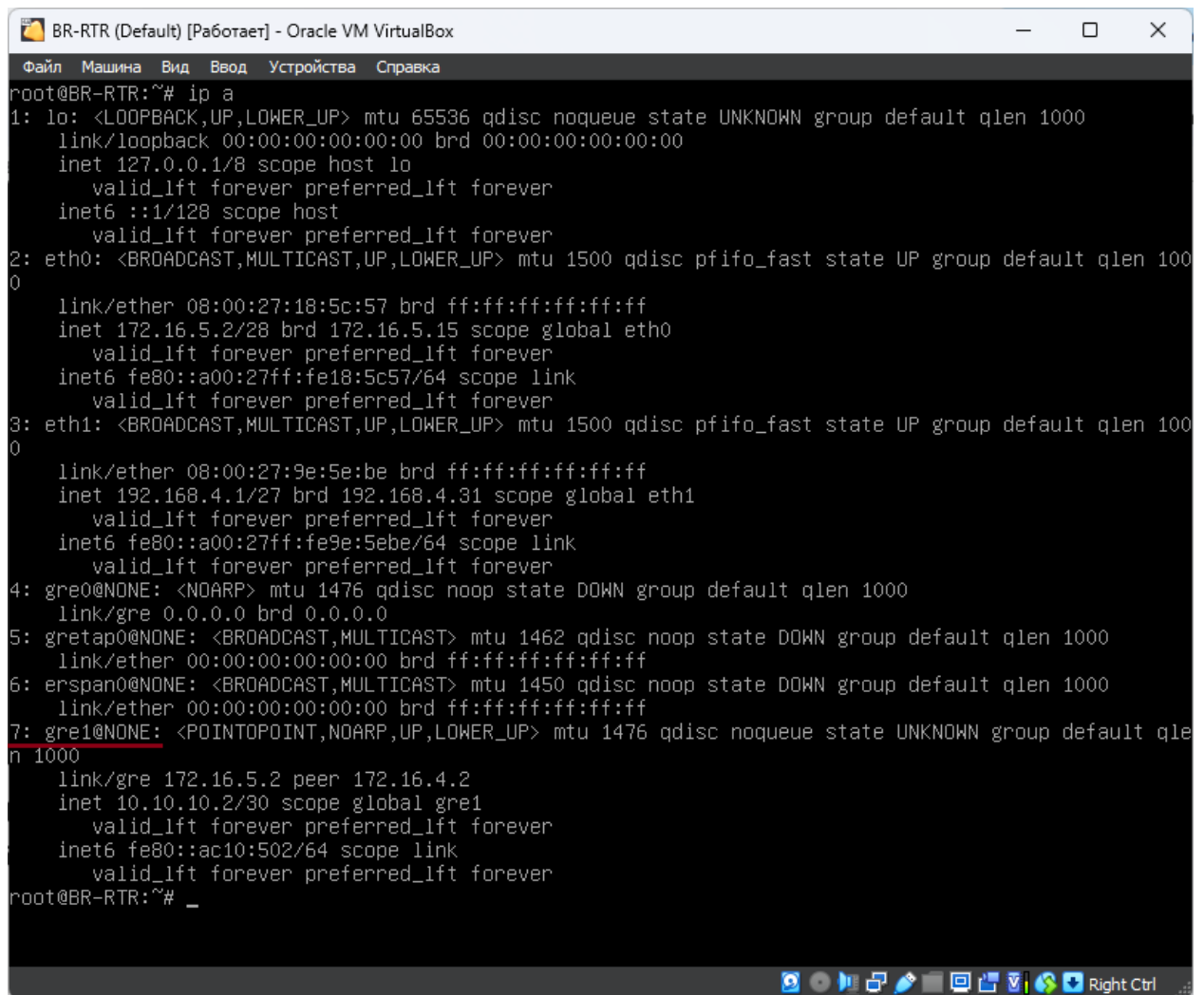
Сохраняем файл, выходим из редактора.

Также перезапускаем службу `networking` для применения изменений:

`systemctl restart networking`

Проверяем наличие IP-туннеля:

`ip a`

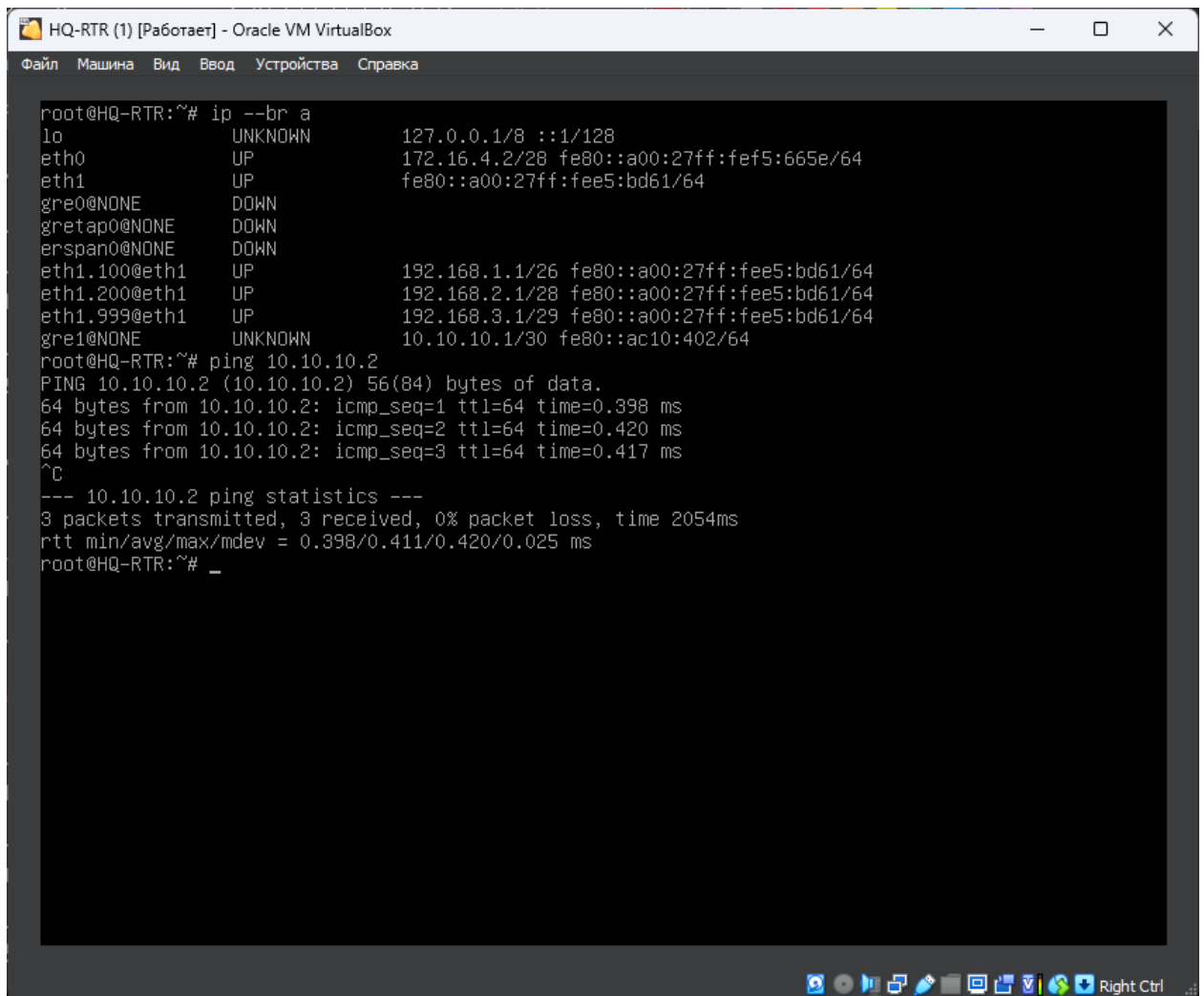


```
root@BR-RTR:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:18:5c:57 brd ff:ff:ff:ff:ff:ff
    inet 172.16.5.2/28 brd 172.16.5.15 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe18:5c57/64 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 08:00:27:9e:5e:be brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.1/27 brd 192.168.4.31 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9e:5ebe/64 scope link
        valid_lft forever preferred_lft forever
4: gre0@NONE: <NOARP> mtu 1476 qdisc noop state DOWN group default qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
5: gretap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
6: erspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
7: gre1@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default qlen 1000
    link/gre 172.16.5.2 peer 172.16.4.2
    inet 10.10.10.2/30 scope global gre1
        valid_lft forever preferred_lft forever
    inet6 fe80::ac10:502/64 scope link
        valid_lft forever preferred_lft forever
root@BR-RTR:~# _
```

Туннель между офисами настроен, полностью проверить его работу можно после настройки **OSPF**. Но пинги между **10.10.10.1** и **10.10.10.2** уже должны доходить.

Отправим с **HQ-RTR** эхо-запрос до **BR-RTR** по туннелю:

ping 10.10.10.2



```
root@HQ-RTR:~# ip --br a
lo                UNKNOWN      127.0.0.1/8 ::1/128
eth0              UP            172.16.4.2/28 fe80::a00:27ff:fe5:665e/64
eth1              UP            fe80::a00:27ff:fe5:bd61/64
gre0@NONE        DOWN
gretap0@NONE      DOWN
erspan0@NONE      DOWN
eth1.100@eth1     UP            192.168.1.1/26 fe80::a00:27ff:fe5:bd61/64
eth1.200@eth1     UP            192.168.2.1/28 fe80::a00:27ff:fe5:bd61/64
eth1.999@eth1     UP            192.168.3.1/29 fe80::a00:27ff:fe5:bd61/64
gre1@NONE        UNKNOWN     10.10.10.1/30 fe80::ac10:402/64
root@HQ-RTR:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data:
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.398 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.420 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.417 ms
^C
--- 10.10.10.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2054ms
rtt min/avg/max/mdev = 0.398/0.411/0.420/0.025 ms
root@HQ-RTR:~# _
```

Работает, приступаем к следующему этапу для полной работы туннеля

7. Настройка динамической маршрутизации с помощью link-state протокола OSPF.

Для работы OSPF нам нужна служба `frr`, которой по умолчанию нет на наших маршрутизаторах HQ-RTR и BR-RTR, поэтому сделаем следующие шаги.

HQ-RTR:

Нужно закомментировать в `/etc/apt/sources.list` первую строку с репозиторием АСТРЫ, т.к. он не имеет пакета `frr` даже после обновлений репозитория, вместо него мы будем использовать `debian` репозиторий.

Для начала зайдём туда следующей командой:

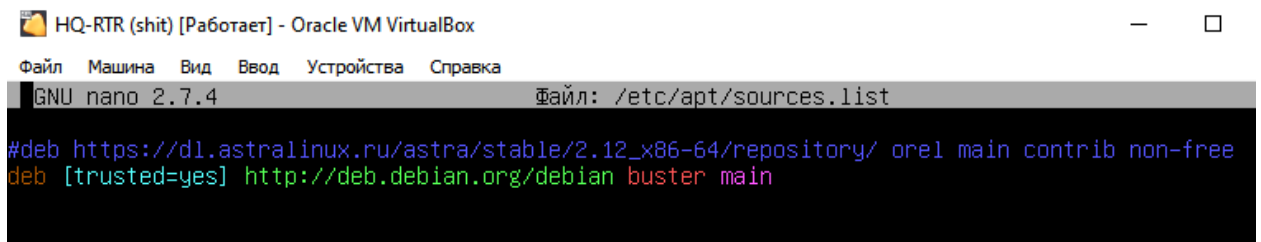
```
mcedit /etc/apt/sources.list
```

Комментируем первую строку знаком `#`:

```
#deb https://dl.astralinux.ru/astra/stables/2.12\_x86-64/repository/ orel main  
contrib non-free
```

Ниже пишем следующую строку:

deb [trusted=yes] <http://deb.debian.org/debian> buster main



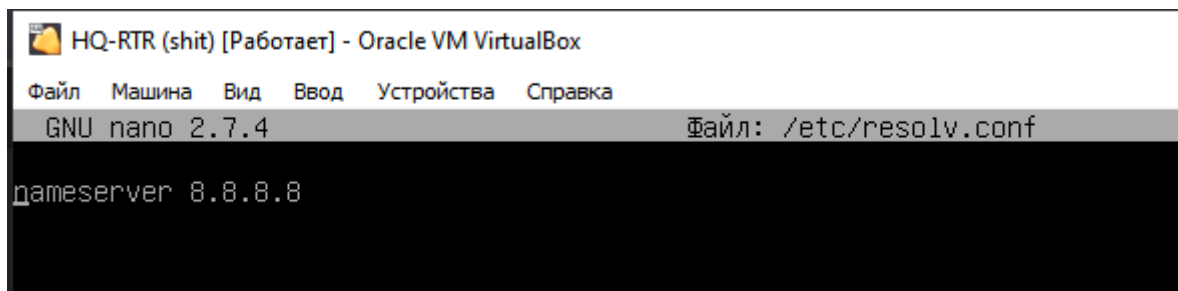
```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 2.7.4                               Файл: /etc/apt/sources.list
#deb https://dl.astralinux.ru/astra/stable/2.12_x86-64/repository/ orel main contrib non-free
deb [trusted=yes] http://deb.debian.org/debian buster main
```

Ещё нам нужно добавить в `/etc/resolv.conf` сервер Google, иначе мы не сможем обновить репозитории, поэтому идём его редактировать следующей командой:

mcedit /etc/resolv.conf

И добавляем следующую строку в него:

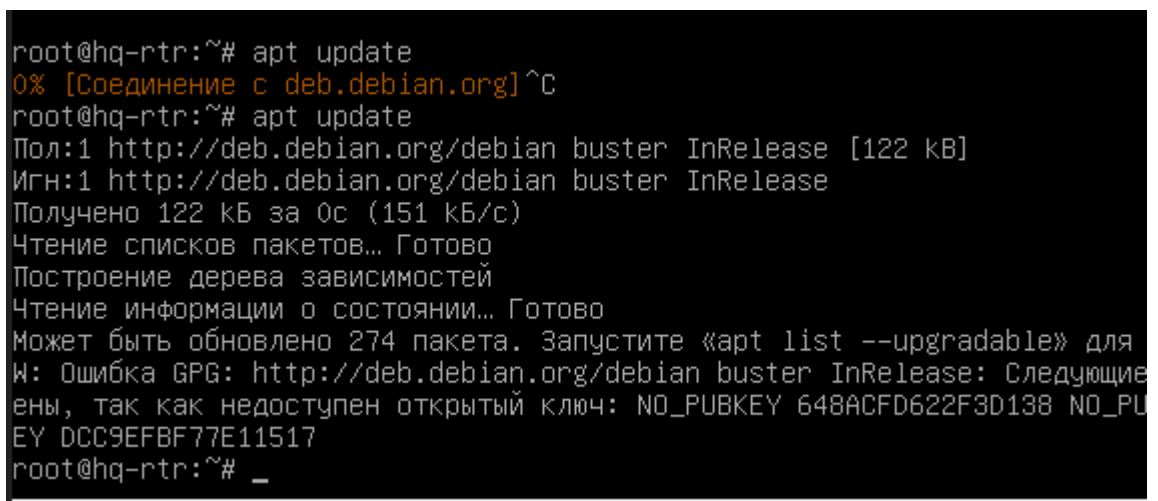
nameserver 8.8.8.8



```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 2.7.4                               Файл: /etc/resolv.conf
nameserver 8.8.8.8
```

Сохраняем и идём теперь обновлять список пакетов:

apt update

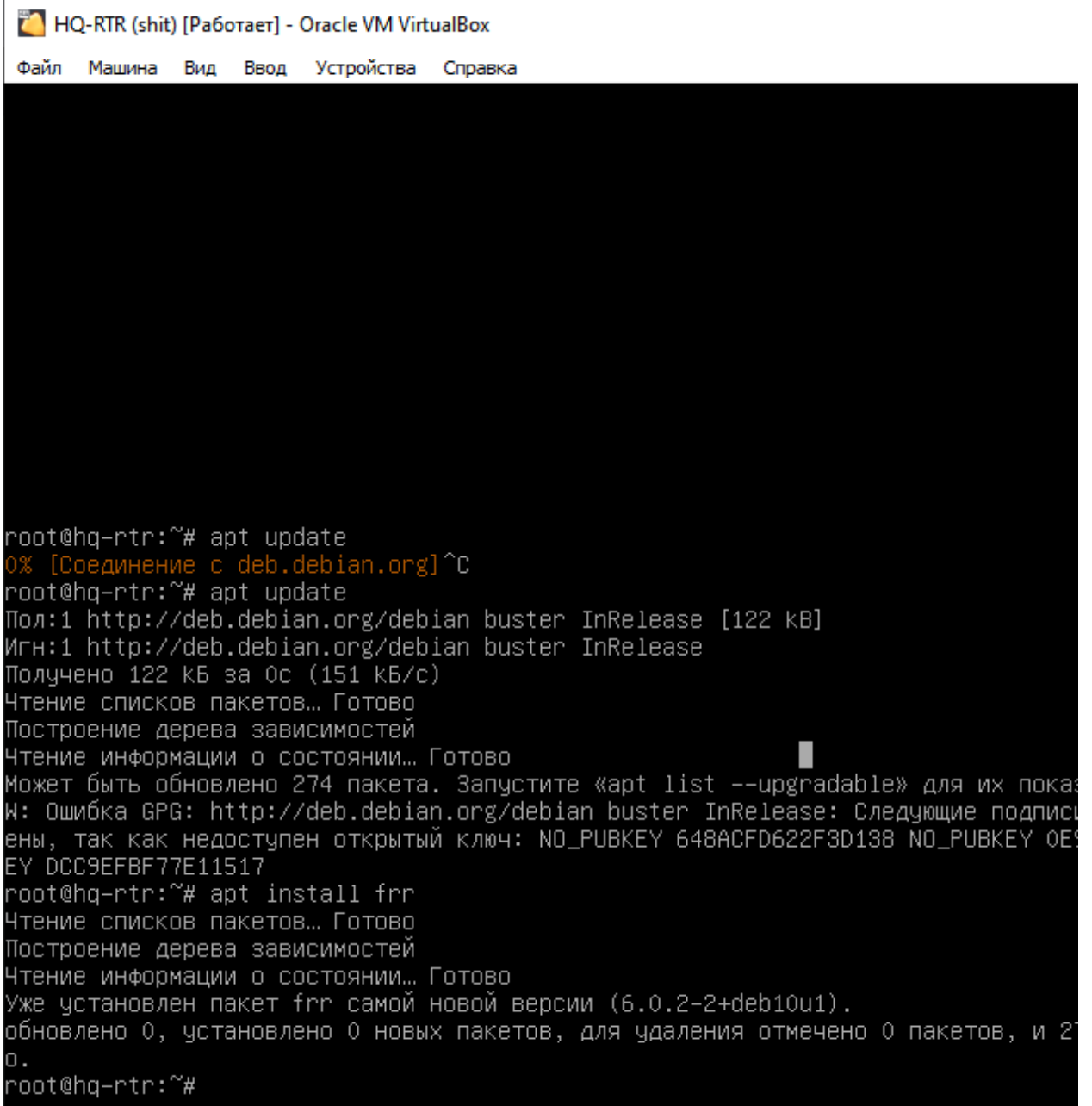


```
root@hq-rtr:~# apt update
0% [Соединение с deb.debian.org]^C
root@hq-rtr:~# apt update
Пол:1 http://deb.debian.org/debian buster InRelease [122 kB]
Игн:1 http://deb.debian.org/debian buster InRelease
Получено 122 kB за 0с (151 kB/с)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Может быть обновлено 274 пакета. Запустите «apt list --upgradable» для
W: Ошибка GPG: http://deb.debian.org/debian buster InRelease: Следующие
ены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PU
EY DCC9EFBF77E11517
root@hq-rtr:~# _
```

То, что он может ругаться на недоступный открытый ключ, это нормально, идём дальше!

Теперь качаем сам пакет `frr`:

apt install frr



```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

root@hq-rtr:~# apt update
0% [Соединение с deb.debian.org]^C
root@hq-rtr:~# apt update
Пол:1 http://deb.debian.org/debian buster InRelease [122 kB]
Игн:1 http://deb.debian.org/debian buster InRelease
Получено 122 kB за 0с (151 kB/с)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Может быть обновлено 274 пакета. Запустите «apt list --upgradable» для их показа
W: Ошибка GPG: http://deb.debian.org/debian buster InRelease: Следующие подписи
ены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PUBKEY 0E9
EY DCC9EFBF77E11517
root@hq-rtr:~# apt install frr
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет frr самой новой версии (6.0.2-2+deb10u1).
обновлено 0, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 27
0.
root@hq-rtr:~#
```

У нас он уже установлен, поэтому не обращаем внимание, скриншот нужен для того, чтобы вы поняли.

Затем нам нужно включить настройку ospf через конфигурационный файл /etc/frr/daemons:

mcedit /etc/frr/daemons

Находим в нём следующую строку и приводим её к такому виду:

ospfd=yes


```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 2.7.4                               Файл: /etc/frr/daemons

# This file tells the frr package which daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activation a daemon at the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /etc/init.d/frr. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrvty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr and zebra daemons are always started.
#
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
ldpd=no
nhdpd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfd=no
```

А затем перезагрузим службу командой:

systemctl restart frr

А затем начнём настройку:

vtysh (зайти в режим настройки)

conf t (режим конфигурации, ВСПОМИНАЕМ ЦИСКО, РЕБЯТКИ!)

router ospf

network 10.10.10.0/30 area 0

network 192.168.1.0/26 area 0

network 192.168.2.0/28 area 0

network 192.168.3.0/29 area 0

do wr mem

```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Astra Linux CE 2.12.46 (orel) hq-rtr.au-team.irpo tty1
hq-rtr login: root
Password:
Last login: Thu Sep 26 21:25:54 +07 2024 on tty1
root@hq-rtr:~# vtysh

Hello, this is FRRouting (version 6.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

hq-rtr.au-team.irpo# conf t
hq-rtr.au-team.irpo(config)# router ospf
hq-rtr.au-team.irpo(config-router)# network 10.10.10.0/30 area 0
hq-rtr.au-team.irpo(config-router)# network 192.168.1.0/26 area 0
hq-rtr.au-team.irpo(config-router)# network 192.168.2.0/28 area 0
hq-rtr.au-team.irpo(config-router)# network 192.168.3.0/29 area 0
hq-rtr.au-team.irpo(config-router)# do wr mem
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
hq-rtr.au-team.irpo(config-router)#
```

Теперь настроим парольную защиту на нашем GRE туннеле через frr:

vysh

conf t

int gre1

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 P@ssw0rd

do wr mem

HQ-RTR (shit) [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

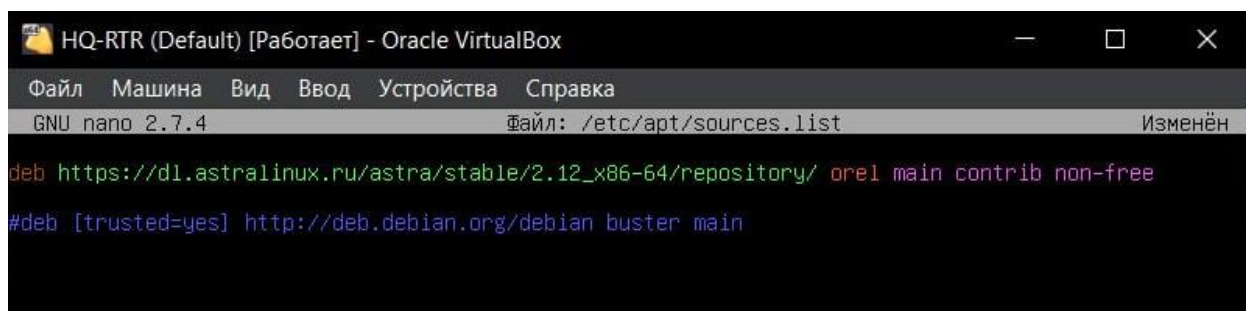
```
root@hq-rtr:~# vtysh

Hello, this is FRRouting (version 6.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

hq-rtr.au-team.irpo# conf t
hq-rtr.au-team.irpo(config)# int gre1
hq-rtr.au-team.irpo(config-if)# ip ospf authentication message-digest
hq-rtr.au-team.irpo(config-if)# ip ospf message-digest-key 1 md5 P@ssw0rd
OSPF: Key 1 already exists
hq-rtr.au-team.irpo(config-if)# no ip ospf message-digest-key 1 md5 P@ssw0rd
hq-rtr.au-team.irpo(config-if)# ip ospf message-digest-key 1 md5 P@ssw0rd
hq-rtr.au-team.irpo(config-if)# do wr mem
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
hq-rtr.au-team.irpo(config-if)# _
```

OSPF на HQ-RTR настроен.

ПОСЛЕ ПРОДЕЛАННОЙ РАБОТЫ, РАСКОММЕНТИРУЙТЕ РЕПОЗИТОРИЙ АСТРЫ И ЗАКОММЕНТИРУЙТЕ РЕПОЗИТОРИЙ DEBIAN!!! ВОТ ТАК:



The screenshot shows a terminal window titled "HQ-RTR (Default) [Работает] - Oracle VirtualBox". The terminal is running the GNU nano 2.7.4 editor on the file /etc/apt/sources.list. The current content of the file is:

```
deb https://dl.astralinux.ru/astra/stable/2.12_x86-64/repository/ orel main contrib non-free
#deb [trusted=yes] http://deb.debian.org/debian buster main
```

BR-RTR:

Продельваем тоже самое с репозиториями.

Для начала зайдём туда следующей командой:

mcedit /etc/apt/sources.list

Комментируем первую строку знаком #:

#deb https://dl.astralinux.ru/astra/stables/2.12_x86-64/repository/ orel main contrib non-free

Ниже пишем следующую строку:

deb [trusted=yes] <http://deb.debian.org/debian> buster main



```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 2.7.4                               Файл: /etc/apt/sources.list

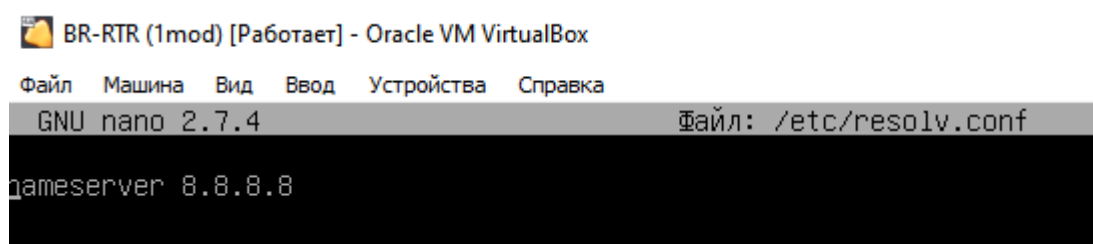
#deb https://dl.astralinux.ru/astra/stable/2.12_x86-64/repository/ ore1 main contrib non-free
deb [trusted=yes] http://deb.debian.org/debian buster main
```

Теперь нам нужно добавить в /etc/resolv.conf сервер Google:

mcedit /etc/resolv.conf

И добавляем следующую строку в него:

nameserver 8.8.8.8

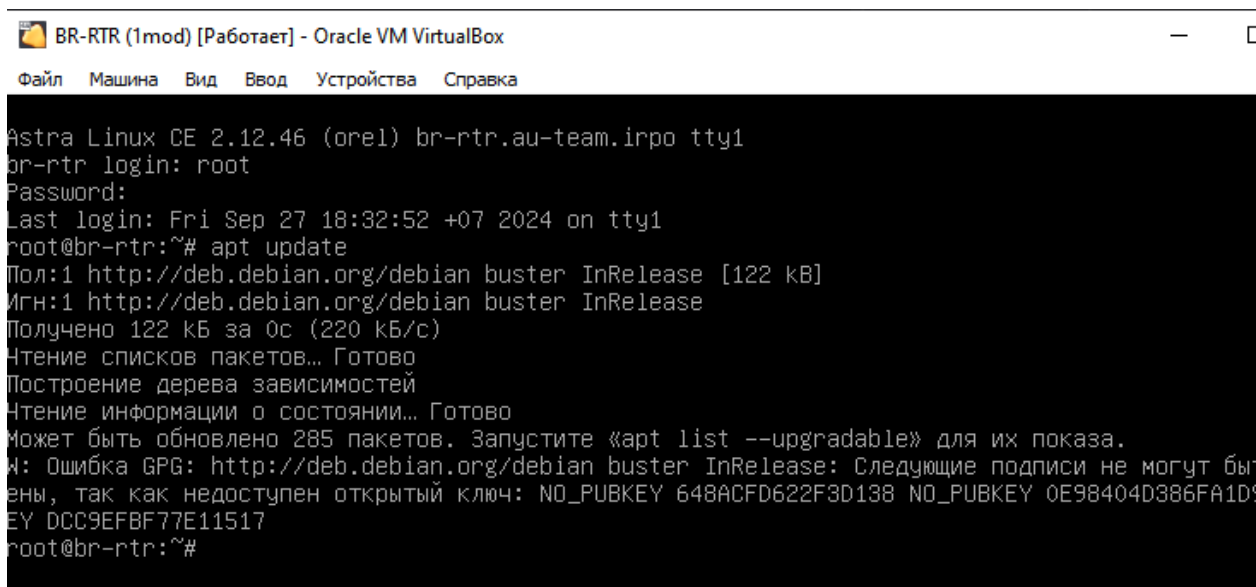


```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 2.7.4                               Файл: /etc/resolv.conf

nameserver 8.8.8.8
```

Сохраняем и идём теперь обновлять список пакетов:

apt update



```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Astra Linux CE 2.12.46 (ore1) br-rtr.au-team.irpo tty1
br-rtr login: root
Password:
Last login: Fri Sep 27 18:32:52 +07 2024 on tty1
root@br-rtr:~# apt update
Пол:1 http://deb.debian.org/debian buster InRelease [122 kB]
Игн:1 http://deb.debian.org/debian buster InRelease
Получено 122 kB за 0с (220 kB/с)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Может быть обновлено 285 пакетов. Запустите «apt list --upgradable» для их показа.
W: Ошибка GPG: http://deb.debian.org/debian buster InRelease: Следующие подписи не могут бы
ены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PUBKEY 0E98404D386FA1D
EY DCC9EFBF77E11517
root@br-rtr:~#
```

Теперь качаем сам пакет frr:

apt install frr

```
Astra Linux CE 2.12.46 (orel) br-rtr.au-team.irpo tty1
br-rtr login: root
Password:
Last login: Fri Sep 27 18:32:52 +07 2024 on tty1
root@br-rtr:~# apt update
Пол:1 http://deb.debian.org/debian buster InRelease [122 kB]
Игн:1 http://deb.debian.org/debian buster InRelease
Получено 122 kB за 0с (220 kB/с)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Может быть обновлено 285 пакетов. Запустите «apt list --upgradable» для их показа.
W: Ошибка GPG: http://deb.debian.org/debian buster InRelease: Следующие подписи не могут бы
ены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PUBKEY 0E98404D386FA1D
EY DCC9EFBF77E11517
root@br-rtr:~# apt install frr
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет frr самой новой версии (6.0.2-2+deb10u1).
обновлено 0, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 285 пакетов не
о.
root@br-rtr:~#
```

Затем нам нужно включить настройку ospf через конфигурационный файл **/etc/frr/daemons**:

mcedit /etc/frr/daemons

Находим в нём следующую строку и приводим её к такому виду:

ospfd=yes

```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 2.7.4  Файл: /etc/frr/daemons

# This file tells the frr package which daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activation a daemon at the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /etc/init.d/frr. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrvty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr and zebra daemons are always started.
#
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
ldpd=no
nhripd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfdd=no
```

А затем перезагрузим службу командой:

systemctl restart frr

А затем начнём настройку:

vtysh

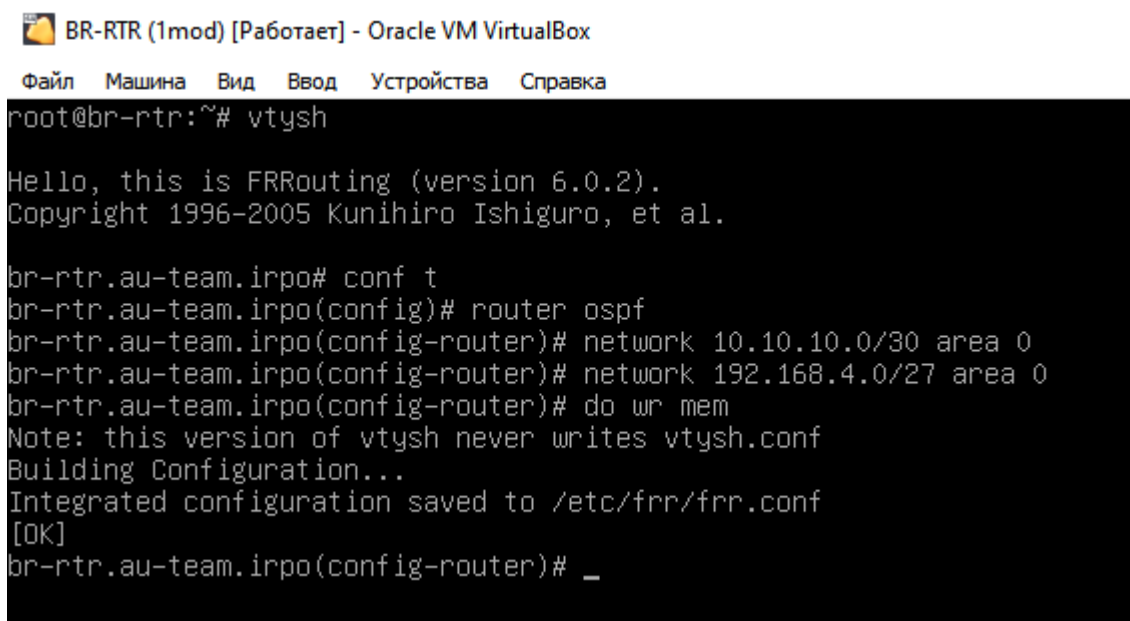
conf t

router ospf

network 10.10.10.0/30 area 0

network 192.168.4.0/27 area 0

do wr mem



```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@br-rtr:~# vtysh

Hello, this is FRRouting (version 6.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

br-rtr.au-team.irpo# conf t
br-rtr.au-team.irpo(config)# router ospf
br-rtr.au-team.irpo(config-router)# network 10.10.10.0/30 area 0
br-rtr.au-team.irpo(config-router)# network 192.168.4.0/27 area 0
br-rtr.au-team.irpo(config-router)# do wr mem
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
br-rtr.au-team.irpo(config-router)# _
```

Теперь настроим парольную защиту на нашем GRE туннеле через **frr** на второй стороне тоже:

vtysh

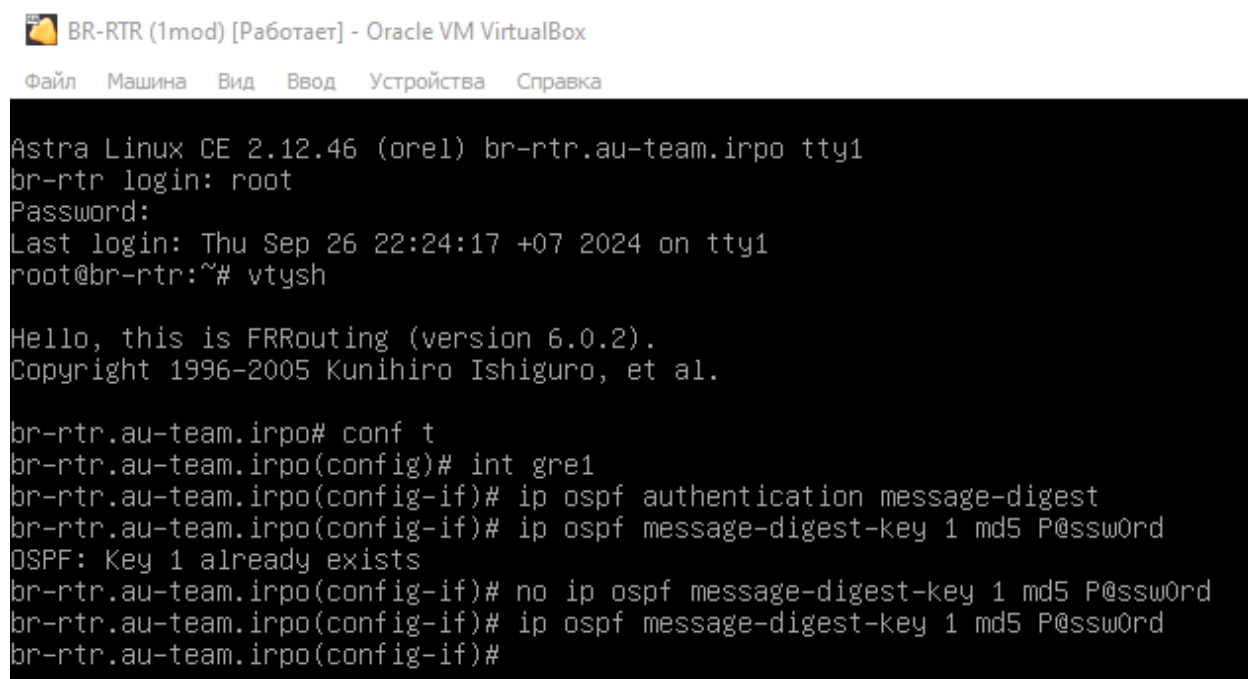
conf t

int gre1

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 P@ssw0rd

do wr mem



```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Astra Linux CE 2.12.46 (orel) br-rtr.au-team.irpo tty1
br-rtr login: root
Password:
Last login: Thu Sep 26 22:24:17 +07 2024 on tty1
root@br-rtr:~# vtysh

Hello, this is FRRouting (version 6.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

br-rtr.au-team.irpo# conf t
br-rtr.au-team.irpo(config)# int gre1
br-rtr.au-team.irpo(config-if)# ip ospf authentication message-digest
br-rtr.au-team.irpo(config-if)# ip ospf message-digest-key 1 md5 P@ssw0rd
OSPF: Key 1 already exists
br-rtr.au-team.irpo(config-if)# no ip ospf message-digest-key 1 md5 P@ssw0rd
br-rtr.au-team.irpo(config-if)# ip ospf message-digest-key 1 md5 P@ssw0rd
br-rtr.au-team.irpo(config-if)#
```

OSPF на BR-RTR настроен.

Также нужно вернуть репозиторий астры обратно, смотрите выше, как мы это делали, но в обратном порядке выполняя шаги.

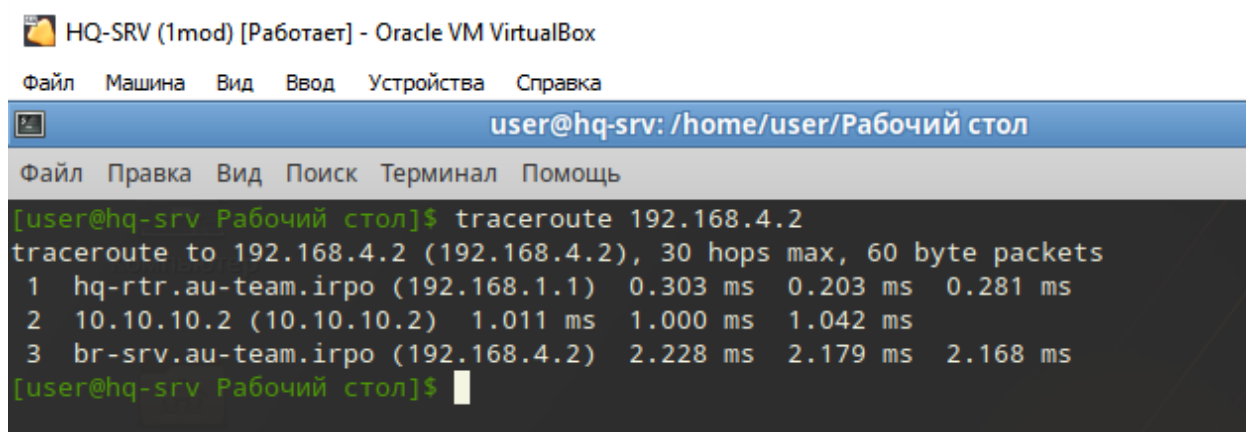
OSPF полностью настроен, теперь пинг должен идти везде и по туннелям, проверим это.

ИНОГДА НУЖНО ЧУТЬ ПОДОЖДАТЬ, ПОКА ПОЯВИТСЯ СОСЕД, ПОЭТОМУ ПИНГ И ТРАССИРОВКА МОГУТ СРАЗУ НЕ ПОЙТИ, ПРОВЕРЯЙТЕ СОСЕДЕЙ ЧЕРЕЗ VTYSN С ПОМОЩЬЮ КОМАНДЫ:

do show ip ospf neighbor

Сделаем трассировку от сервера **HQ-SRV** до **BR-SRV**:

traceroute 192.168.4.2



The screenshot shows a terminal window titled "HQ-SRV (1mod) [Работает] - Oracle VM VirtualBox". The terminal prompt is "user@hq-srv: /home/user/Рабочий стол". The command "traceroute 192.168.4.2" has been executed. The output shows three hops: 1. hq-rtr.au-team.irpo (192.168.1.1) with 0.303 ms, 0.203 ms, and 0.281 ms. 2. 10.10.10.2 (10.10.10.2) with 1.011 ms, 1.000 ms, and 1.042 ms. 3. br-srv.au-team.irpo (192.168.4.2) with 2.228 ms, 2.179 ms, and 2.168 ms.

```
HQ-SRV (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
user@hq-srv: /home/user/Рабочий стол
Файл  Правка  Вид  Поиск  Терминал  Помощь
[user@hq-srv Рабочий стол]$ traceroute 192.168.4.2
traceroute to 192.168.4.2 (192.168.4.2), 30 hops max, 60 byte packets
 1  hq-rtr.au-team.irpo (192.168.1.1)  0.303 ms  0.203 ms  0.281 ms
 2  10.10.10.2 (10.10.10.2)  1.011 ms  1.000 ms  1.042 ms
 3  br-srv.au-team.irpo (192.168.4.2)  2.228 ms  2.179 ms  2.168 ms
[user@hq-srv Рабочий стол]$
```

Всё отлично проходит **через наш туннель**, поздравляю!

(Доменные имена будут показываться после настройки **DNS**, просто мы это сделали для себя ранее, а вы следуйте пунктам дальше!)

8. Настройка протокола динамической конфигурации хостов (DHCP):

Настройка будет производиться на **HQ-RTR**!

Использовать в качестве **DHCP** мы будем **dnsmasq**, служба, которой по умолчанию нет в наших ОС Российского производства.

Ещё нам нужно добавить в **resolv.conf** сервер **Google**, иначе мы не сможем обновить репозитории, поэтому идём его редактировать следующей командой:

mcedit /etc/resolv.conf

И добавляем следующую строку в него:

nameserver 8.8.8.8


```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 2.7.4                               Файл: /etc/resolv.conf

nameserver 8.8.8.8
```

Обновим пакеты и установим её командами:

apt update

apt install dnsmasq

```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
ены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PUBKEY 0E98404D386FA1D9 NO_P
EY DCC9EFBF77E11517
root@hq-rtr:~# apt install dnsmasq
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Предлагаемые пакеты:
  resolvconf
Пакеты, которые будут обновлены:
  dnsmasq
обновлено 1, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 274 пакетов не обно
о.
Необходимо скачать 16,4 кБ архивов.
После данной операции, объём занятого дискового пространства возрастёт на 3+072 Б.
Пол:1 http://deb.debian.org/debian buster/main amd64 dnsmasq all 2.80-1+deb10u1 [16,4 kB]
Получено 16,4 кБ за 0с (70,8 кБ/с)
(Чтение базы данных ... на данный момент установлено 66970 файлов и каталогов.)
Подготовка к распаковке .../dnsmasq_2.80-1+deb10u1_all.deb ...
Распаковывается dnsmasq (2.80-1+deb10u1) на замену (2.76-5+deb9u3) ...
Настраивается пакет dnsmasq (2.80-1+deb10u1) ...
Устанавливается новая версия файла настройки /etc/init.d/dnsmasq ...

Файл настройки «/etc/dnsmasq.conf»
==> Изменён с момента установки (вами или сценарием).
==> Автор пакета предоставил обновлённую версию.
Что нужно сделать? Есть следующие варианты:
  Y или I : установить версию, предлагаемую сопровождающим пакета
  N или O : оставить установленную на данный момент версию
  D       : показать различия между версиями
  Z       : запустить оболочку командной строки для проверки ситуации
По умолчанию сохраняется текущая версия файла настройки.
*** dnsmasq.conf (Y/I/N/O/D/Z) [по умолчанию N] ? Y
Устанавливается новая версия файла настройки /etc/dnsmasq.conf ...
Обрабатываются триггеры для systemd (232-25+deb9u14astra.ce11) ...
root@hq-rtr:~# _
```

Затем зайдём в настройки конфигурационного файла командой:

mcedit /etc/dnsmasq.conf

И внесём в него следующие строки (можно прямо в начало файла):

no-resolv

dhcp-range=192.168.2.2,192.168.2.14,9999h

dhcp-option=3,192.168.2.1

dhcp-option=6,192.168.1.2

interface=eth1.200

```
demo.peacedeath.su:7015 QEMU (HQ-RTR) - noVNC
/etc/dnsmasq.conf [----] 0 L: [ 1+ 5 6/675] *(123 /26842b) 0010 0x00A
no-resolv
dhcp-range=192.168.2.2,192.168.2.14,9999h
dhcp-option=3,192.168.2.1
dhcp-option=6,192.168.1.2
interface=eth1.200
```

Затем перезапускаем службу и посмотрим её статус:

systemctl restart dnsmasq

systemctl status dnsmasq

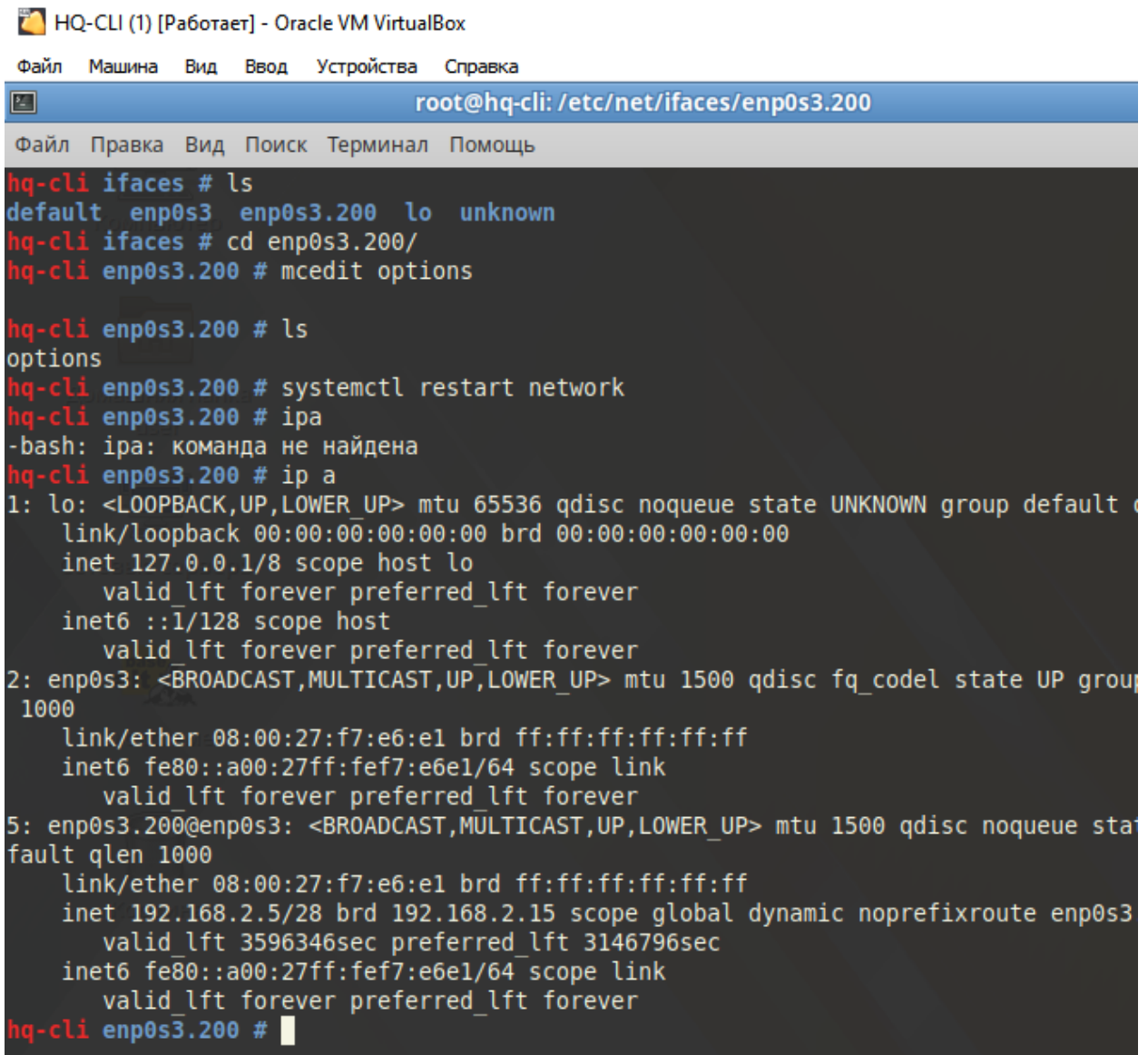
```
root@hq-rtr:~# systemctl restart dnsmasq
root@hq-rtr:~# systemctl status dnsmasq
• dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server
  Loaded: loaded (/lib/systemd/system/dnsmasq.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2024-09-26 10:27:21 +07; 6s ago
    Process: 1231 ExecStop=/etc/init.d/dnsmasq systemd-stop-resolvconf (code=exited, status=0/SUCCESS)
    Process: 1257 ExecStartPost=/etc/init.d/dnsmasq systemd-start-resolvconf (code=exited, status=0/SUCCESS)
    Process: 1243 ExecStart=/etc/init.d/dnsmasq systemd-exec (code=exited, status=0/SUCCESS)
    Process: 1242 ExecStartPre=/usr/sbin/dnsmasq --test (code=exited, status=0/SUCCESS)
  Main PID: 1256 (dnsmasq)
    Tasks: 1 (limit: 4915)
   CGroup: /system.slice/dnsmasq.service
           └─1256 /usr/sbin/dnsmasq -x /run/dnsmasq/dnsmasq.pid -u dnsmasq -7 /etc/dnsmasq.d,.dp

сен 26 10:27:21 hq-rtr.au-team.irpo systemd[1]: Stopped dnsmasq - A lightweight DHCP and caching
сен 26 10:27:21 hq-rtr.au-team.irpo systemd[1]: Starting dnsmasq - A lightweight DHCP and caching
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1242]: dnsmasq: syntax check OK.
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1256]: started, version 2.76 cachesize 150
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1256]: compile time options: IPv6 GNU-getopt DBus i1
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1256]: warning: no upstream servers configured
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq-dhcp[1256]: DHCP, IP range 192.168.2.2 -- 192.168.2.
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq-dhcp[1256]: DHCP, sockets bound exclusively to inter
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1256]: read /etc/hosts - 5 addresses
сен 26 10:27:21 hq-rtr.au-team.irpo systemd[1]: Started dnsmasq - A lightweight DHCP and caching
lines 1-22/22 (END)
```

Проверим работу службы на **HQ-CLI**, перезапускаем службу **network** на нём и посмотрим, выдался ли нам адрес:

systemctl restart network

ip a



```

HQ-CLI (1) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@hq-cli: /etc/net/ifaces/enp0s3.200
Файл  Правка  Вид  Поиск  Терминал  Помощь
hq-cli ifaces # ls
default enp0s3 enp0s3.200 lo unknown
hq-cli ifaces # cd enp0s3.200/
hq-cli enp0s3.200 # mcedit options

hq-cli enp0s3.200 # ls
options
hq-cli enp0s3.200 # systemctl restart network
hq-cli enp0s3.200 # ipa
-bash: ipa: команда не найдена
hq-cli enp0s3.200 # ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default c
    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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
    1000
    link/ether 08:00:27:f7:e6:e1 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fef7:e6e1/64 scope link
        valid_lft forever preferred_lft forever
5: enp0s3.200@enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue stat
    fault qlen 1000
    link/ether 08:00:27:f7:e6:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.5/28 brd 192.168.2.15 scope global dynamic noprefixroute enp0s3
        valid_lft 3596346sec preferred_lft 3146796sec
    inet6 fe80::a00:27ff:fef7:e6e1/64 scope link
        valid_lft forever preferred_lft forever
hq-cli enp0s3.200 #
```

enp0s3.200 на **HQ-CLI** успешно получил адрес из диапазона.

9. Настройка DNS для офисов HQ и BR:

Для начала необходимо отключить несовместимую службу **bind** если она есть, командой

systemctl disable --now bind

Для работы **DNS** есть служба **dnsmasq** (она же и для **DHCP**)

Установим её на наш сервер **HQ-SRV** (если есть, как у нас, то переходите к следующему шагу).

Ещё нам нужно добавить в **resolv.conf** сервер **Google**, иначе мы не сможем обновить репозитории, поэтому идём его редактировать следующей командой:

mcedit /etc/resolv.conf

И добавляем следующую строку в него:


nameserver 8.8.8.8

Обновим пакеты и установим её командами:

apt-get update

apt-get install dnsmasq (Установка пакета dnsmasq)

systemctl enable --now dnsmasq (Добавление службы в автозапуск)

 HQ-SRV [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

```
[root@hq-srv ~]# apt-get install dnsmasq
Reading Package Lists... Done
Building Dependency Tree... Done
dnsmasq is already the newest version.
0 upgraded, 0 newly installed, 0 removed and 120 not upgraded.
[root@hq-srv ~]#
```

Проверим её состояние перед работой:

systemctl status dnsmasq

```
[root@hq-srv ~]# systemctl status dnsmasq
dnsmasq.service - A lightweight DHCP and caching DNS server
   Loaded: loaded (/lib/systemd/system/dnsmasq.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2024-09-12 11:48:13 MSK; 8min ago
   Process: 6722 ExecStartPost=/usr/sbin/dnsmasq-helper poststart (code=exited, status=0/SUCCESS)
   Main PID: 6721 (dnsmasq)
     Tasks: 1 (limit: 4680)
    Memory: 352.0K
       CPU: 55ms
   CGroup: /system.slice/dnsmasq.service
           └─ 6721 /usr/sbin/dnsmasq --bind-interfaces --interface lo -s au-team.irpo -u _dnsmasq

Sep 12 11:48:13 hq-srv.au-team.irpo systemd[1]: Starting A lightweight DHCP and caching DNS server.
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: started, version 2.90 cachesize 150
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: compile time options: IPv6 GNU-getopt no-DBus no>
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: ignoring nameserver 192.168.1.2 - local interface>
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: using nameserver 8.8.8.8#53
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: read /etc/hosts - 15 names
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq-helper[6870]: Setup resolv.conf for local resolver: suc>
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq-helper[6722]: Setup resolv.conf for local resolver: [ DO>
Sep 12 11:48:13 hq-srv.au-team.irpo systemd[1]: Started A lightweight DHCP and caching DNS server.
lines 1-20/20 (END)
```

Затем откроем файл для редактирования конфигурации нашего DNS-сервера:

mcedit /etc/dnsmasq.conf

И добавляем в неё строки (для удобства прям с первой строки файла):

no-resolv (не будет использовать /etc/resolv.conf)

domain=au-team.irpo

server=8.8.8.8 (адрес общедоступного DNS-сервера)

interface=* (на каком интерфейсе будет работать служба)

address=/hq-rtr.au-team.irpo/192.168.1.1

ptr-record=1.1.168.192.in-addr.arpa,hq-rtr.au-team.irpo

cname=moodle.au-team.irpo,hq-rtr.au-team.irpo

cname=wiki.au-team.irpo,hq-rtr.au-team.irpo

address=/br-rtr.au-team.irpo/192.168.4.1

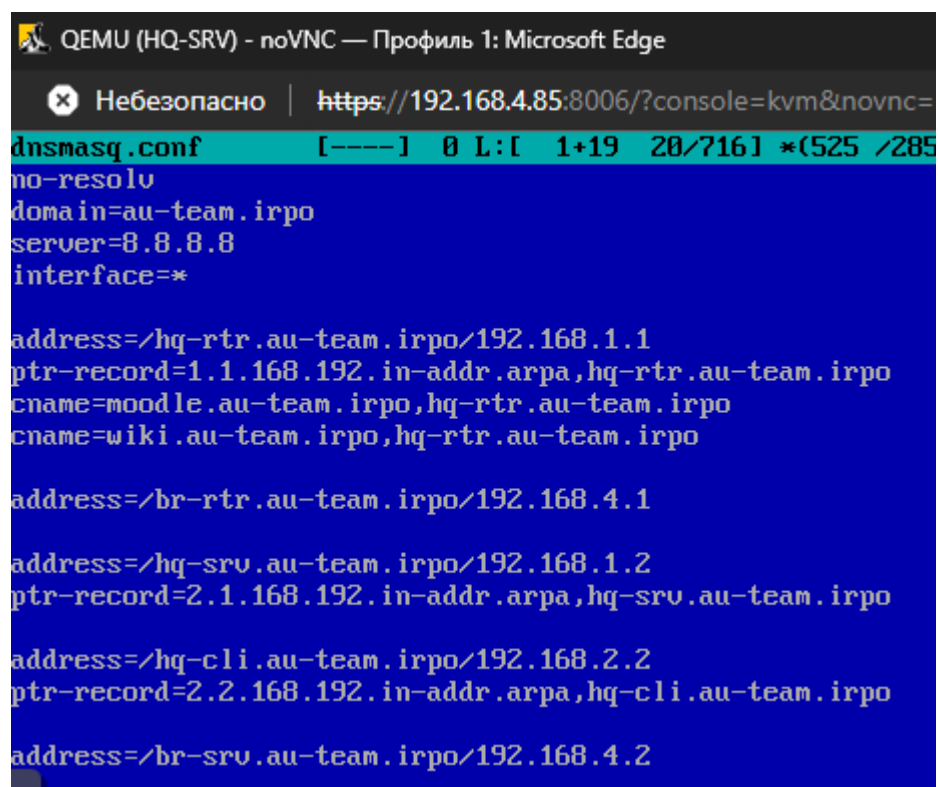
address=/hq-srv.au-team.irpo/192.168.1.2

ptr-record=2.1.168.192.in-addr.arpa,hq-srv.au-team.irpo

address=/hq-cli.au-team.irpo/192.168.2.2 (Смотрите адрес на **HQ-CLI**, т.к он выдаётся по DHCP)

ptr-record=2.2.168.192.in-addr.arpa,hq-cli.au-team.irpo

address=/br-srv.au-team.irpo/192.168.4.2

A screenshot of a QEMU console window titled "QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge". The address bar shows a URL: "https://192.168.4.85:8006/?console=kvm&novnc=". The console output shows the configuration for dnsmasq.conf. The first line is "no-resolv". The second line is "domain=au-team.irpo". The third line is "server=8.8.8.8". The fourth line is "interface=*". The fifth line is "address=/hq-rtr.au-team.irpo/192.168.1.1". The sixth line is "ptr-record=1.1.168.192.in-addr.arpa,hq-rtr.au-team.irpo". The seventh line is "cname=moodle.au-team.irpo,hq-rtr.au-team.irpo". The eighth line is "cname=wiki.au-team.irpo,hq-rtr.au-team.irpo". The ninth line is "address=/br-rtr.au-team.irpo/192.168.4.1". The tenth line is "address=/hq-srv.au-team.irpo/192.168.1.2". The eleventh line is "ptr-record=2.1.168.192.in-addr.arpa,hq-srv.au-team.irpo". The twelfth line is "address=/hq-cli.au-team.irpo/192.168.2.2". The thirteenth line is "ptr-record=2.2.168.192.in-addr.arpa,hq-cli.au-team.irpo". The fourteenth line is "address=/br-srv.au-team.irpo/192.168.4.2".

```
QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=
dnsmasq.conf [-----] 0 L: [ 1+19 20/716] *(525 /285
no-resolv
domain=au-team.irpo
server=8.8.8.8
interface=*

address=/hq-rtr.au-team.irpo/192.168.1.1
ptr-record=1.1.168.192.in-addr.arpa,hq-rtr.au-team.irpo
cname=moodle.au-team.irpo,hq-rtr.au-team.irpo
cname=wiki.au-team.irpo,hq-rtr.au-team.irpo

address=/br-rtr.au-team.irpo/192.168.4.1

address=/hq-srv.au-team.irpo/192.168.1.2
ptr-record=2.1.168.192.in-addr.arpa,hq-srv.au-team.irpo

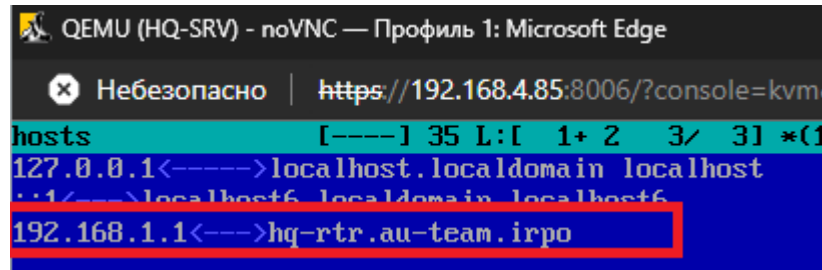
address=/hq-cli.au-team.irpo/192.168.2.2
ptr-record=2.2.168.192.in-addr.arpa,hq-cli.au-team.irpo

address=/br-srv.au-team.irpo/192.168.4.2
```

Сохраняем файл нажатием кнопки **F2**, а затем выход с помощью **F10**.

Теперь необходимо добавить строку **192.168.1.1 hq-rtr.au-team.irpo** в файл `/etc/hosts`:

mcedit /etc/hosts



```
QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.4.85:8006/?console=kvm6
hosts [----] 35 L:[ 1+ 2 3/ 3] *(1
127.0.0.1<----->localhost.localdomain localhost
::1<----->localhost6.localdomain localhost6
192.168.1.1<--->hq-rtr.au-team.irpo
```

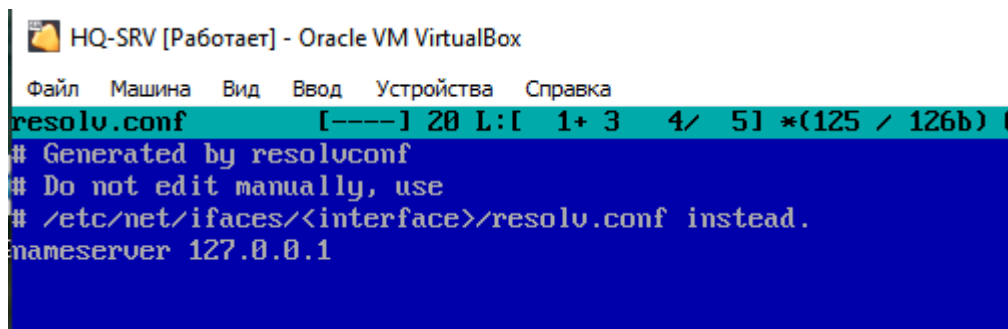
Сохраняем файл, выходим из редактора.

И также нужно изменить файл **resolv.conf**:

mcedit /etc/resolv.conf

Теперь там должен находиться следующий адрес:

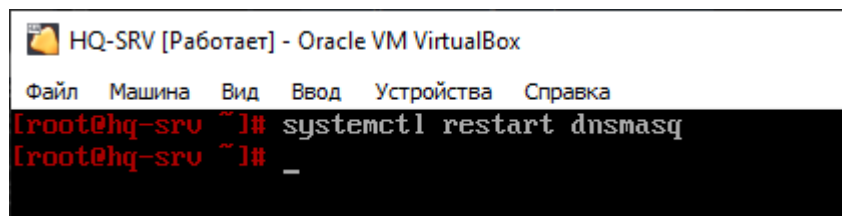
127.0.0.1



```
HQ-SRV [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
resolv.conf [----] 20 L:[ 1+ 3 4/ 5] *(125 / 126b) (
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/iface/<interface>/resolv.conf instead.
nameserver 127.0.0.1
```

Перезапускаем службу командой:

systemctl restart dnsmasq



```
HQ-SRV [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[root@hq-srv ~]# systemctl restart dnsmasq
[root@hq-srv ~]# _
```

Проверим пинг сначала с HQ-SRV на google.com и hq-rtr.au-team.irpo:

ping google.com

ping hq-rtr.au-team.irpo

```

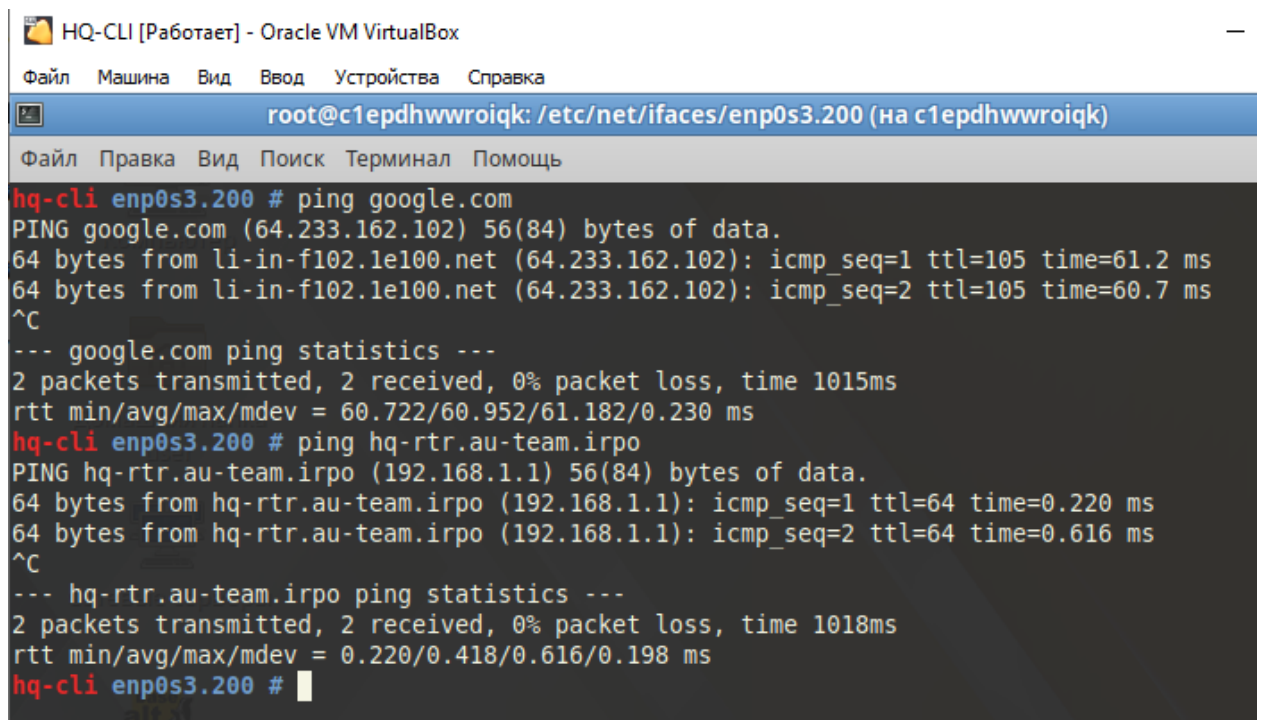
[root@hq-srv ~]# ping google.com
PING google.com (64.233.162.102) 56(84) bytes of data.
64 bytes from li-in-f102.1e100.net (64.233.162.102): icmp_seq=1 ttl=105 time=63.9 ms
64 bytes from li-in-f102.1e100.net (64.233.162.102): icmp_seq=2 ttl=105 time=63.4 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 63.353/63.604/63.855/0.251 ms
[root@hq-srv ~]# ping hq-rtr.au-team.irpo
PING hq-rtr.au-team.irpo (192.168.1.1) 56(84) bytes of data.
64 bytes from hq-rtr.au-team.irpo (192.168.1.1): icmp_seq=1 ttl=64 time=0.406 ms
64 bytes from hq-rtr.au-team.irpo (192.168.1.1): icmp_seq=2 ttl=64 time=0.730 ms
^C
--- hq-rtr.au-team.irpo ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1054ms
rtt min/avg/max/mdev = 0.406/0.568/0.730/0.162 ms
[root@hq-srv ~]#

```

Теперь проверим пинг с HQ-CLI:

ping google.com

ping hq-rtr.au-team.irpo



```

HQ-CLI [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@c1epdhwwroiqr: /etc/net/ifaces/enp0s3.200 (на c1epdhwwroiqr)
Файл  Правка  Вид  Поиск  Терминал  Помощь
hq-cli enp0s3.200 # ping google.com
PING google.com (64.233.162.102) 56(84) bytes of data.
64 bytes from li-in-f102.1e100.net (64.233.162.102): icmp_seq=1 ttl=105 time=61.2 ms
64 bytes from li-in-f102.1e100.net (64.233.162.102): icmp_seq=2 ttl=105 time=60.7 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 60.722/60.952/61.182/0.230 ms
hq-cli enp0s3.200 # ping hq-rtr.au-team.irpo
PING hq-rtr.au-team.irpo (192.168.1.1) 56(84) bytes of data.
64 bytes from hq-rtr.au-team.irpo (192.168.1.1): icmp_seq=1 ttl=64 time=0.220 ms
64 bytes from hq-rtr.au-team.irpo (192.168.1.1): icmp_seq=2 ttl=64 time=0.616 ms
^C
--- hq-rtr.au-team.irpo ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1018ms
rtt min/avg/max/mdev = 0.220/0.418/0.616/0.198 ms
hq-cli enp0s3.200 #

```

И проверим работу CNAME записей с HQ-CLI:

dig moodle.au-team.irpo


```
user@host-15: /home/user
Файл Правка Вид Поиск Терминал Помощь
[user@host-15 ~]$ dig moodle.au-team.irpo

; <<>> DiG 9.16.48 <<>> moodle.au-team.irpo
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5764
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;moodle.au-team.irpo.          IN      A

;; ANSWER SECTION:
moodle.au-team.irpo.  0      IN      CNAME   hq-rtr.au-team.irpo.
hq-rtr.au-team.irpo.  0      IN      A       192.168.1.1

;; Query time: 0 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Sun Sep 29 17:03:08 +07 2024
;; MSG SIZE rcvd: 97

[user@host-15 ~]$
```

dig wiki.au-team.irpo

```
hq-cli ~ # dig wiki.au-team.irpo

; <<>> DiG 9.16.35 <<>> wiki.au-team.irpo
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46488
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;wiki.au-team.irpo.          IN      A

;; ANSWER SECTION:
wiki.au-team.irpo.  0      IN      CNAME   hq-rtr.au-team.irpo.
hq-rtr.au-team.irpo.  0      IN      A       192.168.1.1

;; Query time: 1 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Wed Oct 02 16:22:29 +07 2024
;; MSG SIZE rcvd: 95
```

Наш DNS-сервер настроен.

10. Создание локальных учетных записей:

Создание на **HQ-SRV**:

Для создания пользователя с определённым идентификатором на машине под управлением ОС Alt Linux нужно использовать команду:

useradd sshuser -u 1010

```
[root@hq-srv ~]# useradd sshuser -u 1010
```

Для проверки можно использовать команду:

id sshuser

```
[root@hq-srv ~]# id sshuser
uid=1010(sshuser) gid=1010(sshuser) groups=1010(sshuser)
```

Чтобы задать пользователю новый пароль нужно использовать команду:

passwd sshuser

После чего ввести и подтвердить новый пароль:

P@ssw0rd

```
[root@hq-srv ~]# passwd sshuser
passwd: updating all authentication tokens for user sshuser.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters, digits, and
other characters. You can use a password containing at least 7 characters
from all of these classes, or a password containing at least 8 characters
from just 3 of these 4 classes.
An upper case letter that begins the password and a digit that ends it do not
count towards the number of character classes used.

A passphrase should be of at least 3 words, 11 to 72 characters long, and
contain enough different characters.

Alternatively, if no one else can see your terminal now, you can pick this as
your password: "drag3speech*fog".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@hq-srv ~]#
```

Чтобы **sshuser** мог запускать **sudo** без дополнительной аутентификации, необходимо убрать комментарий с двух строчек в файле **/etc/sudoers**, откроем его командой:

mcedit /etc/sudoers

И уберём комментарий на следующей строке:

WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL

```
##
## User privilege specification
##
# root ALL=(ALL:ALL) ALL

## Uncomment to allow members of group wheel to execute any command
#WHEEL_USERS ALL=(ALL:ALL) ALL

## Same thing without a password
WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL
```

После чего добавить пользователя **sshuser** в группу **wheel**:

usermod -aG wheel sshuser

```
[root@hq-srv ~]# usermod -aG wheel sshuser
[root@hq-srv ~]# id sshuser
uid=1010(sshuser) gid=1010(sshuser) groups=10(wheel),1010(sshuser)
[root@hq-srv ~]#
```

Создание на **BR-SRV**:

Создание пользователя:

```
root@br-srv enp0s3l# useradd sshuser -u 1010
root@br-srv enp0s3l# id sshuser
uid=1010(sshuser) gid=1010(sshuser) groups=1010(sshuser)
root@br-srv enp0s3l#
```

Редактирование пароля:

```

[root@br-srv enp0s3l]# passwd sshuser
passwd: updating all authentication tokens for user sshuser.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters, digits, and
other characters. You can use a password containing at least 7 characters
from all of these classes, or a password containing at least 8 characters
from just 3 of these 4 classes.
An upper case letter that begins the password and a digit that ends it do not
count towards the number of character classes used.

A passphrase should be of at least 3 words, 11 to 72 characters long, and
contain enough different characters.

Alternatively, if no one else can see your terminal now, you can pick this as
your password: "cold&fort&Merger".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.

```

Повышение прав:

```

##
root ALL=(ALL:ALL) ALL

## Uncomment to allow members of group wheel to execute any command
WHEEL_USERS ALL=(ALL:ALL) ALL

## Same thing without a password
WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL

```

```

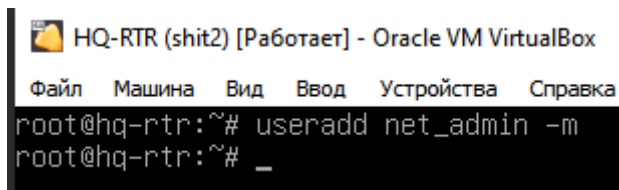
[root@br-srv enp0s3l]# usermod -aG wheel sshuser
[root@br-srv enp0s3l]# id sshuser
uid=1010(sshuser) gid=1010(sshuser) groups=10(wheel),1010(sshuser)
[root@br-srv enp0s3l]#

```

Создание на HQ-RTR:

Для создания пользователя на машине под управлением ОС Astra Linux нужно использовать команду:

useradd net_admin -m



```

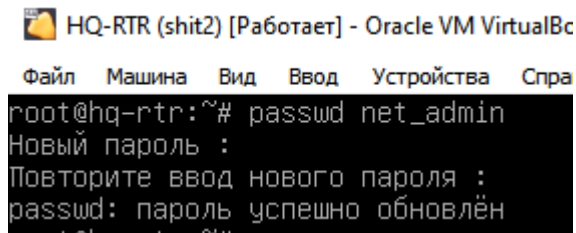
HQ-RTR (shit2) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@hq-rtr:~# useradd net_admin -m
root@hq-rtr:~# _

```

Изменим пароль:

passwd net_admin

P@\$Sword

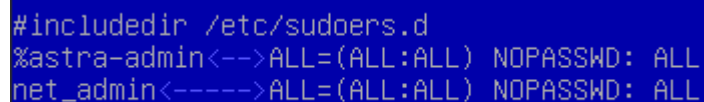


```
HQ-RTR (shit2) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Спра
root@hq-rtr:~# passwd net_admin
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
```

Чтобы **net_admin** мог запускать **sudo** без дополнительной аутентификации необходимо добавить следующую строчку в файл **/etc/sudoers**, в самый конец:

mcedit /etc/sudoers

net_admin ALL=(ALL:ALL) NOPASSWD: ALL

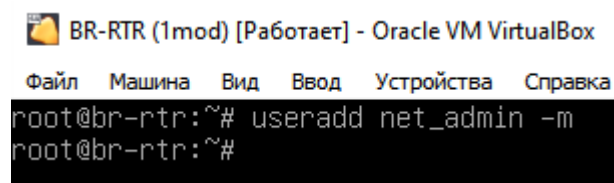


```
#includedir /etc/sudoers.d
%astra-admin<-->ALL=(ALL:ALL) NOPASSWD: ALL
net_admin<----->ALL=(ALL:ALL) NOPASSWD: ALL
```

Создание на **BR-RTR**:

Создание пользователя:

useradd net_admin -m

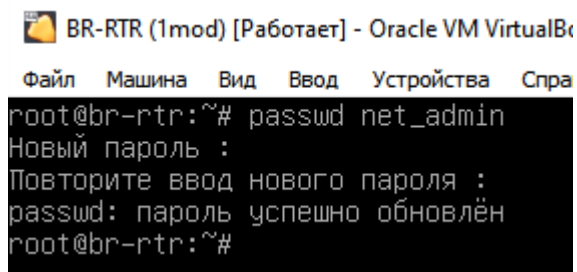


```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@br-rtr:~# useradd net_admin -m
root@br-rtr:~#
```

Изменение пароля:

passwd net_admin

P@\$Sword



Повышение прав:

mcedit /etc/sudoers

net_admin ALL=(ALL:ALL) NOPASSWD: ALL

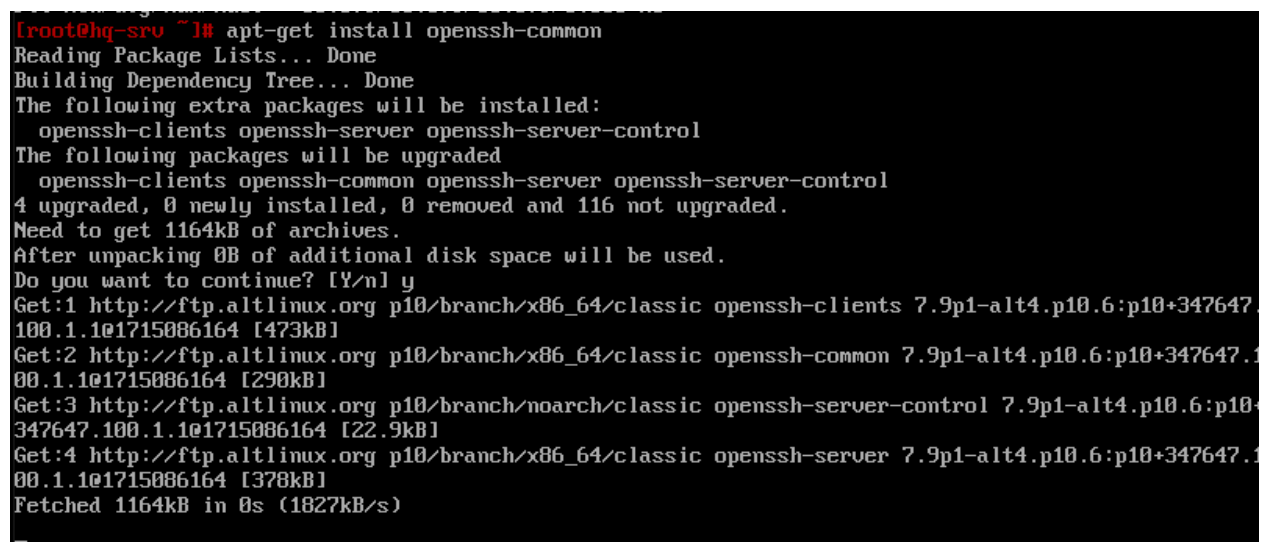
```
#includedir /etc/sudoers.d
%astra-admin<-->ALL=(ALL:ALL) NOPASSWD: ALL
net_admin<----->ALL=(ALL:ALL) NOPASSWD: ALL
```

11. Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV (SSH):

Настройка на HQ-SRV :

Для работы SSH нам понадобится служба **openssh-common**, которой изначально нет, поэтому установим её:

apt-get install openssh-common



Затем зайдём в файл конфигурации для внесения изменений:

mcedit /etc/openssh/sshd_config

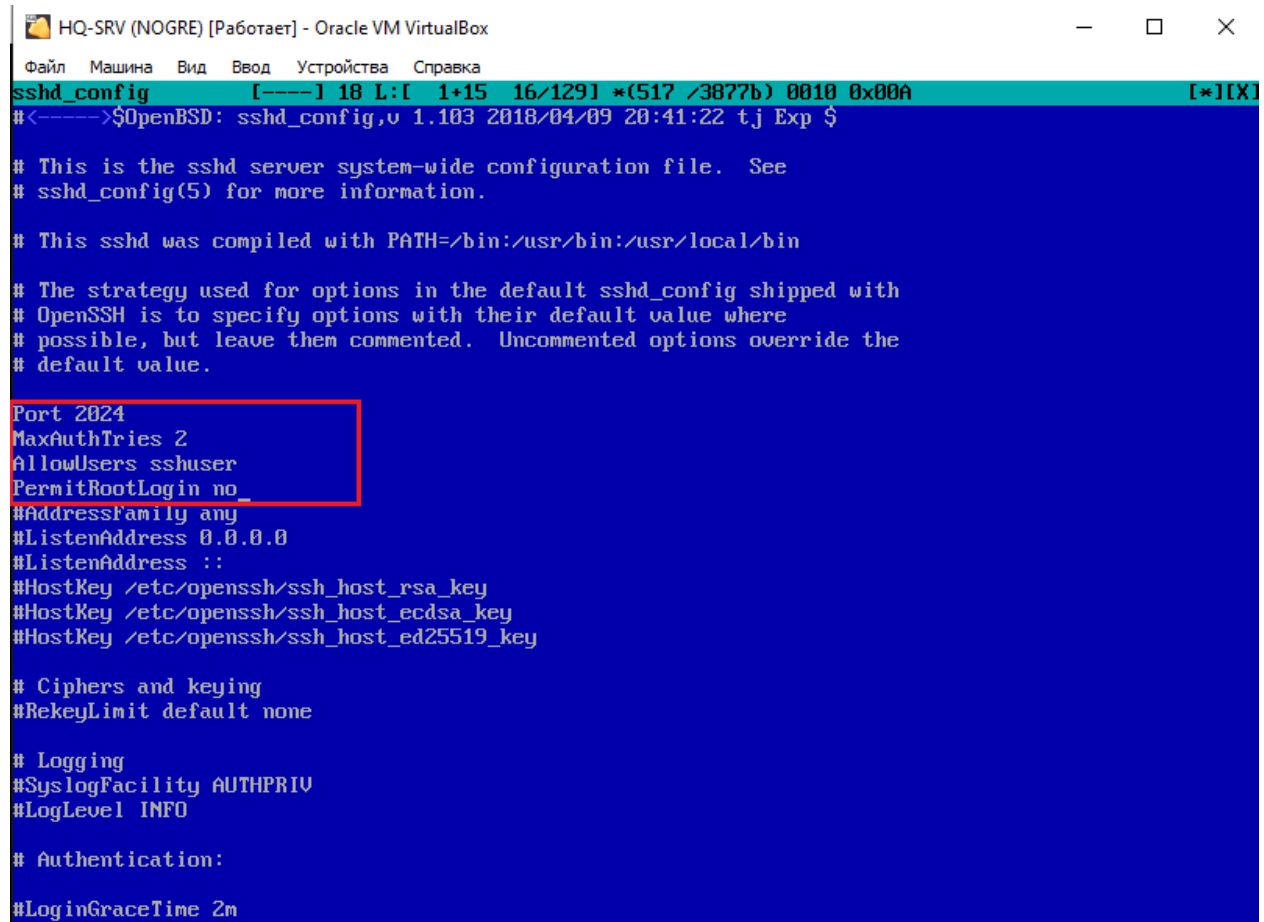
И внесём туда следующие строки:

Port 2024

MaxAuthTries 2

AllowUsers sshuser

PermitRootLogin no



```
sshd_config [-----] 18 L:[ 1+15 16/129] *(517 /3877b) 0010 0x00A [*][X]
#<----->$OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/bin:/usr/bin:/usr/local/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Port 2024
MaxAuthTries 2
AllowUsers sshuser
PermitRootLogin no
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/openssh/ssh_host_rsa_key
#HostKey /etc/openssh/ssh_host_ecdsa_key
#HostKey /etc/openssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
```

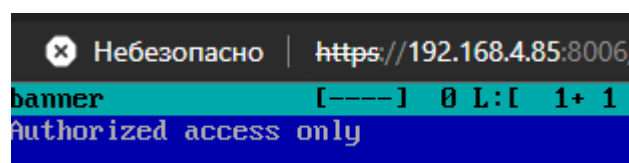
Далее нам нужен баннер.

Создаём его, вносим предложение, которое требуется по заданию через команду:

mcedit /root/banner

Пишем туда следующую строку (ОБЯЗАТЕЛЬНО ПОСЛЕ НЕЁ НАЖАТЬ ENTER, чтобы под ней была пустая строка):

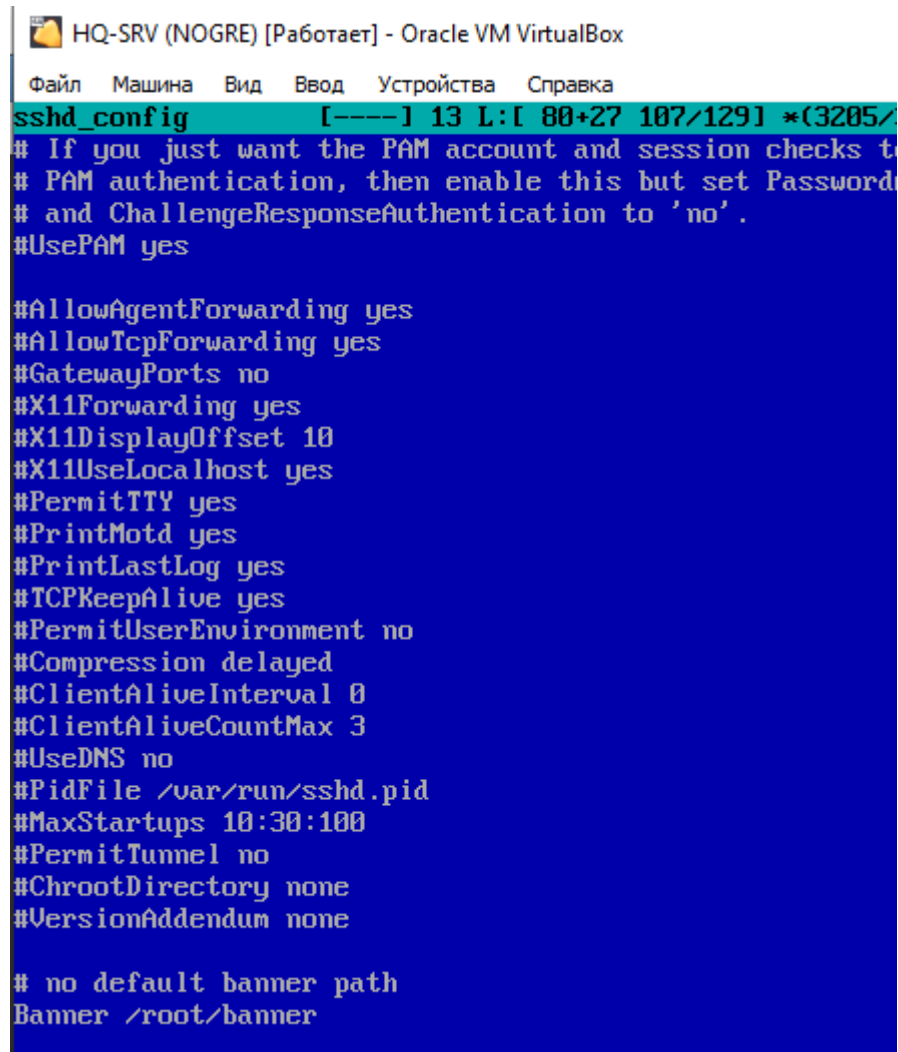
Authorized access only



Затем сохраняем и возвращаемся в **/etc/openssh/sshd_config**.

Добавляем/Редактируем следующую строку:

Banner /root/banner



```
HQ-SRV (NOGRE) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
sshd_config  [----] 13 L:[ 80+27 107/129] *(3205/
# If you just want the PAM account and session checks to
# PAM authentication, then enable this but set Password
# and ChallengeResponseAuthentication to 'no'.
#UsePAM yes

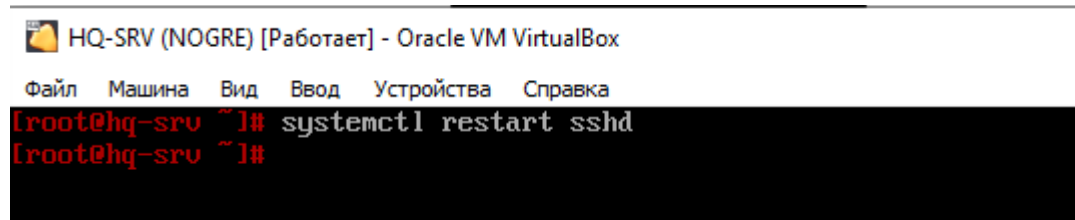
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
Banner /root/banner
```

После внесения изменений, сохраняем и выходим. И делаем перезапуск службы:

systemctl enable --now sshd

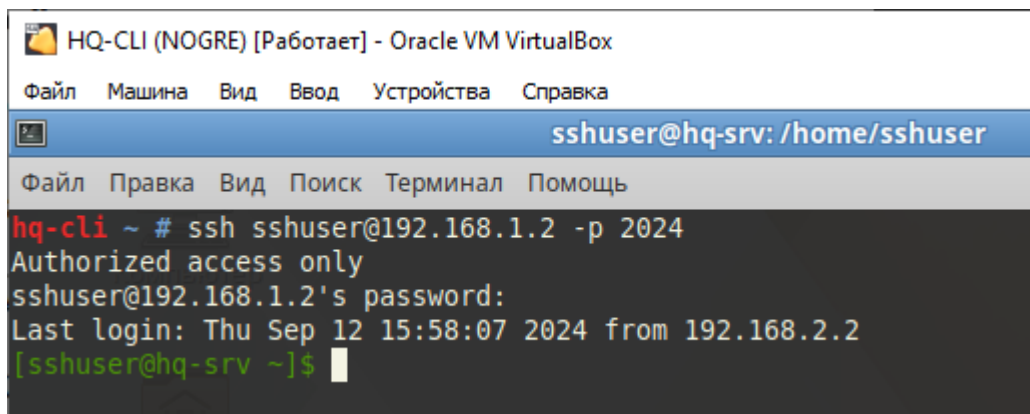
systemctl restart sshd



```
HQ-SRV (NOGRE) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@hq-srv ~]# systemctl restart sshd
[root@hq-srv ~]#
```

Затем попробуем подключиться по SSH через HQ-CLI:

ssh sshuser@192.168.1.2 -p 2024



The screenshot shows a terminal window titled "HQ-CLI (NOGRE) [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar is a status bar showing "sshuser@hq-srv: /home/sshuser". The terminal content shows the command `ssh sshuser@192.168.1.2 -p 2024` being executed. The output is: `Authorized access only`, `sshuser@192.168.1.2's password:`, `Last login: Thu Sep 12 15:58:07 2024 from 192.168.2.2`, and the prompt `[sshuser@hq-srv ~]$`.

sshuser – пользователь, под которым вы подключаетесь

192.168.1.2 – адрес сервера, к которому мы подключаемся (**HQ-SRV**)

-p 2024 – порт, по которому мы подключаемся (мы заменили со стандартного 22 на 2024)

Проделываем все тоже самое и на сервере BR-SRV.

Сервис безопасного удаленного доступа настроен.