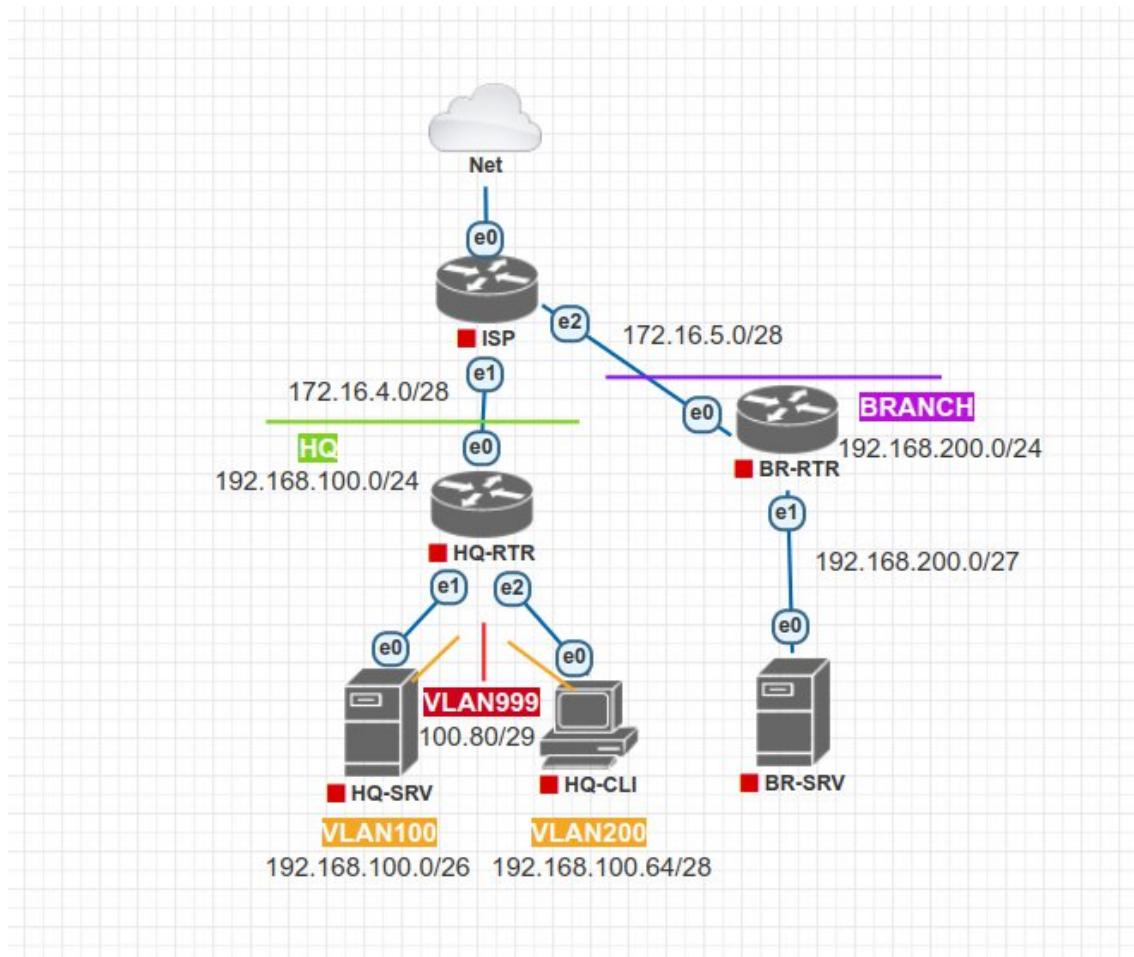


Разбор демонстрационного экзамена 2025 понятным языком

Модуль 1

Создадим в PNetLab такую схему:



(подписи и прочие графические элементы добавлены для лучшего понимания, их у себя на схеме их добавлять не обязательно)

- Net: cloud_nat
- ISP: 1 CPU, 1024 RAM, 3 Ethernet
- HQ-RTR: 1 CPU, 1024 RAM, 4 Ethernet
- BR-RTR: 1 CPU, 1024 RAM, 2 Ethernet
- HQ-SRV: 1 CPU, 1024 RAM, 1 Ethernet
- HQ-CLI: 1 CPU, 1024 RAM, 1 Ethernet
- BR-SRV: 1 CPU, 1024 RAM, 1 Ethernet

Все устройства на базе Linux Debian 10.

АННОТАЦИЯ ОТ АВТОРА

Информация под данный гайд была взята из источника каб-220.рф и адаптирована под ОС Debian 10.

На Debian 10 некоторые пакеты отсутствуют и их придется устанавливать вручную (в гайде описаны какие).

Рекомендации по заданиям:

!! Задание 5 требует установки SELinux, а он устанавливается довольно долго (около 5-10 минут), поэтому рекомендую выполнить его после выполнения основных заданий, чтобы не терять время и не смотреть впустую 5 минут в монитор.

Задание 8 можно выполнить сразу с заданием 2 (динамическая трансляция адресов)

Остальное все можно делать по порядку.

Если что-то не понятно, например с настройкой сети через pmtui, рекомендую просмотреть гайд за 2024 год. Там это гораздо более подробно разобрано (пошагово)

Задание 1. Произведите базовую настройку устройств

- Настройте имена устройств согласно топологии. Используйте полное доменное имя
- На всех устройствах необходимо сконфигурировать IPv4
- IP-адрес должен быть из приватного диапазона, в случае, если сеть локальная, согласно RFC1918
- Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов
- Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 16 адресов
- Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов
- Локальная сеть для управления(VLAN999) должна вмещать не более 8 адресов
- Сведения об адресах занесите в отчёт, в качестве примера используйте Таблицу 3

Настроим имена устройств. Для этого вводим команду

```
hostnamectl set-hostname <полное доменное имя>; exec bash
```

- Для ISP
`hostnamectl set-hostname isp.au-team.irpo; exec bash`
- Для HQ-RTR
`hostnamectl set-hostname hq-rtr.au-team.irpo; exec bash`
- Для HQ-SRV
`hostnamectl set-hostname hq-srv.au-team.irpo; exec bash`
- Для HQ-CLI
`hostnamectl set-hostname hq-cli.au-team.irpo; exec bash`
- Для BR-RTR
`hostnamectl set-hostname br-rtr.au-team.irpo; exec bash`
- Для BR-SRV
`hostnamectl set-hostname br-srv.au-team.irpo; exec bash`

Рассчитаем IP-адресацию.

- Для офиса **HQ** выделим сеть 192.168.100.0/24
- Для офиса **BR** выделим сеть 192.168.200.0/24.
- Сеть офиса **HQ** необходимо разделить на подсети для каждого VLAN.
- Сеть между **HQ**-RTR и **HQ**-SRV – **VLAN100** не более **64** адресов
- Сеть между **HQ**-RTR и **HQ**-CLI – **VLAN200** не более **16** адресов
- Локальная сеть управления **Management** – **VLAN999** не более **8** адресов

Рассчитаем подсети для каждого VLAN офиса **HQ** и адресацию локальной сети офиса **BR**

RFC 1918 обозначил диапазоны IP-адресов, которые невозможно маршрутизировать в Интернете (короче это локальные IP-адреса):

10.0.0.0 — 10.255.255.255 (10/8 префикс);

172.16.0.0 — 172.31.255.255 (172.16/12 префикс);

192.168.0.0 — 192.168.255.255 (192.168/16 префикс).

Получаем примерно следующую таблицу разделения сетей на подсети

Офис HQ

Имя подсети	Количество адресов	IP адрес подсети	Маска подсети	Префикс маски	Диапазон адресов
VLAN100	64	192.168.100.0	255.255.255.192	/26	192.168.100.1 - 192.168.100.62
VLAN200	16	192.168.100.64	255.255.255.240	/28	192.168.100.65 - 192.168.100.78
VLAN999	8	192.168.100.80	255.255.255.248	/29	192.168.100.81 - 192.168.100.86

Офис BR

Имя подсети	Количество адресов	IP адрес подсети	Маска подсети	Префикс маски	Диапазон адресов
HQ	32	192.168.200.0	255.255.255.224	/27	192.168.200.1 - 192.168.200.30

Таблица адресации устройств

Имя устройства	IP- адрес	Шлюз по умолчанию	Сеть
ISP	DHCP		Internet
	172.16.4.1 /28	–	ISP_HQ-RTR
	172.16.5.1 /28	–	ISP-BR-RTR
HQ-RTR	172.16.4.2 /28	172.16.4.1	ISP_HQ-RTR
	192.168.100.1 /26	–	HQ-RTR_HQ-SRV (VLAN100)
	192.168.100.65/28	–	HQ-RTR_HQ_CLI (VLAN200)
	192.168.100.81 /29	–	VLAN999
HQ-SRV	192.168.100.2 /26	192.168.100.1	HQ-RTR_HQ-SRV
HQ-CLI	DHCP	192.168.100.65 (DHCP)	HQ-RTR_HQ-CLI
BR-RTR	172.16.5.2 /28	172.16.5.1	ISP_BR-RTR
	192.168.200.1 /27	–	BR-RTR_BR-SRV
BR-SRV	192.168.200.2 /27	192.168.200.1	BR-RTR_BR-SRV

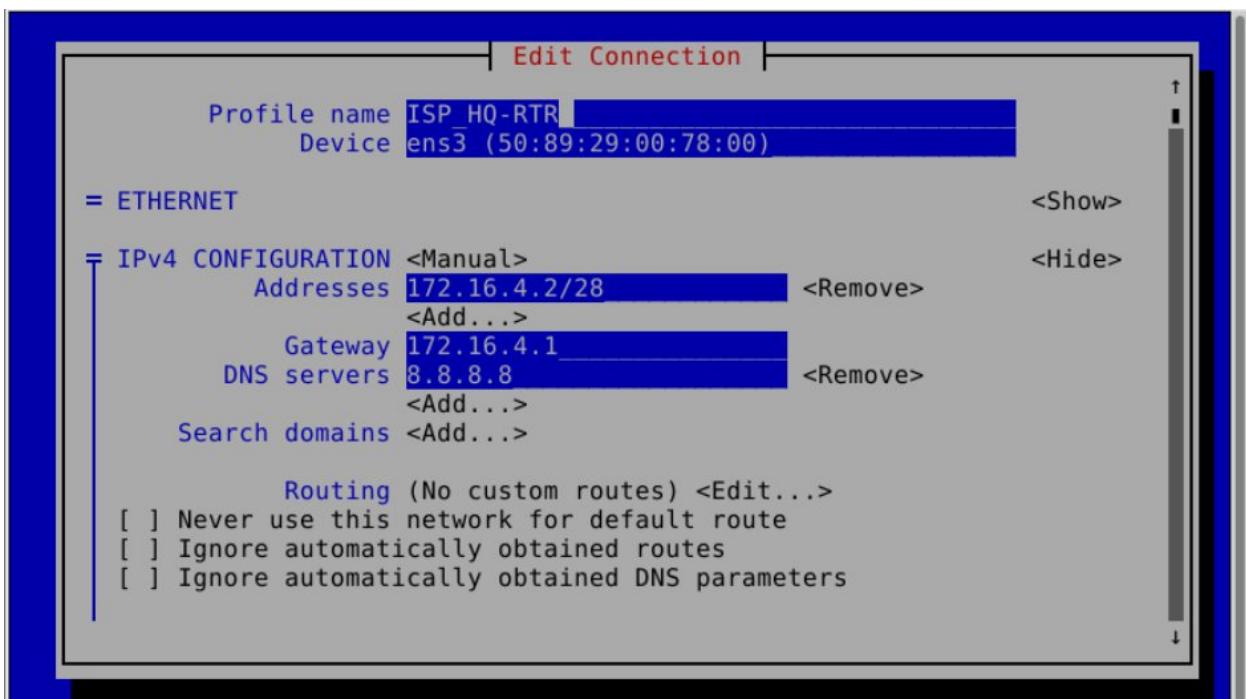
Как мы видим, ISP, HQ-RTR и BR-RTR используют сетевую часть 172.16.*.* с маской подсети 28.

Данная сетевая часть будет использоваться для соединения между ISP и HQ-RTR, а также между ISP и BR-RTR.

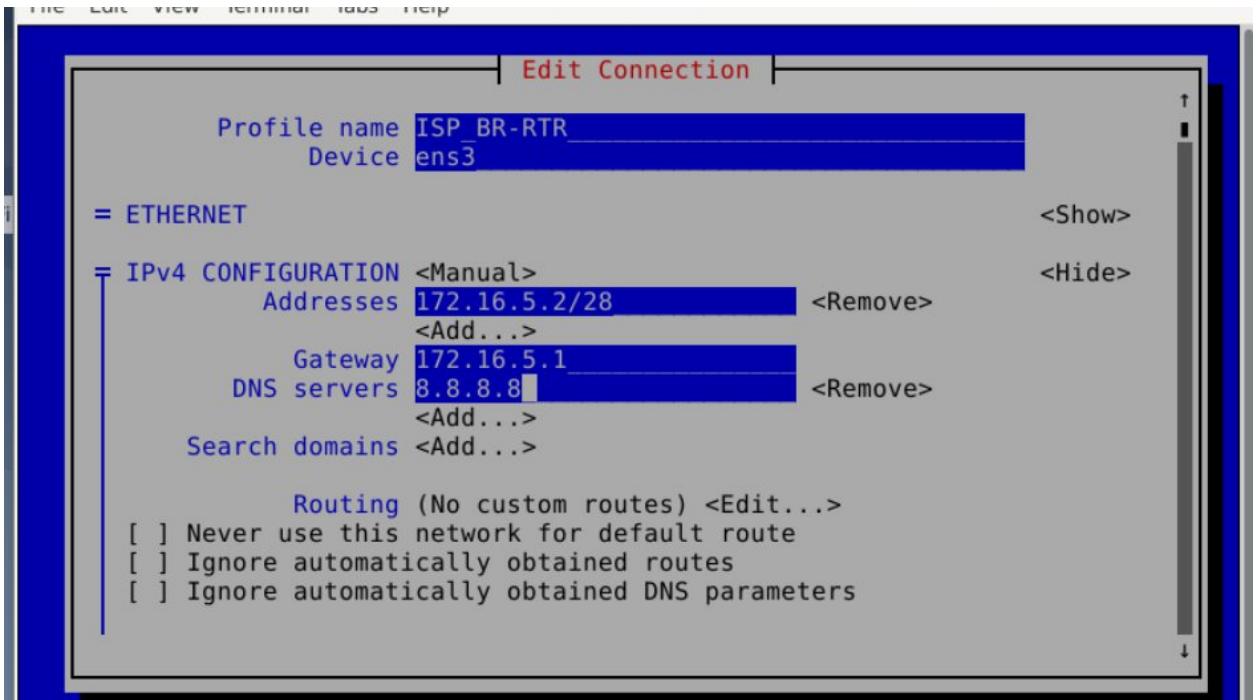
Все что далее, использует сетевую часть 192.168.*.*

Проведем базовую настройку сети.

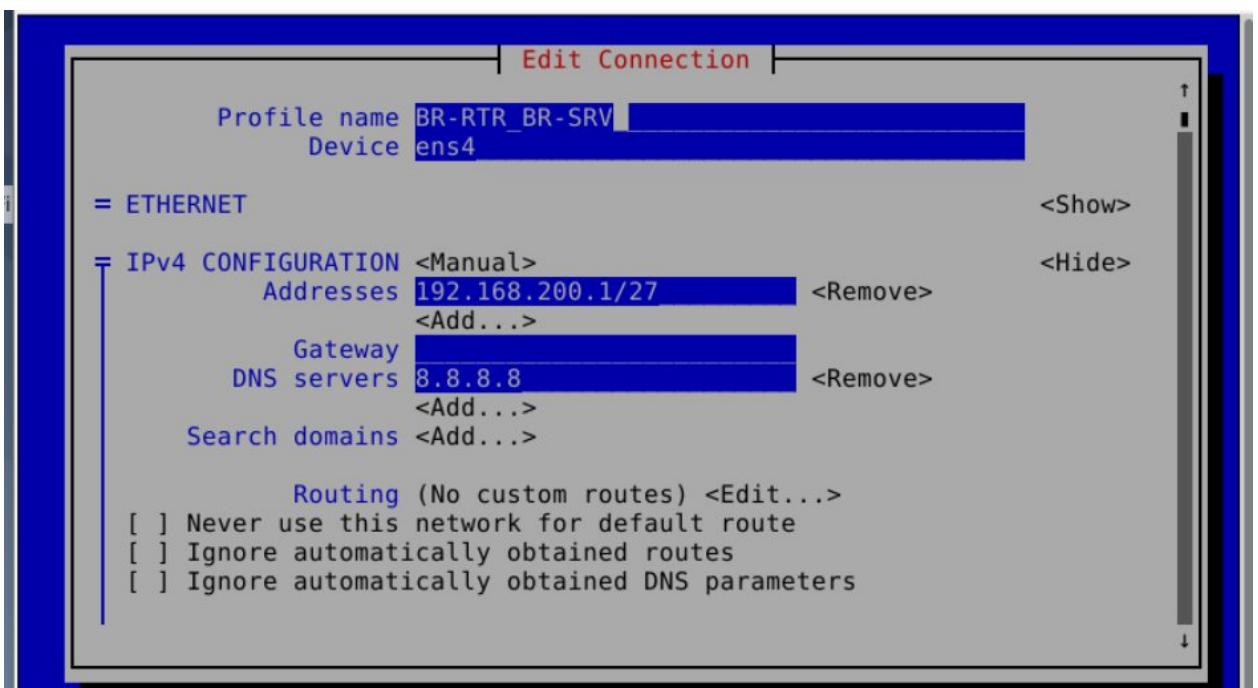
Настраиваем на HQ-RTR ens3.



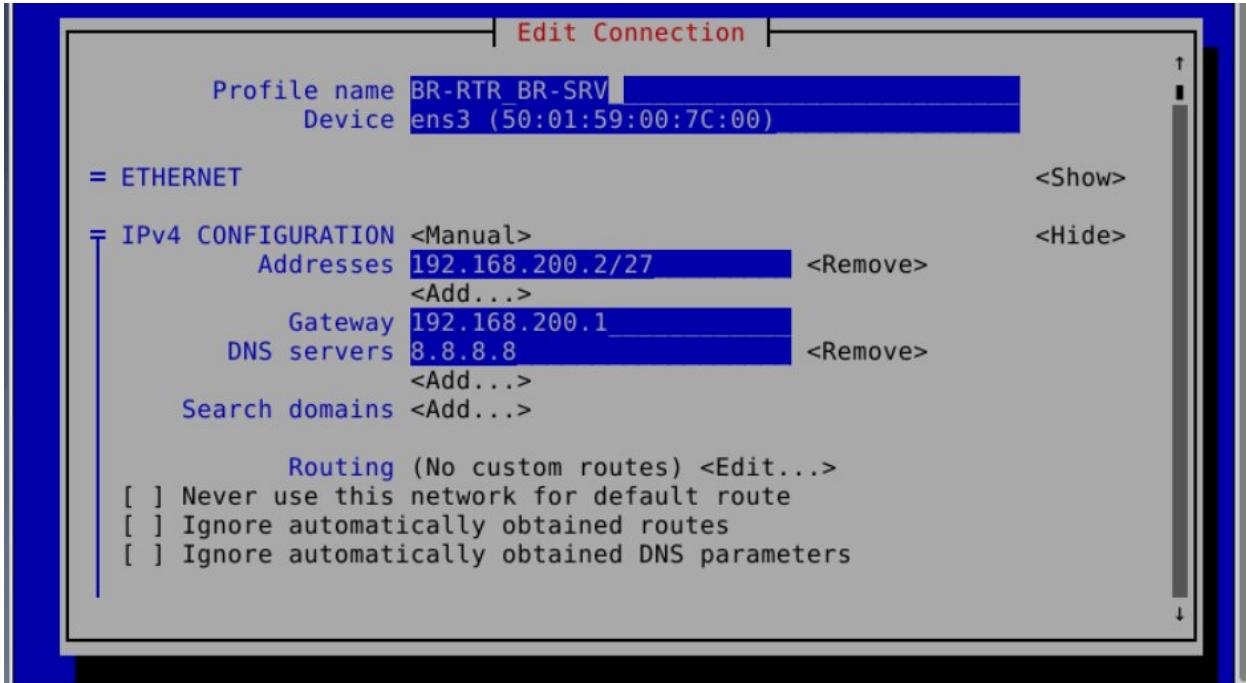
Настраиваем на BR-RTR ens3



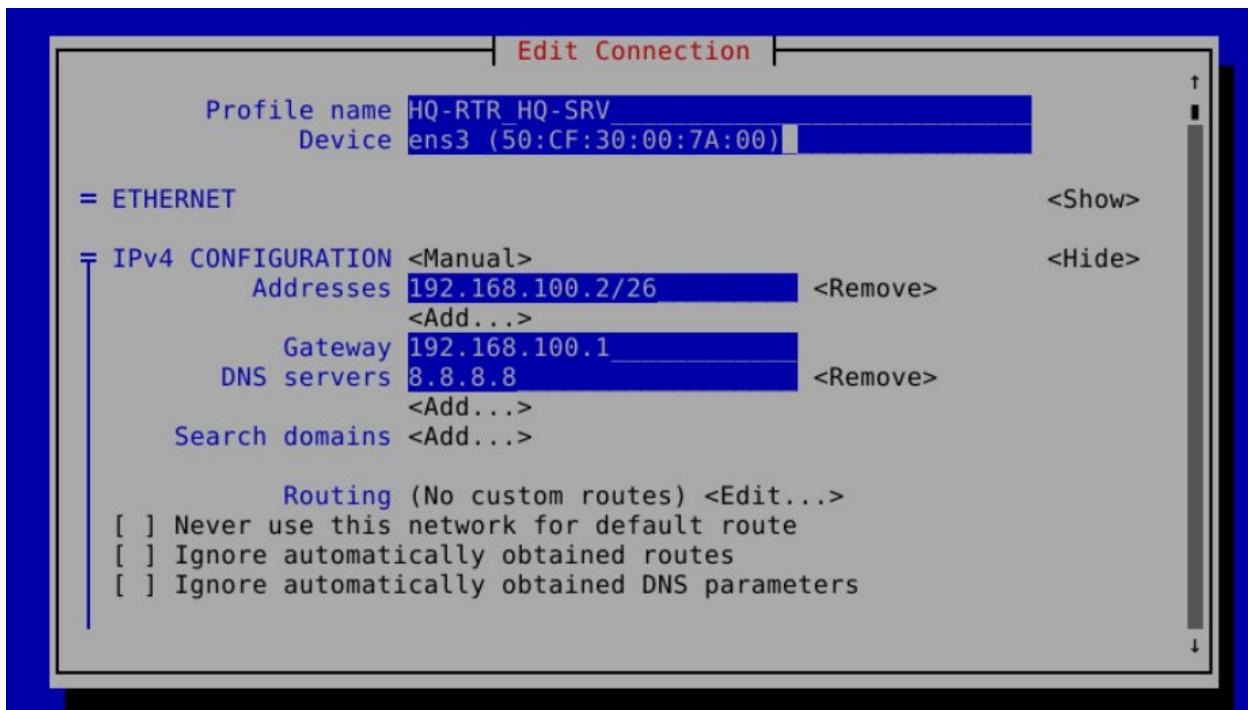
Настраиваем ens4 на BR-RTR. Здесь мы организуем соединение между BR-RTR и BR-SRV. Изменяется сетевая часть на 192.168.*.* с маской подсети /27



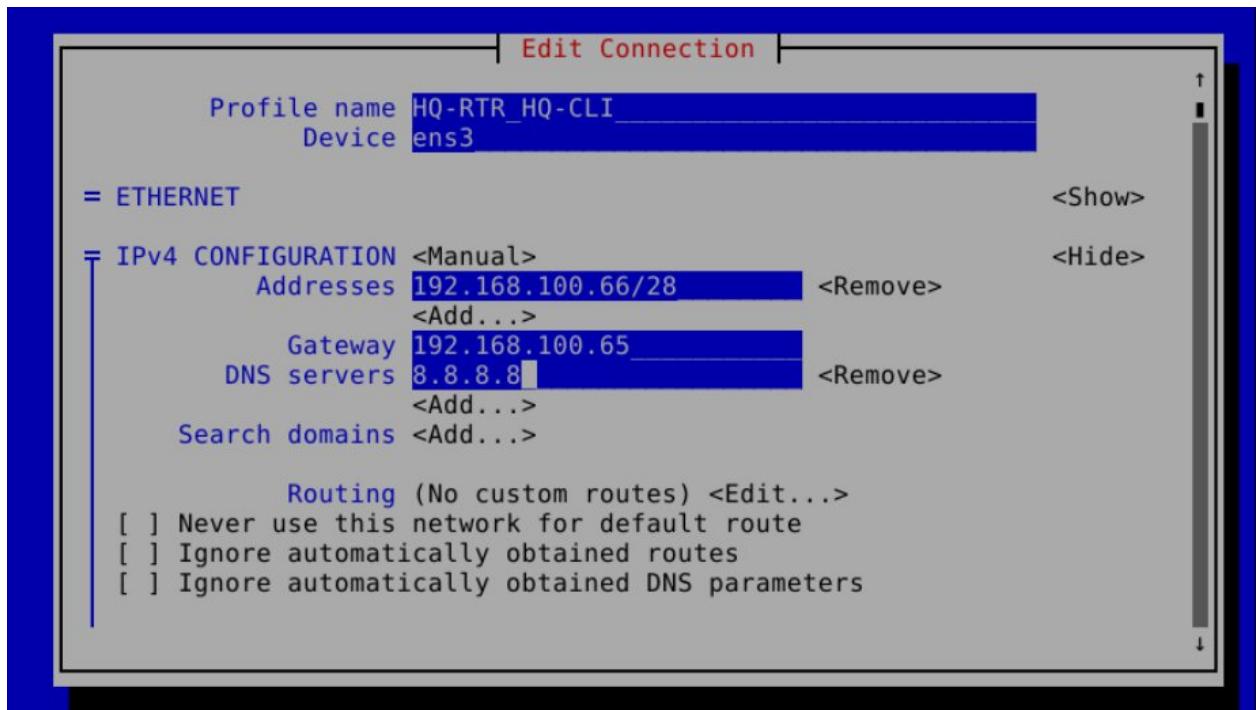
Настраиваем ens3 на BR-SRV.



Настраиваем ens3 на HQ-SRV



Временно настроим ens3 на HQ-CLI, позже его нужно будет перенастроить на получение IP-адреса через DHCP

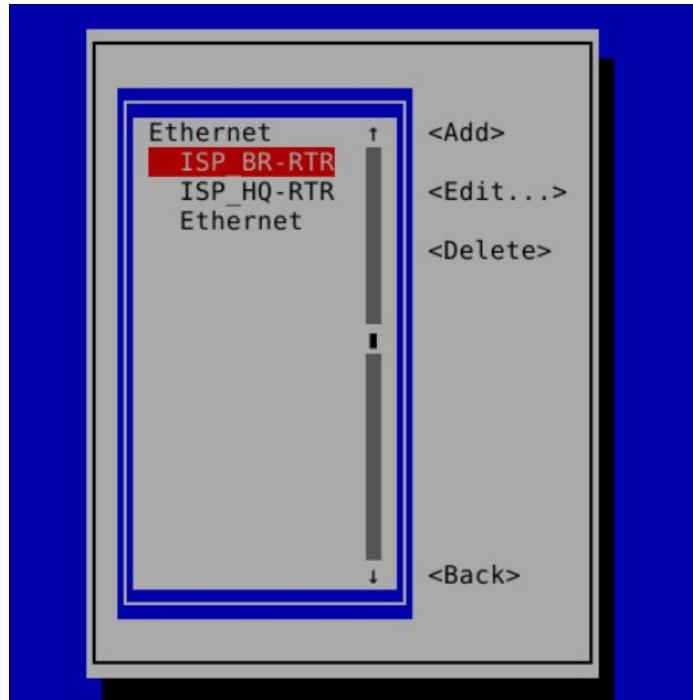


Задание 2. Настройка ISP

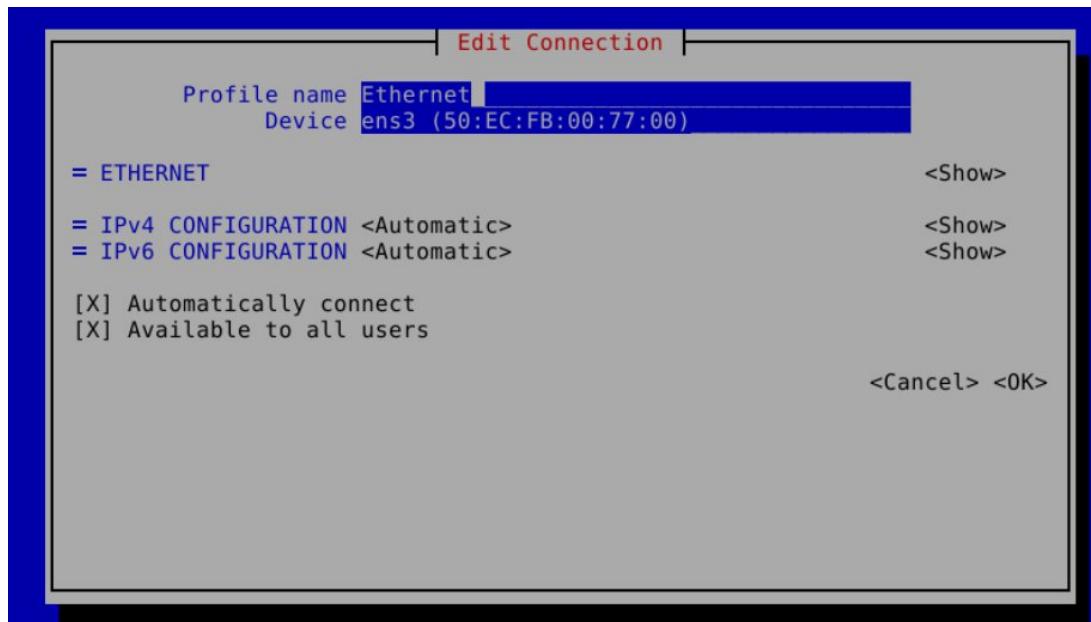
- Настройте адресацию на интерфейсах:
- Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP
- Настройте маршруты по умолчанию там, где это необходимо
- Интерфейс, к которому подключен HQ-RTR, подключен к сети 172.16.4.0/28
- Интерфейс, к которому подключен BR-RTR, подключен к сети 172.16.5.0/28
- На ISP настройте динамическую сетевую трансляцию в сторону HQ-RTR и BR-RTR для доступа к сети Интернет

P.S. На этом шаге можно параллельно сделать задание 8

Настроим сеть на ISP.



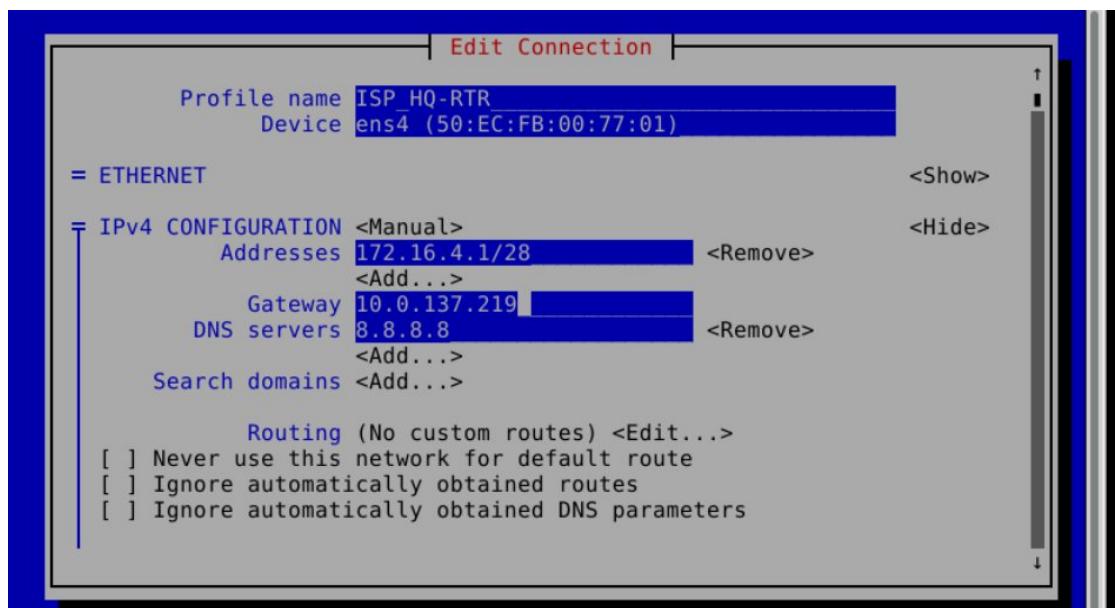
Интерфейс ens3 будет получать адрес по DHCP для Интернета. (IPv4 CONFIGURATION <Automatic>)



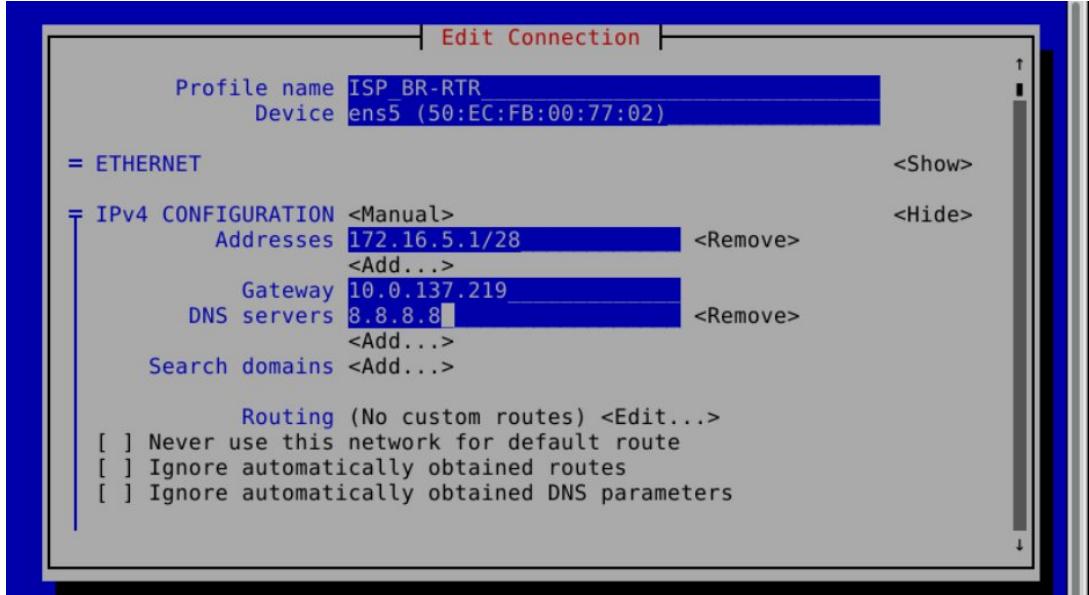
После перезапускаем интерфейс ens3 и командой `ip -c -br a` смотрим наш IP адрес Интернета (он будет использоваться для шлюзов).

```
ens3          UP      10.0.137.219/24 fe80::a932:8d37:4723:e5a2/64
```

Подключение от ISP к **HQ-RTR** (ens4). В Gateway (шлюз) пишем IP-адрес интерфейса ens3 (Интернет).



От ISP к **BR-RTR** (ens5)



После настройки перезапускаем все интерфейсы, проверяем любой из команд ниже:

```
ip -c -br a
```

```
ip -c a
```

```
ip a
```

```
root@isp:~# ip -c -br a
lo          UNKNOWN      127.0.0.1/8 ::1/128
ens3         UP          10.0.137.219/24 fe80::a932:8d37:4723:e5a2/64
ens4         UP          172.16.4.1/28 fe80::52ec:fbff:fe00:7701/64
ens5         UP          172.16.5.1/28 fe80::52ec:fbff:fe00:7702/64
root@isp:~#
```

Настроим динамическую сетевую трансляцию в сторону для доступа к интернету.

На ISP пишем:

```
nano /etc/sysctl.conf
```

Найдем строчку

```
#net.ipv4.ip_forward=1
```

Раскомментируем её

```
net.ipv4.ip_forward=1
```

Применим командой `sysctl -p`

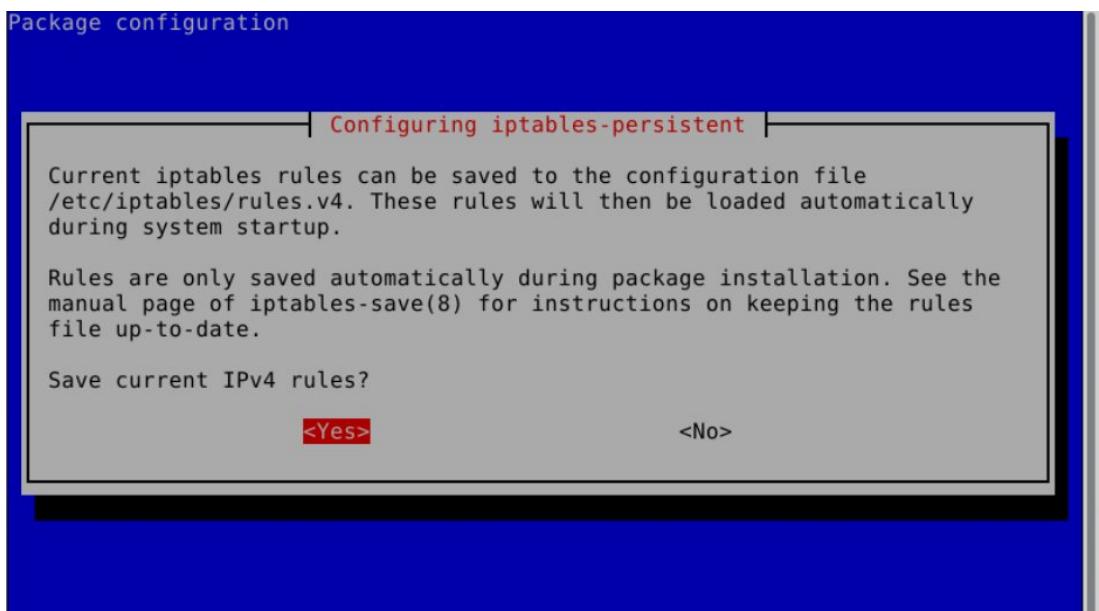
Если все ок, вывод будет: `net.ipv4.ip_forward = 1`

Задаем правила IPTABLES на ISP для маскарадинга пакетов.

```
iptables -t nat -A POSTROUTING -j MASQUERADE
```

Для сохранения правил после перезапуска системы установим пакет на ISP
`iptables-persistent`

Для этого введем обновим пакеты командой `apt update` и введем
команду: `apt install iptables-persistent`



Нажимаем везде “Yes”

Задание 3. Создание локальных учетных записей

- Создайте пользователя `sshuser` на серверах `HQ-SRV` и `BR-SRV`
- Пароль пользователя `sshuser` с паролем `P@ssw0rd`
- Идентификатор пользователя `1010`
- Пользователь `sshuser` должен иметь возможность запускать `sudo` без дополнительной аутентификации.
- Создайте пользователя `net_admin` на маршрутизаторах `HQ-RTR` и `BR-RTR`
- Пароль пользователя `net_admin` с паролем `P@$$word`

Для добавления нового пользователя используем команды `useradd` и `passwd`

Зайдем на `HQ-SRV`, пропишем команды `useradd sshuser -u 1010 -U` и `passwd sshuser`

`P@ssw0rd`

В пароль укажем P@ssw0rd.

Пользователя добавим в группу sudo

```
usermod -aG sudo sshuser
```

Для беспарольного доступа к sudo заходим в /etc/sudoers, командой

```
nano /etc/sudoers (или просто команда visudo) и пишем там строку  
sshuser ALL=NOPASSWD: ALL
```

Тоже самое делаем на BR-SRV

На HQ-RTR и BR-RTR делаем тоже самое, только заменяем пользователя sshuser на net_admin, пользователя создаем без id, и в пароль ставим P@\$\$word.

```
useradd net_admin -U
```

```
passwd net_admin
```

```
P@$$word
```

Пользователя добавим в группу sudo

```
usermod -aG sudo net_admin
```

В /etc/sudoers

```
net_admin ALL=(ALL) NOPASSWD: ALL
```

Выполняем вход под пользователем net_admin (`login net_admin`) и выполняем `sudo -i` или другие команды требующую повышения привилегий до root

Задание 4. Настройте на интерфейсе HQ-RTR в сторону офиса HQ виртуальный коммутатор:

- Сервер HQ-SRV должен находиться в ID VLAN 100
- Клиент HQ-CLI в ID VLAN 200
- Создайте подсеть управления с ID VLAN 999
- Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт

Устанавливаем Openvswitch на HQ-RTR.

```
apt-get update
```

```
apt-get install openvswitch-switch
```

Добавляем в автозагрузку и запускаем

```
systemctl enable --now openvswitch-switch
```

Создаем мост (виртуальный коммутатор) hq-sw

```
ovs-vsctl add-br hq-sw
```

Добавляем порт ens4 к hq-sw и назначаем ему vlan100

```
ovs-vsctl add-port hq-sw ens4 tag=100
```

Добавляем порт ens5 к hq-sw и назначаем ему vlan200

```
ovs-vsctl add-port hq-sw ens5 tag=200
```

Добавляем порт ens6 к hq-sw и назначаем ему vlan999

```
ovs-vsctl add-port hq-sw ens6 tag=999
```

Интерфейсам ens4, ens5, ens6 назначим тип internal (internal - виртуальный сетевой интерфейс, созданный внутри OVS, который поддерживает настройку IP-адреса.)

Добавляем внутренний порт vlan100 к мосту hq-sw в качестве порта доступа к VLAN 100

```
ovs-vsctl add-port hq-sw vlan100 tag=100 -- set interface  
vlan100 type=internal
```

Добавляем внутренний порт vlan200 к мосту hq-sw в качестве порта доступа к VLAN 200

```
ovs-vsctl add-port hq-sw vlan200 tag=200 -- set interface  
vlan200 type=internal
```

Добавляем внутренний порт vlan999 к мосту hq-sw в качестве порта доступа к VLAN 999

```
ovs-vsctl add-port hq-sw vlan999 tag=999 -- set interface  
vlan999 type=internal
```

Перезагружаем openvswitch и NetworkManager

```
systemctl restart openvswitch-switch
```

```
systemctl restart NetworkManager
```

Включаем мост

```
ip link set hq-sw up
```

Назначаем IP-адреса интерфейсам VLAN и включаем их

```
ip a add 192.168.100.1/26 dev vlan100
```

```
ip a add 192.168.100.65/28 dev vlan200
```

```
ip a add 192.168.100.81/29 dev vlan999
```

Запустим VLANы

```
ip link set vlan100 up
```

```
ip link set vlan200 up
```

```
ip link set vlan999 up
```

Если IP-адреса после перезагрузки слетели, повторяем команды с ip link set hq-sw up

Проверяем

```
root@hq-rtr:~# ip -c -br a  
lo          UNKNOWN      127.0.0.1/8 ::1/128  
ens3         UP          172.16.4.2/28 fe80::5289:29ff:fe00:7800/64  
ens4         UP          fe80::1ce:ed37:9f9d:a363/64  
ens5         UP          fe80::6d1c:9a2a:87bf:9e2b/64  
ens6         DOWN  
ovs-system   DOWN  
hq-sw        UNKNOWN      fe80::5289:29ff:fe00:7801/64  
vlan100      UNKNOWN      192.168.100.1/26 fe80::871:b0ff:fe72:1f01/64  
vlan200      UNKNOWN      192.168.100.65/28 fe80::a43b:5fff:fe9c:5e67/64  
vlan999      UNKNOWN      192.168.100.81/29 fe80::24ee:fdff:fe75:712c/64  
root@hq-rtr:~#
```

Попробуем пингануть VLAN200

```
ping 192.168.100.65
root@hq-rtr:~# ping 192.168.100.65
PING 192.168.100.65 (192.168.100.65) 56(84) bytes of data.
64 bytes from 192.168.100.65: icmp_seq=1 ttl=64 time=0.178 ms
64 bytes from 192.168.100.65: icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from 192.168.100.65: icmp_seq=3 ttl=64 time=0.089 ms
^C
--- 192.168.100.65 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 42ms
rtt min/avg/max/mdev = 0.071/0.112/0.178/0.048 ms
root@hq-rtr:~# ping 192.168.100.64
Do you want to ping broadcast? Then -b. If not, check your local firewall rules.
root@hq-rtr:~#
```

Задание 5. Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV

- Для подключения используйте порт 2024
- Разрешите подключения только пользователю sshuser
- Ограничьте количество попыток входа до двух
- Настройте баннер «Authorized access only»

Заходим на **HQ-SRV**.

Так как на Debian не предустановлены утилиты управления SELinux, мы их установим сами:

```
apt install policycoreutils selinux-policy-default selinux-basics
```

Включим SELinux:

```
selinux-activate
```

Перезагрузим **HQ-SRV**

```
reboot
```

```
*** Warning -- SELinux default policy relabel is required.  
*** Relabeling could take a very long time, depending on file  
*** system size and speed of hard drives.  
Warning: Skipping the following R/O filesystems:  
/sys/fs/cgroup  
Relabeling /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /run/lock /sys /sys/fs/cgroup/blkio /sys/fs/cgroup/cpu,cpuacct /sys/fs/cgroup/cpuset /sys/fs/cgroup/devices /sys/fs/cgroup/freezer /sys/fs/cgroup/memory /sys/fs/cgroup/net_cls.net_prio /sys/fs/cgroup/perf_event /sys/fs/cgroup/pids /sys/fs/cgroup/rdma /sys/fs/cgroup/systemd /sys/fs/cgroup/unified /sys/fs/pstore /sys/kernel/debug  
9.3%
```

Может появиться такое сообщение, это норма. SELinux в процессе активации.

Проверим, что SELinux работает командой `sestatus`

```
root@hq-srv:~# sestatus  
SELinux status:                      enabled  
SELinuxfs mount:                     /sys/fs/selinux  
SELinux root directory:              /etc/selinux  
Loaded policy name:                  default  
Current mode:                       permissive  
Mode from config file:              permissive  
Policy MLS status:                  enabled  
Policy deny_unknown status:         allowed  
Memory protection checking:        actual (secure)  
Max kernel policy version:          31
```

Разрешим порт 2024 для работы SSH:

```
semanage port -a -t ssh_port_t -p tcp 2024
```

Переключаем SELinux с режима enforcing в режим permissive:

```
setenforce 0
```

Устанавливаем SSH `apt install openssh-server`

Открываем файл конфигурации SSH `nano /etc/ssh/sshd_config`

Находим директиву Port 22

Снимаем комментарий и прописываем номер порта 2024

```
#Port 22  
Port 2024
```

В этот же файл добавим строку `AllowUsers sshuser`, для возможности подключения только пользователю sshuser

Чуть ниже раскомментируем строку, и поменяем ее значение на 2.

```
#MaxAuthTries 6  
MaxAuthTries 2
```

Это нужно для установки максимального количества попыток ввода пароля до двух.

Создадим баннер. Еще ниже будет закомментированная строчка

```
#Banner none
```

Раскомментируем и укажем путь к баннеру: `/etc/ssh-banner`

```
Banner /etc/ssh-banner
```

Выходим с nano: Ctrl+X, затем y, затем Enter

Пишем `nano /etc/ssh-banner`

Напишем в этом файле:

```
GNU nano 3.2          /etc/ssh-banner
*****
*                         *
* Authorized access only *
*                         *
*****
```

Выходим с nano: Ctrl+X, затем y, затем Enter

Перезапускаем службу SSH командой `systemctl restart sshd`

Попробуем подключиться по SSH с **HQ**-CLI на **HQ**-SRV:

```
ssh sshuser@192.168.100.2 -p 2024
```

```
root@hq-cli:~# ssh sshuser@192.168.100.2 -p 2024
The authenticity of host '[192.168.100.2]:2024 ([192.168.100.2]:2024)' can't be
established.
ECDSA key fingerprint is SHA256:xXY4fQriG+qCcY4w4DLhUGr3VCuhxhmVc74/fREaXFw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.168.100.2]:2024' (ECDSA) to the list of known h
osts.
*****
*                         *
* Authorized access only *
*                         *
*****
```

sshuser@192.168.100.2's password:

```
Linux hq-srv.au-team.irpo 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-0
9-20) x86_64
```

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

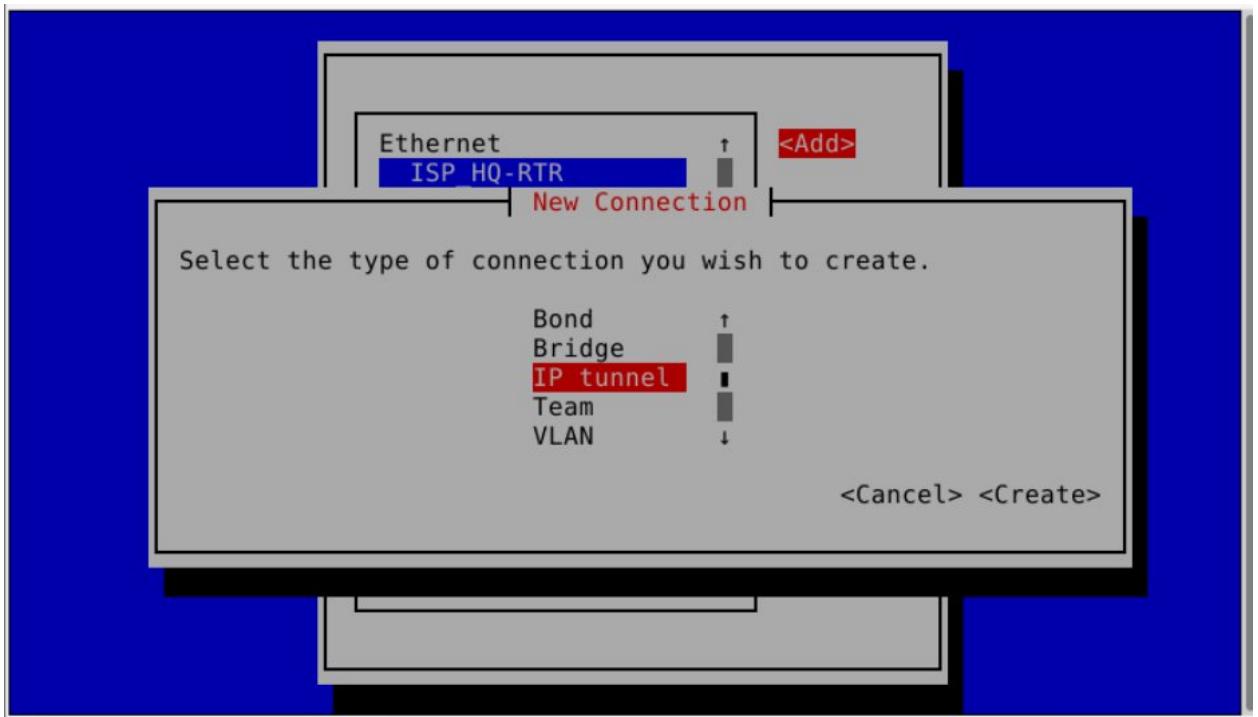
```
Could not chdir to home directory /home/sshuser: No such file or directory
$
```

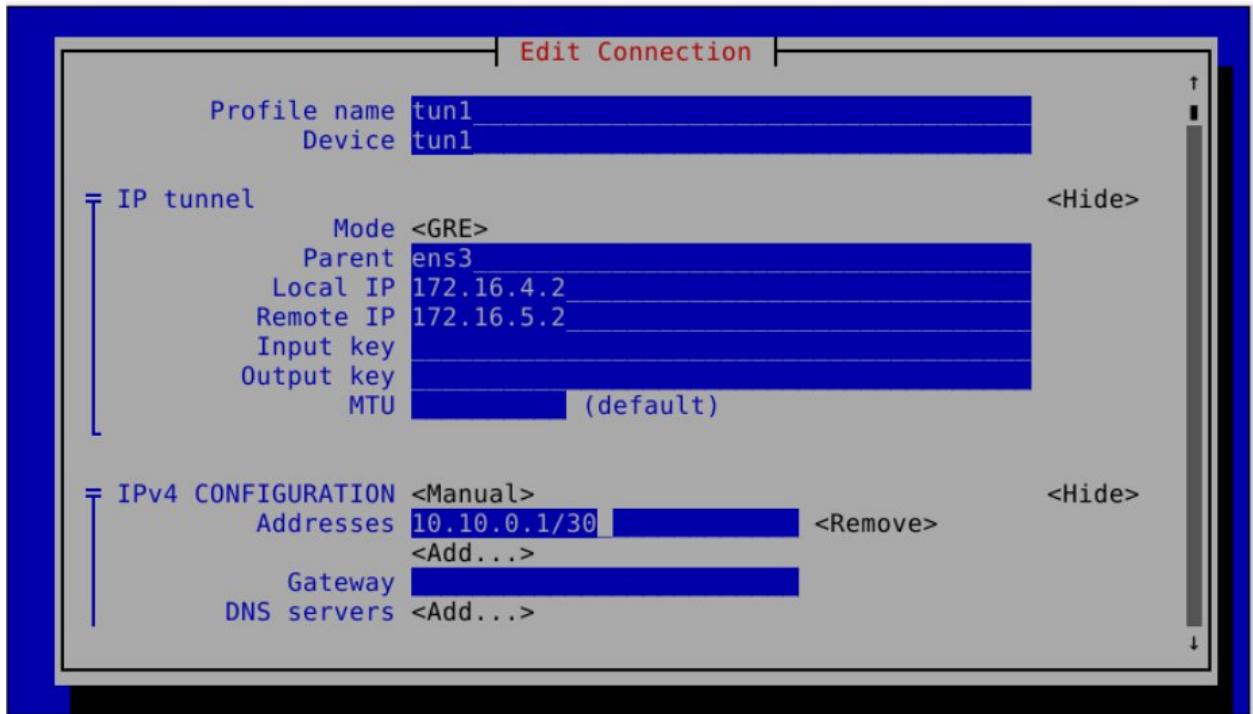
Аналогичную настройку производим на **BR**-SRV.

Задание 6. Между офисами HQ и BR необходимо сконфигурировать IP туннель

Производим настройку на HQ-RTR.

- Выбираем «Edit a connection»
- Выбираем «Add»
- Выбираем «IP tunnel»
- Задаём понятные имена «Profile name» и «Device»
- «Mode» выбираем «GRE»
- «Parent» указываем интерфейс в сторону ISP (ens3)
- Задаём «Local IP» (IP на интерфейсе HQ-RTR в сторону ISP 172.16.4.2)
- Задаём «Remote IP» (IP на интерфейсе BR-RTR в сторону ISP 172.16.5.2)
- Переходим к «IPv4 CONFIGURATION», переключаем на «Manual»
- Задаём адрес IPv4 для туннеля (10.10.0.1/30)





Для корректной работы протокола динамической маршрутизации требуется увеличить параметр TTL на интерфейсе туннеля (ОБЯЗАТЕЛЬНО ЧТОБЫ РАБОТАЛ OSPF!!!):

```
nmcli connection modify tun1 ip-tunnel.ttl 64
```

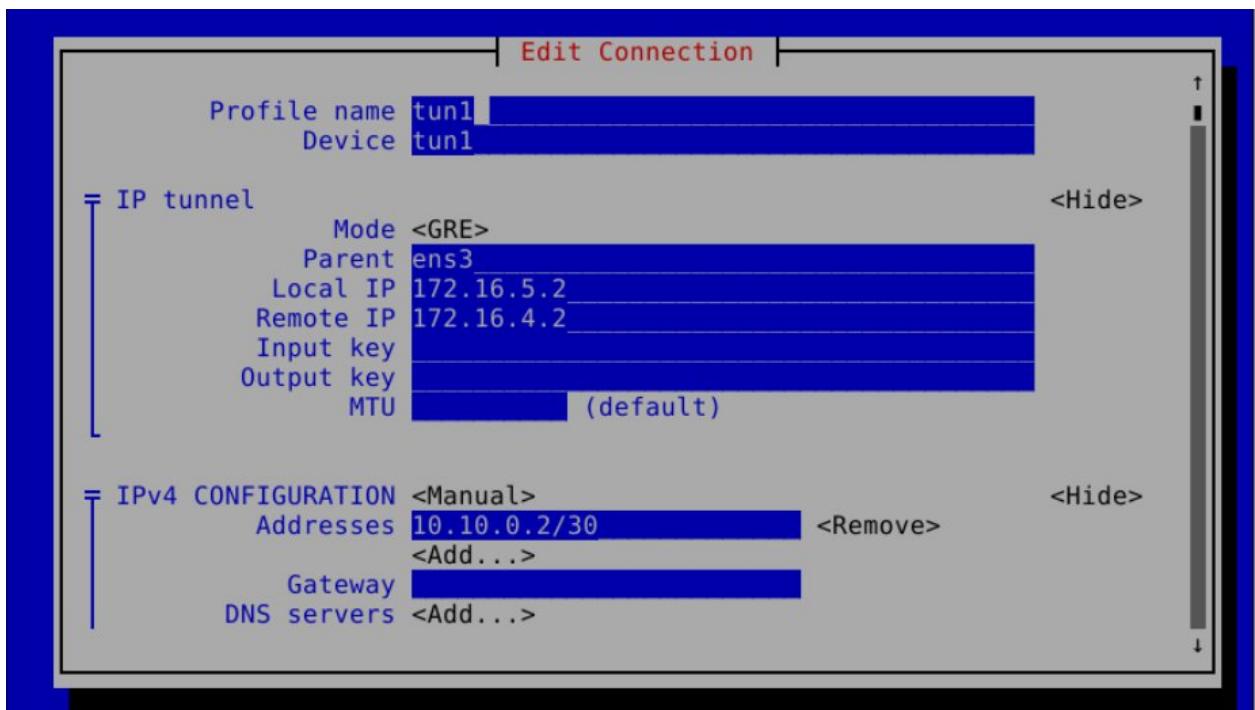
Перезагружаем интерфейс tun1.

Проверяем `ip -c -br a`.

```
root@hq-rtr:~# ip -c -br a
lo          UNKNOWN      127.0.0.1/8 ::1/128
ens3         UP          172.16.4.2/28 fe80::5260:89ff:fe00:7800/64
ens4         UP
ens5         UP
ens6         DOWN
ovs-system   DOWN
hq-sw        UNKNOWN      fe80::5260:89ff:fe00:7801/64
vlan100      UNKNOWN      192.168.100.1/26 fe80::60c0:2bff:feba:4240/64
vlan200      UNKNOWN      192.168.100.65/28 fe80::6441:f3ff:fe05:66be/64
vlan999      UNKNOWN      192.168.100.81/29 fe80::7492:58ff:fe0e:dc77/64
gre0@NONE    DOWN
gretap0@NONE DOWN
erspan0@NONE DOWN
tun1@ens3    UNKNOWN      10.10.0.1/30 fe80::c08d:a013:d70e:1b64/64
root@hq-rtr:~#
```

Настройка на BR-RTR.

- Выбираем «Edit a connection»
- Выбираем «Add»
- Выбираем «IP tunnel»
- Задаём понятные имена «Profile name» и «Device»
- «Mode» выбираем «GRE»
- «Parent» указываем интерфейс в сторону ISP (ens3)
- Задаём «Local IP» (IP на интерфейсе BR-RTR в сторону ISP 172.16.5.2)
- Задаём «Remote IP» (IP на интерфейсе HQ-RTR в сторону ISP 172.16.4.2)
- Переходим к «IPv4 CONFIGURATION», переключаем на «Manual»
- Задаём адрес IPv4 для туннеля (10.10.0.2/30)



Для корректной работы протокола динамической маршрутизации требуется увеличить параметр TTL на интерфейсе туннеля (ТОЖЕ САМОЕ ОБЯЗАТЕЛЬНО ЧТОБЫ РАБОТАЛ OSPF!!!):

```
nmcli connection modify tun1 ip-tunnel.ttl 64
```

Перезагружаем интерфейс tun1.

Проверяем ip -c -br a.

```
root@br-rtr:~# ip -c -br a
lo                  UNKNOWN      127.0.0.1/8 ::1/128
ens3                UP          172.16.5.2/28 fe80::52a7:40ff:fe00:7900/64
ens4                UP          192.168.200.1/27 fe80::8076:1001:b19a:8f24/64
gre0@NONE          DOWN
gretap0@NONE        DOWN
erspan0@NONE        DOWN
tun1@ens3           UNKNOWN     10.10.0.2/30 fe80::alad:704f:d119:2d89/64
root@br-rtr:~#
```

Был создан новый виртуальный интерфейс (туннель) для прямого взаимодействия устройств **HQ**-RTR и **BR**-RTR. Они будут напрямую обмениваться маршрутами внутренних сетей **HQ** и **BR** через это соединение.

Теперь проверим наш туннель.

Зайдем на **HQ**-RTR и пинганем туннель к **BR**-RTR: `ping 10.10.0.2`

```
root@hq-rtr:~# ping 10.10.0.2
PING 10.10.0.2 (10.10.0.2) 56(84) bytes of data.
64 bytes from 10.10.0.2: icmp_seq=1 ttl=64 time=3.14 ms
64 bytes from 10.10.0.2: icmp_seq=2 ttl=64 time=2.21 ms
64 bytes from 10.10.0.2: icmp_seq=3 ttl=64 time=2.60 ms
64 bytes from 10.10.0.2: icmp_seq=4 ttl=64 time=2.80 ms
^C
--- 10.10.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 2.206/2.688/3.140/0.339 ms
root@hq-rtr:~#
```

Пинг идет.

Теперь зайдем на **BR**-RTR и пинганем туннель к **HQ**-RTR: `ping 10.10.0.1`

```
root@br-rtr:~# ping 10.10.0.1
PING 10.10.0.1 (10.10.0.1) 56(84) bytes of data.
64 bytes from 10.10.0.1: icmp_seq=1 ttl=64 time=2.23 ms
64 bytes from 10.10.0.1: icmp_seq=2 ttl=64 time=2.24 ms
64 bytes from 10.10.0.1: icmp_seq=3 ttl=64 time=2.32 ms
64 bytes from 10.10.0.1: icmp_seq=4 ttl=64 time=5.23 ms
^C
--- 10.10.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 2.234/3.006/5.231/1.286 ms
root@br-rtr:~#
```

Все пингуется, значит соединение между **HQ**-RTR и **BR**-RTR есть.

Задание 7. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.

- Разрешите выбранный протокол только на интерфейсах в ір туннеле
- Маршрутизаторы должны делиться маршрутами только друг с другом
- Обеспечьте защиту выбранного протокола посредством парольной защиты
- Сведения о настройке и защите протокола занесите в отчёт

Настроим протокол OSPF на HQ-RTR средствами FRR.

Установим FRR на HQ-RTR: `apt install frr`

Для настройки внутренней динамической маршрутизации для IPv4 используем протокол OSPFv2

Необходимо включить соответствующий демон в конфигурации `/etc/frr/daemons`

Пропишем

```
nano /etc/frr/daemons
```

В конфигурационном файле `/etc/frr/daemons` необходимо активировать выбранный протокол для дальнейшей реализации его настройки:

```
ospfd = yes
```

Включаем и добавляем в автозагрузку службу FRR

```
systemctl enable --now frr
```

```
systemctl restart frr
```

Переходим в интерфейс управления симуляцией FRR при помощи vtysh (аналог cisco)

```
vtysh
```

Входим в режим глобальной конфигурации

```
hq-rtr.au-team.irpo# configure terminal
```

Переходим в режим конфигурации OSPFv2

```
hq-rtr.au-team.irpo(config)# router ospf
```

Указываем router-id

```
hq-rtr.au-team.irpo(config)# router-id 1.1.1.1
```

Переводим все интерфейсы в пассивный режим

```
hq-rtr.au-team.irpo(config-router)# passive-interface default
```

Объявляем локальные сети офиса HQ (сеть VLAN100 и VLAN200) и сеть (GRE-туннеля)

```
hq-rtr.au-team.irpo(config-router)# network 192.168.100.0/26  
area 0
```

```
hq-rtr.au-team.irpo(config-router)# network 192.168.100.64/28  
area 0
```

```
hq-rtr.au-team.irpo(config-router)# network 10.10.0.0/30 area 0
```

Настройка аутентификации для области

```
area 0 authentication
```

Переводим интерфейс tun1 в активный режим

```
hq-rtr.au-team.irpo(config-if)# no passive-interface  
tun1
```

Выходим из режима конфигурации OSPFv2

```
hq-rtr.au-team.irpo(config-router)# exit
```

Переходим в режим конфигурирования интерфейса tun1

```
hq-rtr.au-team.irpo(config)# interface tun1
```

Туннельный интерфейс tun1 делаем активным, для установления соседства с BR-RTR и обмена внутренними маршрутами

```
hq-rtr.au-team.irpo(config-if)# no ip ospf network broadcast
```

Настройка аутентификации с открытым паролем password

```
ip ospf authentication
```

```
ip ospf authentication-key password
```

Выходим из режима конфигурации и tun1 и режима глобальной конфигурации

```
hq-rtr.au-team.irpo(config-if)# exit
```

```
hq-rtr.au-team.irpo(config)# exit
```

Сохраняем текущую конфигурацию:

```
hq-rtr.au-team.irpo# write
```

```
hq-rtr.au-team.irpo# exit
```

```
Перезапускаем FRR: systemctl restart frr
```

Настроим протокол OSPF на BR-RTR средствами FRR.

Установим FRR на BR-RTR: apt install frr

Для настройки внутренней динамической маршрутизации для IPv4 используем протокол OSPFv2

Необходимо включить соответствующий демон в конфигурации /etc/frr/daemons

Пропишем

```
nano /etc/frr/daemons
```

В конфигурационном файле /etc/frr/daemons необходимо активировать выбранный протокол для дальнейшей реализации его настройки:

```
ospfd = yes
```

Включаем и добавляем в автозагрузку службу FRR

```
systemctl enable --now frr
```

```
systemctl restart frr
```

Переходим в интерфейс управления симуляцией FRR при помощи vtysh (аналог cisco)

```
vtysh
```

Входим в режим глобальной конфигурации

```
br-rtr.au-team.irpo# configure terminal
```

Переходим в режим конфигурации OSPFv2

```
br-rtr.au-team.irpo(config)# router ospf
```

Указываем router-id

```
br-rtr.au-team.irpo(config)# router-id 2.2.2.2
```

Переводим все интерфейсы в пассивный режим

```
br-rtr.au-team.irpo(config-router)# passive-interface default
```

Объявляем локальные сети офиса BR (сеть VLAN100 и VLAN200) и сеть (GRE-туннеля)

```
br-rtr.au-team.irpo(config-router)# network 192.168.200.0/27  
area 0
```

```
br-rtr.au-team.irpo(config-router)# network 10.10.0.0/30 area 0
```

Настройка аутентификации для области

```
area 0 authentication
```

Переводим интерфейс tun1 в активный режим

```
br-rtr.au-team.irpo(config-if)# no passive-interface  
tun1
```

Выходим из режима конфигурации OSPFv2

```
br-rtr.au-team.irpo(config-router)# exit
```

Переходим в режим конфигурирования интерфейса tun1

```
br-rtr.au-team.irpo(config)# interface tun1
```

Туннельный интерфейс tun1 делаем активным, для установления соседства с HQ-RTR и обмена внутренними маршрутами

```
br-rtr.au-team.irpo(config-if)# no ip ospf network broadcast
```

Настройка аутентификации с открытым паролем password

```
ip ospf authentication
```

```
ip ospf authentication-key password
```

Выходим из режима конфигурации и tun1 и режима глобальной конфигурации

```
br-rtr.au-team.irpo(config-if)# exit
```

```
br-rtr.au-team.irpo(config)# exit
```

Сохраняем текущую конфигурацию:

```
br-rtr.au-team.irpo# write
```

```
br-rtr.au-team.irpo# exit
```

```
Перезапускаем FRR:systemctl restart frr
```

Можем проверить настройки на обоих маршрутизаторах командами:

```
vtysh
```

```
show running-config
```

HQ-RTR:

```
Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname hq-rtr.au-team.irpo
no ipv6 forwarding
service integrated-vtysh-config
!
interface tun1
  ip ospf authentication
  ip ospf authentication-key password
!
router ospf
  ospf router-id 1.1.1.1
  network 10.10.0.0/30 area 0
  network 192.168.100.0/26 area 0
  network 192.168.100.64/28 area 0
  area 0 authentication
!
line vty
!
end
hq-rtr.au-team.irpo#
```

BR-RTR:

```
Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname br-rtr.au-team.irpo
no ipv6 forwarding
service integrated-vtysh-config
!
interface tun1
    ip ospf authentication
    ip ospf authentication-key password
!
router ospf
    ospf router-id 2.2.2.2
    passive-interface default
    no passive-interface tun1
    network 10.10.0.0/30 area 0
    network 192.168.200.0/27 area 0
    area 0 authentication
!
line vty
!
end
br-rtr.au-team.irpo#
```

Проверим, что все работает. Пинганем с **BR-SRV HQ-SRV** и после пинганем с **BR-SRV HQ-CLI**.

```
ping 192.168.100.2
```

```
root@br-srv:~# ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=62 time=5.72 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=62 time=4.06 ms
^C
--- 192.168.100.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 4.060/4.889/5.719/0.832 ms
```

```
ping 192.168.100.66
```

```
root@br-srv:~# ping 192.168.100.66
PING 192.168.100.66 (192.168.100.66) 56(84) bytes of data.
64 bytes from 192.168.100.66: icmp_seq=1 ttl=62 time=5.01 ms
64 bytes from 192.168.100.66: icmp_seq=2 ttl=62 time=4.46 ms
64 bytes from 192.168.100.66: icmp_seq=3 ttl=62 time=5.02 ms
^C
--- 192.168.100.66 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 4.456/4.831/5.024/0.265 ms
root@br-srv:~# █
```

Всё пингуется, работает.

Задание 8. Настройка динамической трансляции адресов.

- Настройте динамическую трансляцию адресов для обоих офисов.
- Все устройства в офисах должны иметь доступ к сети Интернет

Настроим динамическую сетевую трансляцию в сторону для доступа к интернету.

На **HQ**-RTR и **BR**-RTR пишем:

```
nano /etc/sysctl.conf
```

Найдем строчку

```
#net.ipv4.ip_forward=1
```

Раскомментируем её

```
net.ipv4.ip_forward=1
```

Применим командой `sysctl -p`

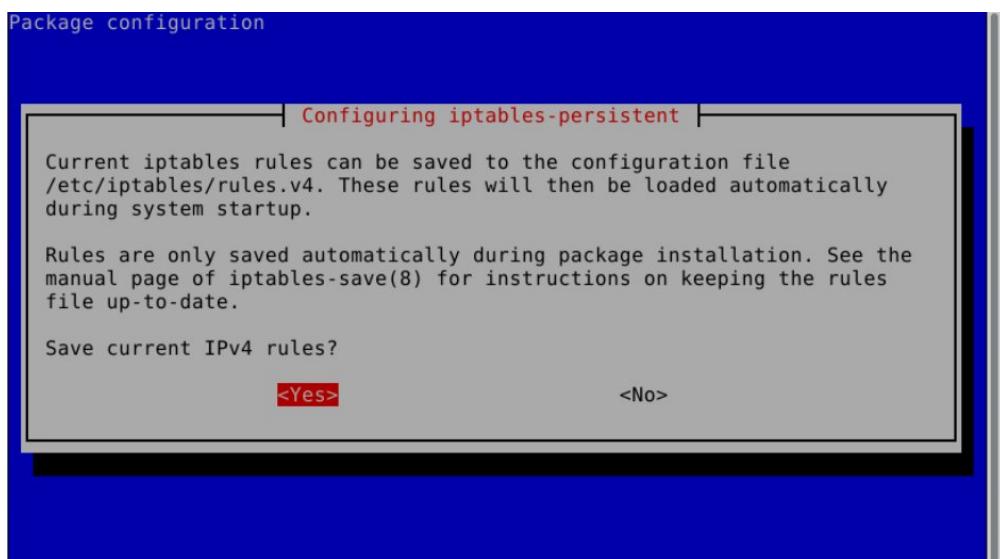
Если все ок, вывод будет: `net.ipv4.ip_forward = 1`

Задаем правила IPTABLES на **HQ**-RTR и **BR**-RTR для маскарадинга пакетов.

```
iptables -t nat -A POSTROUTING -j MASQUERADE
```

Для сохранения правил после перезапуска системы установим пакет на устройствах **HQ**-RTR и **BR**-RTR `iptables-persistent`

Для этого обновим пакеты командой `apt update` и введем команду: `apt install iptables-persistent`



Нажимаем везде “Yes”

Задание 9. Настройка протокола динамической конфигурации хостов.

- Настройте нужную подсеть
- Для офиса HQ в качестве сервера DHCP выступает маршрутизатор HQ-RTR.
- Клиентом является машина HQ-CLI.
- Исключите из выдачи адрес маршрутизатора
- Адрес шлюза по умолчанию – адрес маршрутизатора HQ-RTR.
- Адрес DNS-сервера для машины HQ-CLI – адрес сервера HQ-SRV.
- DNS-суффикс для офисов HQ – au-team.irpo
- Сведения о настройке протокола занесите в отчёт

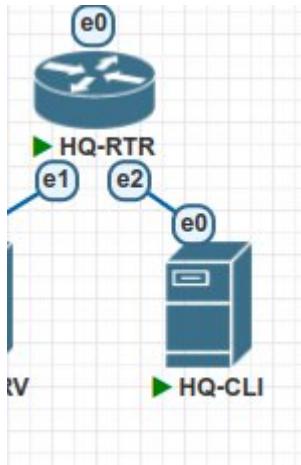
Установим DHCP сервер на HQ-RTR

```
apt install isc-dhcp-server
```

Зайдем в настройки интерфейсов DHCP

```
nano /etc/default/isc-dhcp-server
```

Поставим раздачу на интерфейс ens5 для HQ-CLI, так как по схеме у нас он подключен к e2



Находим строчку `INTERFACESv4=""`

Вписываем туда значение "`vlan200`"

```
INTERFACESv4="vlan200"
INTERFACESv6=""
```

Сохраняем: `Ctrl+X`, `y`, `Enter`.

Настроим непосредственно сам DHCP.

```
nano /etc/dhcp/dhcpd.conf
```

При открытии увидим такой файл

```
GNU nano 3.2                               /etc/dhcp/dhcpd.conf

# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text^T To Spell  ^  Go To Line
```

Меняем строчки как на скриншоте

```
option domain-name "au-team.irpo";
option domain-name-servers 192.168.100.2;
```

И добавляем в самом низу документа

```
#     range 10.0.29.10 10.0.29.230;
# }
#}

subnet 192.168.100.64 netmask 255.255.255.240 {
    range 192.168.100.66 192.168.100.78;
    option routers 192.168.100.65;
}
```

- subnet - обозначает сеть, в области которой будет работать данная группа настроек;
- range — диапазон, из которого будут браться IP-адреса;
- option domain-name-servers — через запятую перечисляем DNS-сервера.
- option domain-name — суффикс доменного имени
- option routers — шлюз по умолчанию;
- default-lease-time, max-lease-time — время и максимальное время в секундах, на которое клиент получит адрес, по его истечению будет выполнено продление срока.

То есть, по сути наш DHCP будет работать в области 192.168.100.64 с маской 255.255.255.240 (/28), выдавать диапазоны адресов от 192.168.100.66 до 192.168.100.78 от нашего шлюза VLAN200 (192.168.100.65).

Сохраняем: Ctrl+X, y, Enter.

Запускаем и добавляем в автозагрузку службу DHCP

```
systemctl enable --now isc-dhcp-server
```

Перезагружаем службу DHCP

```
systemctl restart isc-dhcp-server
```

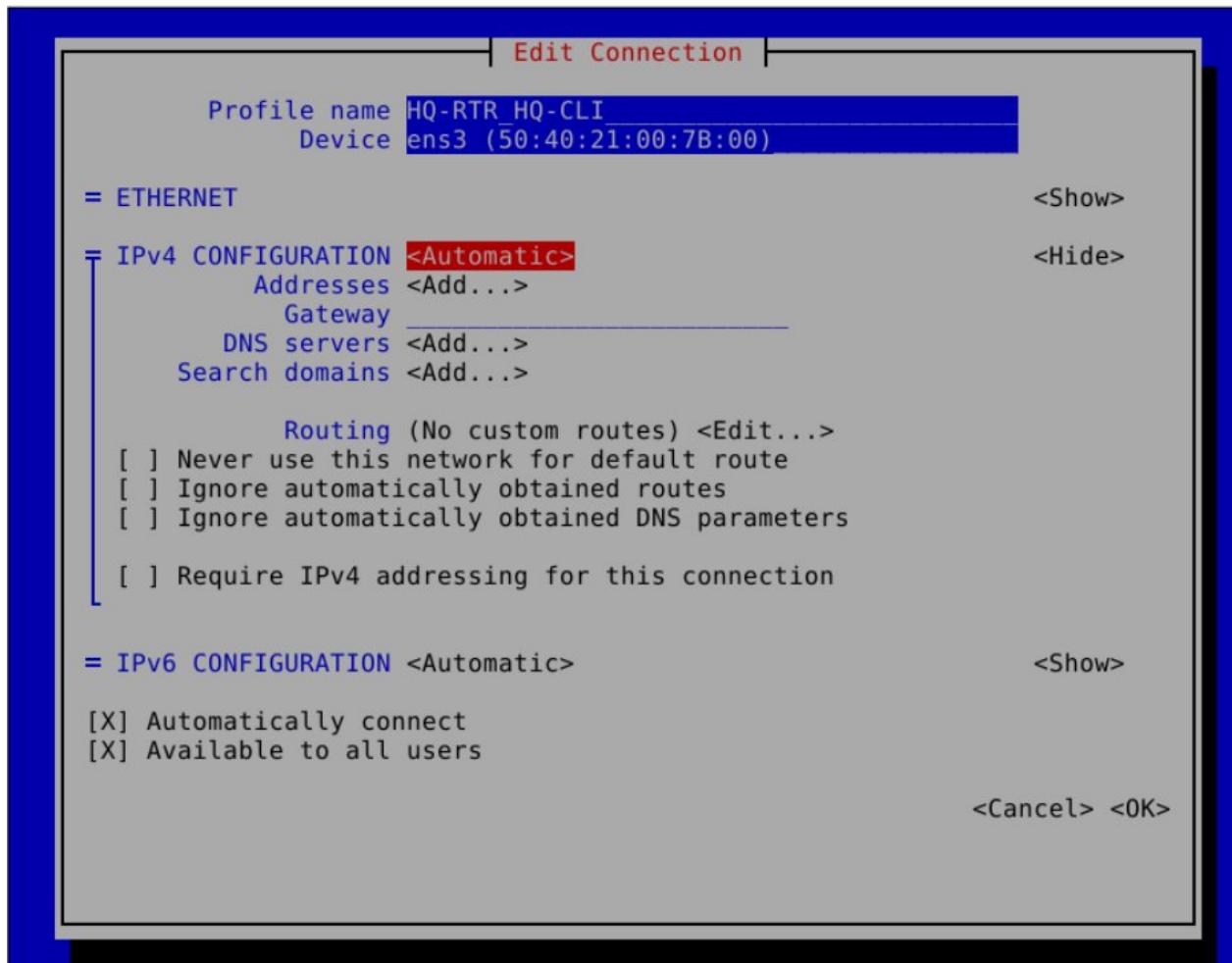
Проверяем службу DHCP.

```
systemctl status isc-dhcp-server
```

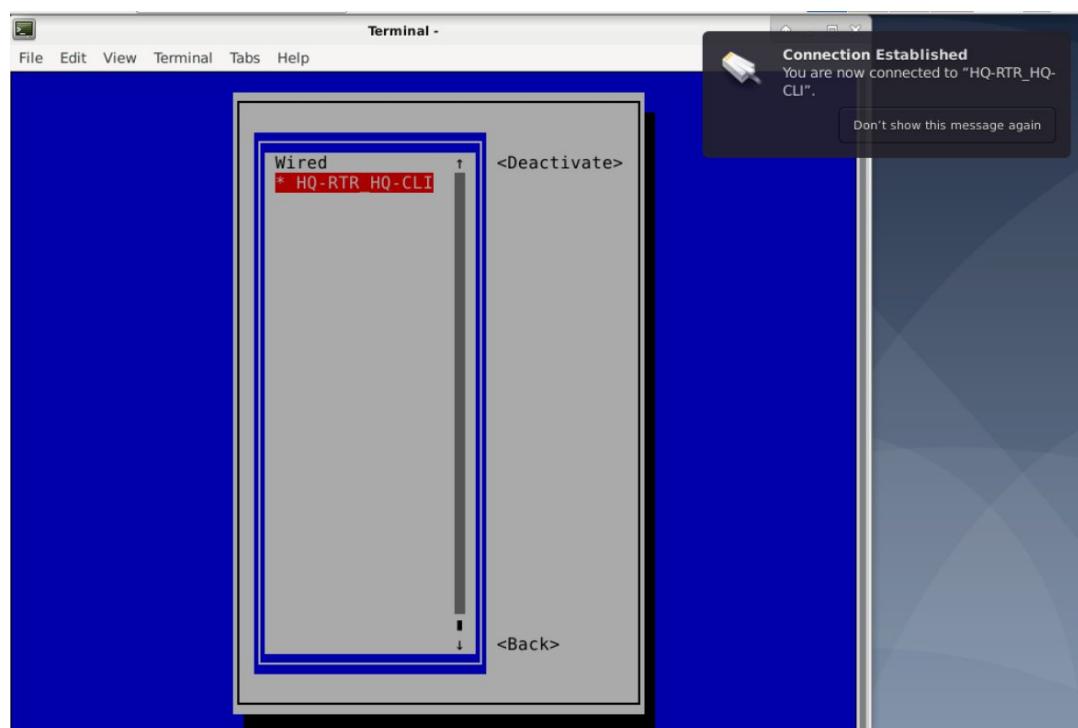
```
root@hq-rtr:~# systemctl status isc-dhcp-server
● isc-dhcp-server.service - LSB: DHCP server
  Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
  Active: active (running) since Tue 2025-03-25 21:20:09 CDT; 33s ago
    Docs: man:systemd-sysv-generator(8)
 Process: 2392 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status
  Tasks: 1 (limit: 1138)
 Memory: 4.8M
 CGroup: /system.slice/isc-dhcp-server.service
         └─2406 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf vlan200

Mar 25 21:20:07 hq-rtr.au-team.irpo systemd[1]: Starting LSB: DHCP server...
Mar 25 21:20:07 hq-rtr.au-team.irpo isc-dhcp-server[2392]: Launching IPv4 server
Mar 25 21:20:07 hq-rtr.au-team.irpo dhcpd[2406]: Wrote 0 leases to leases file.
Mar 25 21:20:07 hq-rtr.au-team.irpo dhcpd[2406]: Server starting service.
Mar 25 21:20:09 hq-rtr.au-team.irpo isc-dhcp-server[2392]: Starting ISC DHCPv4 s
Mar 25 21:20:09 hq-rtr.au-team.irpo systemd[1]: Started LSB: DHCP server.
lines 1-16/16 (END)
```

Теперь входим на HQ-CLI и переводим наш интерфейс ens3 (HQ-RTR_HQ-CLI) в автоматический режим.(IPv4 CONFIGURATION <Automatic>)



Перезапускаем интерфейс. Если все удачно осуществляется подключение.



Проверим наш IP адрес `ip -c -br a`

```
root@hq-cli:~# ip -c -br a
lo      UNKNOWN    127.0.0.1/8 ::1/128
ens3     UP        192.168.100.66/24 fe80::5240:21ff:fe00:7b00/64
root@hq-cli:~#
```

Все верно, IP адрес был успешно выдан точно так, как мы его задали на нашем DHCP сервере.

Задание 10. Настройка DNS для офисов HQ и BR.

- Основной DNS-сервер реализован на HQ-SRV.
- Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 2
- В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер

Заходим на **HQ-SRV**, скачиваем DNS-сервер.

```
apt install bind9
```

Редактируем конфигурационный файл `/etc/bind/named.conf.options`

```
nano /etc/bind/named.conf.options
```

По умолчанию он будет выглядеть так:

```
GNU nano 3.2                               /etc/bind/named.conf.options                         Modified

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //   0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

Листаем вниз и приводим файл к такому виду:

```
GNU nano 3.2          /etc/bind/named.conf.options

    // the all-0's placeholder.

    allow-query { any; };
    forwarders {
        8.8.8.8;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation no;

    listen-on-v6 port 53 { none; };
    listen-on port 53 { 127.0.0.1; 192.168.100.0/26; 192.168.100.64/28; 192$};

[ Read 26 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Полностью строка *listen-on port*

```
listen-on port 53 { 127.0.0.1; 192.168.100.0/26;
192.168.100.64/28; 192.168.200.0/27; }
```

Сохраняем: Ctrl+X, y, Enter.

Редактируем конфигурационный файл /etc/bind/named.conf.local

```
nano /etc/bind/named.conf.local
```

Добавляем наши домены:

```
GNU nano 3.2          /etc/bind/named.conf.local      Modified

// Do any local configuration here

zone "au-team.irpo" {
    type master;
    file "master/au-team.db";
};

zone "100.168.192.in-addr.arpa" {
    type master;
    file "master/au-team_rev.db";
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit     ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

Прямая зона

- **zone "au-team.irpo" { ... };** определения зоны au-team.irpo. В кавычках указывается имя зоны, которое следует разрешать на этом сервере.
- **type master ;** Указывает тип зоны. type master означает, что эта зона является мастер-зоной, то есть она содержит авторитетные записи, которые могут быть изменены и обновлены на этом сервере.
- **file "au-team.db";** Указывает путь к файлу, который содержит данные зоны au-team.irpo. Файлы зоны используются для хранения записей DNS, таких как A-записи, CNAME-записи, MX-записи и т. д.

Обратная зона

- **zone "100.168.192.in-addr.arpa" { ... };** определения обратной зоны au-team.irpo.
- **type master ;** Указывает тип зоны. type master означает, что эта зона является мастер-зоной, то есть она содержит авторитетные записи, которые могут быть изменены и обновлены на этом сервере.

- **file "au-team_rev.db";** Указывает путь к файлу обратной зоны, который содержит данные обратной зоны au-team.irpo.

Проверяем наличие ошибок в конфигах командой `named-checkconf`

Если вывод пустой, значит все ок.

Создаем папку с зонами `mkdir /etc/bind/zones`

В качестве основы для файла зоны прямого просмотра можно использовать файл зоны db.local. Скопируем его в нужное место:

```
sudo cp /etc/bind/db.local /etc/bind/zones/au-team.db
```

Открываем в редакторе: `nano /etc/bind/zones/au-team.db`

Приводим файл к такому виду:

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                      0           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
          IN      NS      au-team.irpo.
          IN      A       192.168.100.2
hq-rtr  IN      A       192.168.100.1
br-rtr  IN      A       192.168.200.1
hq-srv  IN      A       192.168.100.2
hq-cli   IN      A       192.168.100.66
br-srv   IN      A       192.168.200.2
moodle  CNAME   hq-rtr.au-team.irpo.
wiki    CNAME   hq-rtr.au-team.irpo.
```

Сохраняем: Ctrl+X, y, Enter.

Создадим зону обратного просмотра

```
cp /etc/bind/db.127 /etc/bind/zones/au-team_rev.db
```

Отредактируем файл

```
nano /etc/bind/zones/au-team_rev.db
```

Его нужно привести к такому виду:

```
GNU nano 3.2          /etc/bind/zones/au-team_rev.db          Modified

;
; BIND reverse data file for local loopback interface
;

$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                      0           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )     ; Negative Cache TTL
;
        IN      NS      au-team.irpo.
1      IN      PTR      hq-rtr.au-team.irpo.
2      IN      PTR      hq-srv.au-team.irpo.
66     IN      PTR      hq-cli.au-team.irpo.

[ Cancelled ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit     ^R Read File  ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Назначаем владельца и права.

```
chown -R root /etc/bind/zones
```

```
chown 0640
```

Также создаем папку master

```
mkdir /var/cache/bind/master
```

И копируем туда наши зоны

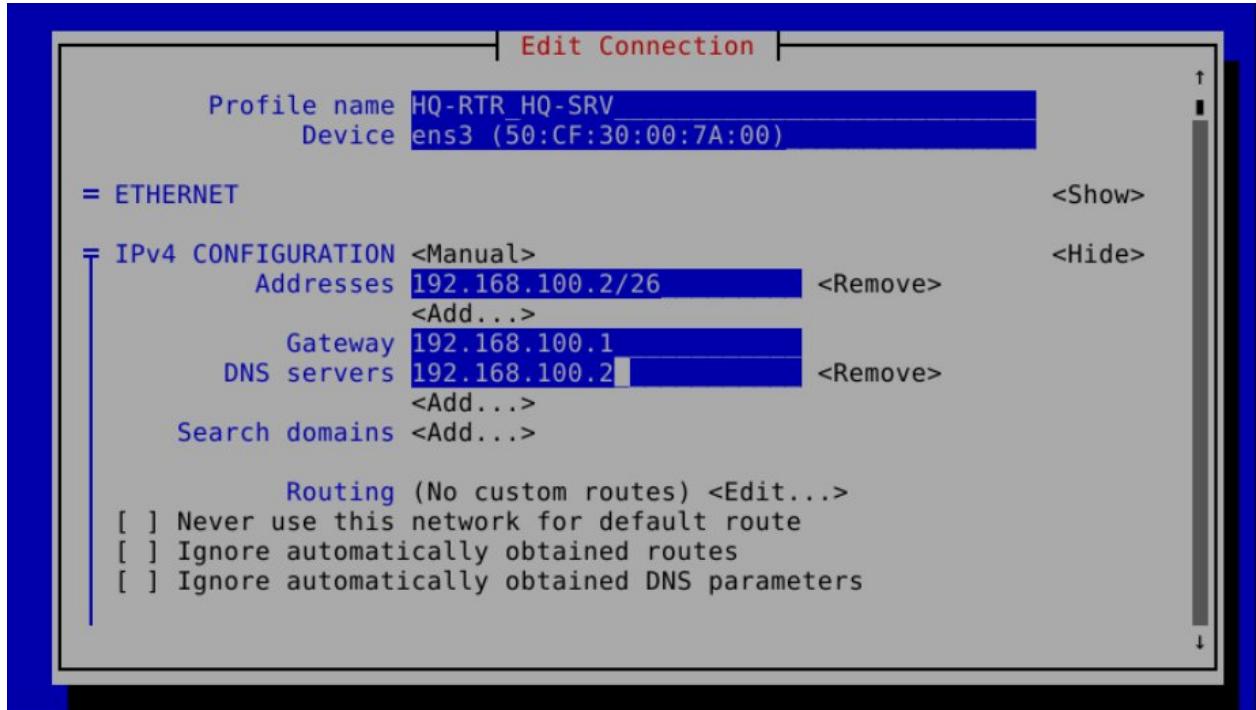
```
cp /etc/bind/zones/au-team.db /var/cache/bind/master
```

```
cp /etc/bind/zones/au-team_r
```

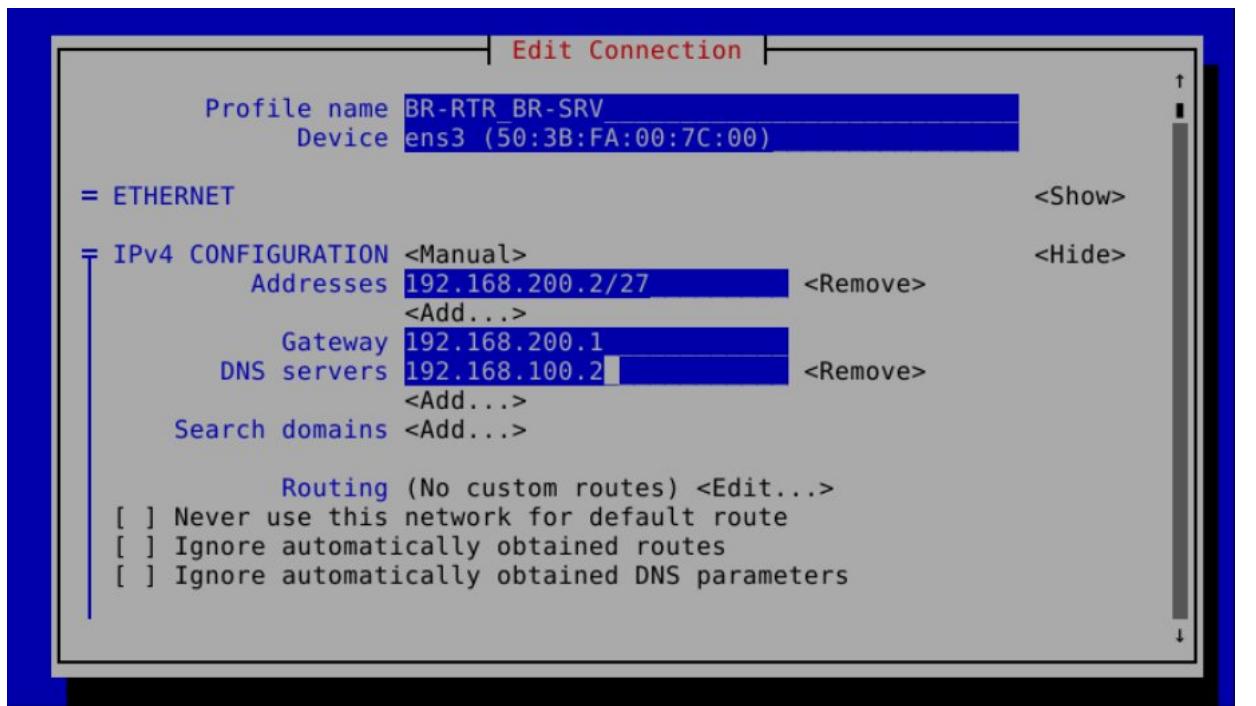
С помощью утилиты `named-checkconf -z` проверяется наличие ошибок в конфигурационном файле и файлах зон.

```
root@hq-srv:/var/cache/bind# named-checkconf -z
zone au-team.irpo/IN: loaded serial 0
zone 100.168.192-in.addr.arpa/IN: loaded serial 0
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
root@hq-srv:/var/cache/bind#
```

Теперь в DNS-сервере HQ_RTR_HQ-SRV укажем 192.168.100.2.



На BR-SRV в DNS-сервере на BR-RTR_BR-SRV также укажем 192.168.100.2.



Добавим DNS-сервер в автозагрузку

```
systemctl enable --now bind9
```

Перезагрузим службу

```
systemctl restart
```

Проверим работоспособность нашего DNS-сервера. Пинганем с BR-SRV домен au-team.irpo.

```
root@br-srv:~# ping au-team.irpo
PING au-team.irpo (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2 (192.168.100.2): icmp_seq=1 ttl=62 time=4.55 ms
64 bytes from 192.168.100.2 (192.168.100.2): icmp_seq=2 ttl=62 time=5.30 ms
64 bytes from 192.168.100.2 (192.168.100.2): icmp_seq=3 ttl=62 time=4.31 ms
^C
--- au-team.irpo ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 4.308/4.720/5.303/0.423 ms
root@br-srv:~# █
```

Все работает. Домен разрешается как 192.168.100.2.

Теперь просмотрим хосты командой `host`.

```
root@br-srv:~# host hq-rtr.au-team.irpo
hq-rtr.au-team.irpo has address 192.168.100.1
root@br-srv:~# host br-rtr.au-team.irpo
br-rtr.au-team.irpo has address 192.168.200.1
root@br-srv:~# host hq-srv.au-team.irpo
hq-srv.au-team.irpo has address 192.168.100.2
root@br-srv:~# host hq-cli.au-team.irpo
hq-cli.au-team.irpo has address 192.168.100.66
root@br-srv:~# host br-srv.au-team.irpo
br-srv.au-team.irpo has address 192.168.200.2
root@br-srv:~# host moodle.au-team.irpo
moodle.au-team.irpo is an alias for hq-rtr.au-team.irpo.
hq-rtr.au-team.irpo has address 192.168.100.1
```

```
root@br-srv:~# host wiki.au-team.irpo
wiki.au-team.irpo is an alias for hq-rtr.au-team.irpo.
hq-rtr.au-team.irpo has address 192.168.100.1
```

Также можно воспользоваться командой `lookup` или пингануть по доменному имени.

Задание 11. Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.

Проверяем часовой пояс.

```
timedatectl
```

Список доступных часовых поясов можно посмотреть командой.

```
ls /usr/share/zoneinfo/
```

Посмотреть список регионов и городов.

```
ls /usr/share/zoneinfo
```

Выберем Красноярск.

```
timedatectl set-timezone Asia/Krasnoyarsk
```

Изменение даты и времени при необходимости.

```
timedatectl set-time "2024-01-01 00:00:00"
```

Проверяем изменения.

```
timedatectl
```

```
root@isp:~# timedatectl set-timezone Asia/Krasnoyarsk
root@isp:~# timedatectl
          Local time: Mon 2025-03-31 11:39:40 +07
          Universal time: Mon 2025-03-31 04:39:40 UTC
                  RTC time: Mon 2025-03-31 04:39:41
                    Time zone: Asia/Krasnoyarsk (+07, +0700)
System clock synchronized: yes
          NTP service: active
      RTC in local TZ: no
```

Повторяем задание 11 на всех устройствах – ISP, **HQ**-RTR, **BR**-RTR, **HQ**-SRV, **HQ**-CLI, **BR**-SRV.