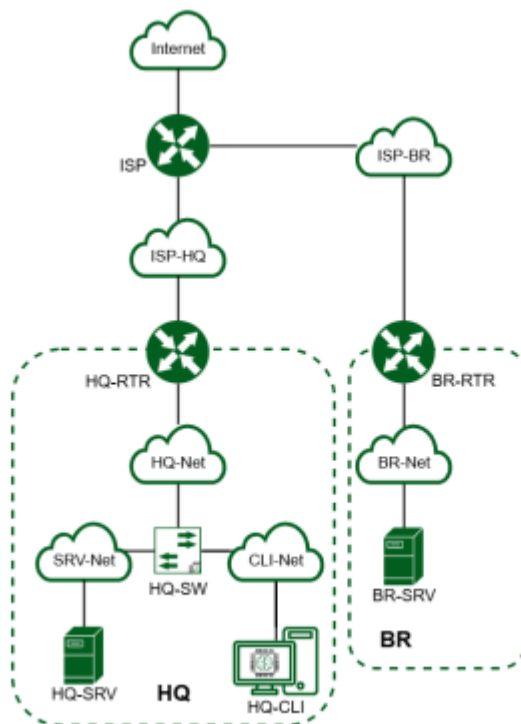


## Обновлено 09.04.2024 V1.3



### Преднастройка

Если в задании не будут использоваться встроенные репозитории, а будет возможность скачивать все пакеты из интернета, необходимо отключить проверку пакетов через `cdrom` зайдя по пути

**Nano /etc/apt/sources.list**

и закомментировать находящуюся там строку.

**Для корректной работы сети используйте NMTUI только на машине ISP. На остальных машинах настройку IP-адресации производите через файл конфигурации /etc/network/interfaces**

### Задание 1 модуля 1

1. Произведите базовую настройку устройств

- Настройте имена устройств согласно топологии. Используйте полное доменное имя

**Примечание:** для выполнения данного задания необходимо постоянное изменение имени каждого устройства, указанного на топологии (временно

изменение, действует только до перезагрузки системы и не является верным выполнением задания)

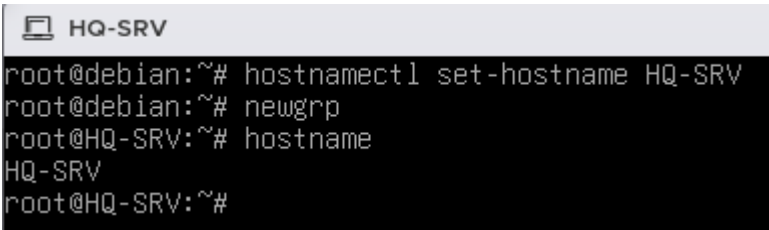
**Решение:**

Для фиксированного изменения имени компьютера, необходимо использовать команду:

**hostnamectl set-hostname Имя устройства**

Для изменения имени компьютера в текущем сеансе без перезагрузки можно воспользоваться командой:

**newgrp**



```
HQ-SRV
root@debian:~# hostnamectl set-hostname HQ-SRV
root@debian:~# newgrp
root@HQ-SRV:~# hostname
HQ-SRV
root@HQ-SRV:~#
```

Рисунок 1 — Пример изменения имени устройства

- 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

Имя устройства	IP
HQ-CLI	192.168.200.2 255.255.255.240 — к HQ-RTR
ISP	172.16.4.1 255.255.255.240 — к HQ-R 172.16.5.1 255.255.255.240 — к BR-R
HQ-RTR	192.168.100.1 255.255.255.192 — к HQ-SRV 172.16.4.2 255.255.255.240 — к ISP 192.168.200.1 255.255.255.240 — к HQ-CLI
HQ-SRV	192.168.100.2 255.255.255.192 — к HQ-RTR

BR-RTR	192.168.0.1 255.255.255.224 — к BR-SRV 172.16.5.2 255.255.255.240— к ISP
BR-SRV	192.168.0.2 255.255.255.224— к BR-RTR
Сеть управления (VLAN 999)	192.168.999.0 255.255.255.248

Вариант ручной настройки без использования любых программ (в случае если не будет возможности установки nmtui или она будет запрещена). Перед установкой интерфейсов необходимо воспользоваться командой IP A для определения имён 7 интерфейсов, находим незаполненный интерфейс, в примере ниже незаполненным интерфейсом является ens256

```
root@HQ-R:~# 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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens192: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:0c:29:24:32:0d brd ff:ff:ff:ff:ff:ff
    altname enp11s0
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:24:32:17 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 192.168.1.1/26 brd 192.168.1.63 scope global noprefixroute ens224
        valid_lft forever preferred_lft forever
    inet6 2001::1:1/122 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::f275:379c:1db3:ec04/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:24:32:21 brd ff:ff:ff:ff:ff:ff
    altname enp27s0
    inet6 fe80::d0fb:69f7:64ae:73b6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Рисунок 5— Поиск имён интерфейсов для настройки

Определив интерфейс, необходимо воспользоваться командой для просмотра и изменения конфигураций интерфейсов

**nano /etc/network/interfaces**

**или**

**vi /etc/network/interfaces**

И затем сконфигурировать настройки интерфейсов в соответствии с таблицей адресации по примеру, представленному на скриншоте ниже

```
# 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

# The primary network interface
allow-hotplug ens192
iface ens192 inet dhcp

auto ens224
iface ens224 inet static
address 172.16.4.1
netmask 255.255.255.240

auto ens256
iface ens256 inet static
address 172.16.5.1
netmask 255.255.255.240
```

Рисунок 6 — Пример настройки интерфейсов ISP

Для настройки VLAN на роутере HQ-RTR нужно скачать утилиту VLAN:

`apt install vlan`. Также нужно установить модуль 8021:

`modprobe 8021q`

и добавить его в автозапуск `echo 8021q >> /etc/modules`

Теперь можно приступить к настройке файла конфигурации `/etc/network/interface`.

Он должен выглядеть следующим образом:

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens192
iface ens192 inet static
address 172.16.4.2
netmask 255.255.255.240
gateway 172.16.4.1

auto ens224
iface ens224 inet static
address 102.168.100.1
netmask 255.255.255.192

auto ens224:1
iface ens224:1 inet static
address 102.168.200.1
netmask 255.255.255.240

auto ens224.100
iface ens224 inet static
address 102.168.100.3
netmask 255.255.255.192
vlan-raw-device ens224

auto ens224.200
iface ens224 inet static
address 102.168.200.3
netmask 255.255.255.240
vlan-raw-device ens224:1
```

Рисунок 7 — Настройка интерфейсов HQ-RTR

## 2) Настройка ISP

iptables:

```
apt-get install iptables iptables-persistent
```

Затем нужно создать правила iptables

```
iptables -t nat -A POSTROUTING -s 172.16.4.0/28 -o ens192 -j MASQUERADE
```

```
iptables -t nat -A POSTROUTING -s 172.16.5.0/28 -o ens192 -j MASQUERADE
```

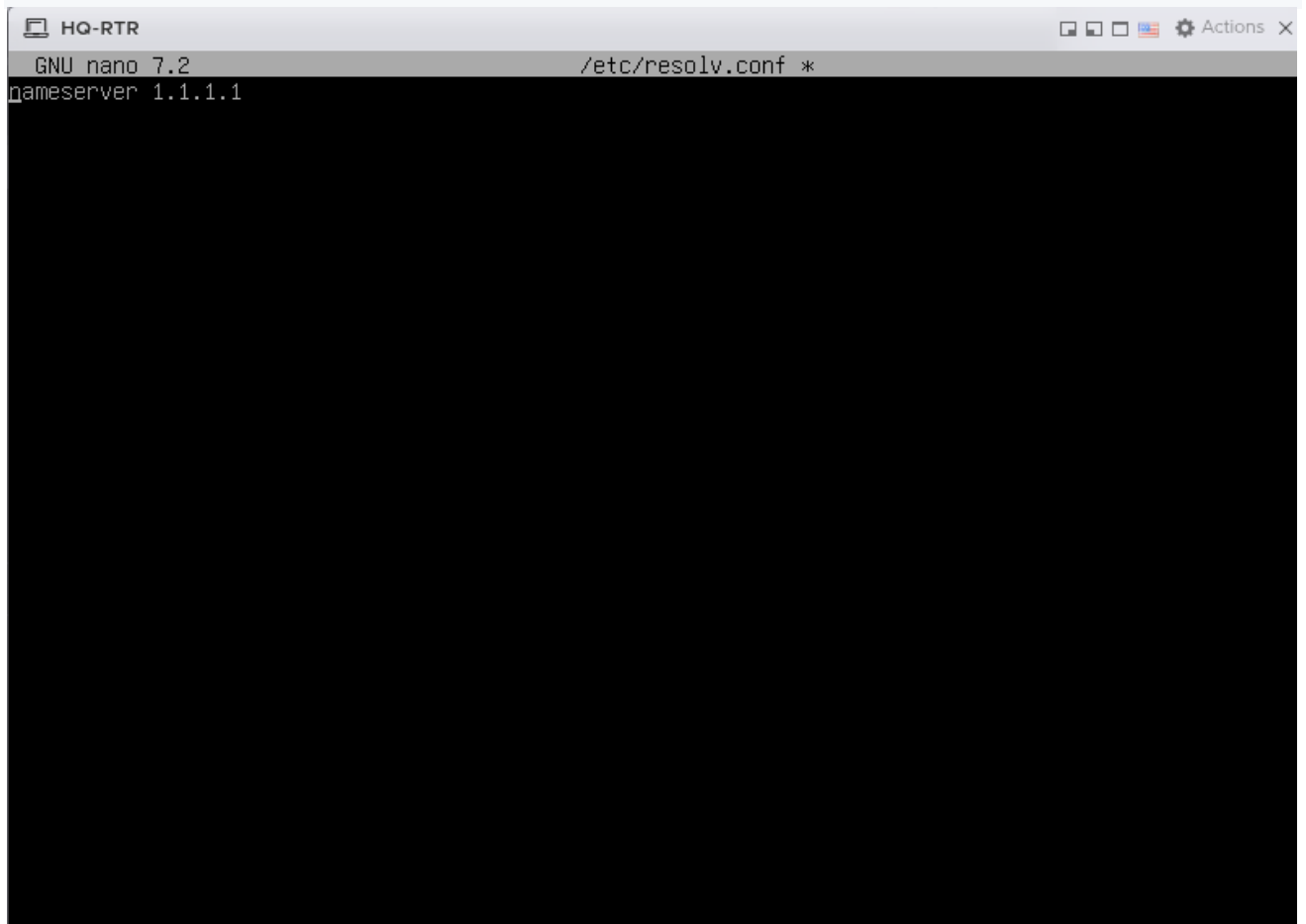
```
iptables-save > /etc/iptables/rules.v4
```

Перезапускаем iptables: `systemctl restart iptables`

Для проверки вводим команду **iptables -L -t nat**

После настройки на интерфейсах ISP может слететь Ip. Также на роутерах и ISP нужно зайти в файл `/etc/sysctl.conf` и раскомментировать строку «`net.ipv4.ip_forward=0`» и привести её к виду «`net.ipv4.ip_forward=1`». Также для работы nat и доступа в интернет на роутерах в качестве gateway указать адрес ISP.

На HQ-RTR и BR-RTR Нужно зайти в файл `/etc/resolv.conf` и оставить там только одну строку: `nameserver 1.1.1.1`



```
HQ-RTR
GNU nano 7.2 /etc/resolv.conf *
nameserver 1.1.1.1
```

Рисунок 8 — Пример настройки интерфейсов ISP

### Правила для HQ-RTR

```
iptables -t nat -A POSTROUTING -s 192.168.100.0/26 -o ens192 -j MASQUERADE
```

### 3. Создание локальных учётных записей

1. `sudo useradd -m -u 1010 -s /bin/bash sshuser`

2. `passwd sshuser`

3. `usermod -aG sudo sshuser`

4. `visudo`

`sshuser ALL=(ALL) NOPASSWD:ALL`

Так же возможно понадобится выдать Root права для данных клиентов это можно выполнить посредством команды **visudo**

в открывшемся окне необходимо вписать изменения для каждой новой

созданной учётной записи как показано на рисунке 10

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

**Рисунок 10 — выдача Root прав пользователям**

## **5. Настройка безопасного удалённого доступа**

Первым делом необходимо перейти по пути **nano /etc/ssh/sshd\_config** где в окне конфигурации нам необходимо на HQ-SRV найти строки и изменить значения как указано на рисунке 10

```
Port 2024
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
AllowUsers sshuser
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```

**Рисунок 10— смена порта доступа по ssh и права подключения только определённого пользователя**

```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 2
#MaxSessions 10
```

**Рисунок 11— Ограничение попыток авторизации**

```
# no default banner path
Banner /etc/ssh-banner
```

**Рисунок 12— Указание файла баннера**

Для настройки баннера нужно зайти в файл **/etc/ssh-banner** и написать следующее: **Authorized acces only**

```
GNU nano 7.2
Authorized acces only
```

**Рисунок 13— баннера**

Для применения конфигурации необходимо перезагрузить службу командой **systemctl restart ssh**

Для проверки доступа нужно написать команду: **ssh sshuser@192.168.100.2**

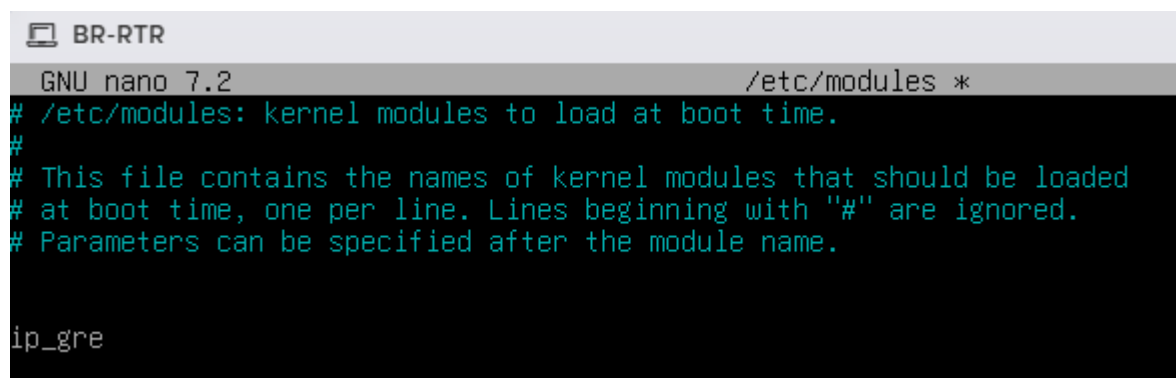
-p 2024

Где -p — указание порта. Без указания порта подключиться не получится

Также, при неправильном вводе пароля должно вывестись сообщение баннера

## 6) Реализация GRE-туннеля между офисами

Нужно зайти в файл /etc/modules и добавить там строку ip\_gre:



```
BR-RTR
GNU nano 7.2 /etc/modules *
# /etc/modules: kernel modules to load at boot time.
#
# This file contains the names of kernel modules that should be loaded
# at boot time, one per line. Lines beginning with "#" are ignored.
# Parameters can be specified after the module name.

ip_gre
```

Вся последующая настройка проводится в файле /etc/network/interfaces

```
auto tun1
iface tun1 inet tunnel
address 10.10.0.1
netmask 255.255.255.252
mode gre
local 172.16.4.2
endpoint 172.16.5.2
ttl 64
```

Рисунок 14 - Настройка GRE на HQ-RTR



```
auto tun1
iface tun1 inet tunnel
address 10.10.0.2
netmask 255.255.255.252
mode gre
local 172.16.5.2
endpoint 172.16.4.2
ttl 64_
```

**Рисунок 15 - Настройка GRE на BR-RTR**

Ping 10.10.0.1 и ping 10.10.0.2 для проверки работоспособности туннеля с обеих сторон:

```
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=0.972 ms
64 bytes from 10.10.0.1: icmp_seq=2 ttl=64 time=0.690 ms
64 bytes from 10.10.0.1: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from 10.10.0.1: icmp_seq=4 ttl=64 time=0.509 ms
^C
--- 10.10.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.509/0.817/1.098/0.231 ms
root@br-rtr:~#
```

**Рисунок 16 - Проверка работоспособности**

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

**Решение:** Первым делом необходимо установить пакеты FRR, для этого необходимо воспользоваться командой:

**apt install frr**

Следующим шагом необходимо произвести изменения конфигурационных файлов

**nano /etc/frr/daemons**

и изменить параметры на YES для протокола OSPF

```
bgpd=no
ospfd=yes
ospf6d=no
```

**Рисунок 17 — настройка конфигурации FRR**

После сохранения конфига, следующим шагом необходимо, перезапустить frr.service командой

## **systemctl restart frr**

Далее, после перезагрузки, посредством команды **vtysh** перейти в режим конфигурирования (Настройки идентичны Cisco IOS).

```
Hello, this is FRRouting (version 8.4.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

BR-R# _
```

Рисунок 18 — пример конфигурационного окна

Посредством команд:

### **Conf t**

### **router ospf**

перейти к конфигурированию протокола ospf

Настройка производится посредством объявления

ospf router-id x.x.x.x

и прилегающих к маршрутизатору сетей

network x.x.x.x/x area x

как показано на рисунке 9

```
rtr.au-team.irpo# conf t
rtr.au-team.irpo(config)# router ospf
rtr.au-team.irpo(config-router)# passive-interface default
rtr.au-team.irpo(config-router)# network 192.168.100.0/26 area 0
rtr.au-team.irpo(config-router)# network 192.168.200.0/28 area 0
rtr.au-team.irpo(config-router)# network 10.10.0.0/30 area 0
rtr.au-team.irpo(config-router)#
```

Рисунок 19 — пример настройки OSPF на HQ-RTR

```
br-rtr.au-team.irpo(config-router)# area 0 authentication
br-rtr.au-team.irpo(config-router)# c
br-rtr.au-team.irpo(config-router)# exit
br-rtr.au-team.irpo(config)# interface tun1
br-rtr.au-team.irpo(config-if)# no ip ospf passive
br-rtr.au-team.irpo(config-if)# ip ospf authentication
br-rtr.au-team.irpo(config-if)# ip ospf authentication-key password
br-rtr.au-team.irpo(config-if)#
```

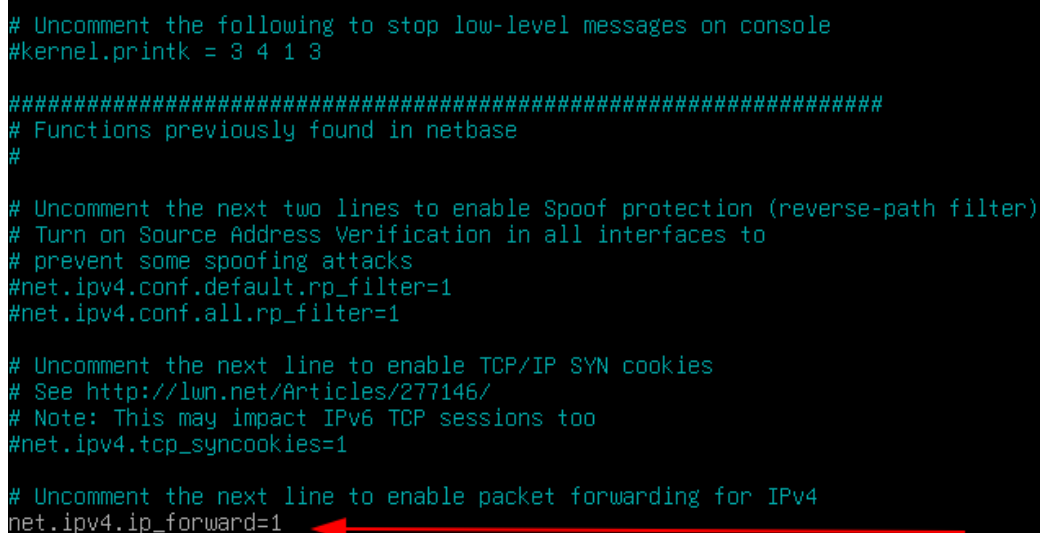
Рисунок 20— Включение авторизации и последующая настройка интерфейса

После завершения конфигурации в frr, необходимо записать конфигурацию в память устройства, командой `write`, иначе при перезагрузке frr или устройства, все настройки вернутся к дефолтным

Для этого необходимо

Для завершения настройки сети необходимо сконфигурировать настройку для передачи пакетов между сетями в файле `nano /etc/sysctl.conf`

переменную `net.ipv4.ip_forward=1` необходимо раскомментировать и сохранить изменения в файле, и применить изменения командой `sysctl -p`



```
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# 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
```

Рисунок 21 — настройка пересылки пакетов в режиме маршрутизатора

**Примечание:** при каждой перезагрузке устройства, данная настройка будет изменяться обратно, что связано с загрузкой операционной системы на виртуальной машине для того, чтобы снова включить пересылку пакетов необходимо прописать `sysctl -p`

Идентичная настройка проводится на BR-RTR, только указывается другая подсеть(192.168.0.0/27). Указание сети туннеля и настройки авторизации абсолютно идентичны

## 8) Настройка динамической трансляции адресов

Точно также как и для ISP устанавливаем пакеты iptables:

apt install iptables iptables-persistent

```
iptables -t nat -A POSTROUTING -s 192.168.100.0/26 -o ens192 -j  
MASQUERADE
```

```
iptables -t nat -A POSTROUTING -s 192.168.200.0/28 -o ens192 -j  
MASQUERADE
```

Правило для BR-RTR

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/27 -o ens192 -j  
MASQUERADE
```

Затем эти правила нужно сохранить: iptables-save > /etc/iptables/rules.v4

После этого перезапускаем службу

## 9. Настройте автоматическое распределение IP-адресов на роутере HQ-R.

а. Учтите, что у сервера должен быть зарезервирован адрес.

Первым шагом необходимо на машине HQ-R установить dhcp server командой

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

После установки пакета следующим шагом необходимо сконфигурировать файл для указания интерфейсов прослушивания DHCP сервера зайти можно с помощью команды

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

и настроить интерфейс, направленный в сторону клиента, если в сети подразумевается DHCP-relay, то 2 интерфейса в сторону клиента, и в сторону сети откуда исходит запрос. Строка v6 закомментирована, чтобы DHCP даже не думал пробовать его раздавать

```
INTERFACESv4="ens224"  
#INTERFACESv6=""
```

Рисунок 22 — Указание интерфейса для передачи адреса

Далее необходимо настроить 2 конфигурационных файла для IPv4 для IPv6

Которые можно найти по путям **nano /etc/dhcp/dhcpd.conf** и **nano /etc/dhcp/dhcpd6.conf** соответственно

```
subnet 192.168.200.0 netmask 255.255.255.240 {  
    range 192.168.200.4 192.168.200.14;  
    option domain-name-servers 192.168.100.2;  
    option domain-name "au-team.irpo";  
    option routers 192.168.200.1;  
    default-lease-time 600;  
    max-lease-time 7200;
```

Рисунок 23— Пример настройки DHCP для ipv4 без Relay

**ddns-update-style interim** — способ автообновления базы dns

**authoritative** — делает сервер доверенным

**subnet** — указание сети

**range** — пул адресов

**option routers** — шлюз по умолчанию

*Перезапускаем службу DHCP: **systemctl restart isc-dhcp-server***

Для проверки на HQ-CLI нужно указать получение адреса по DHCP

```
allow-hotplug ens192  
iface ens192 inet dhcp  
#address 192.168.200.2  
#netmask 255.255.255.240  
#gateway 192.168.200.1
```

Рисунок 24 — Настройка интерфейса

Прописываем **systemctl restart networking** для применения и проверяем выданный ip-адрес командой **ip -c a**

```

root@hq-cli:/home/locadm# ip -c 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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:13:a6:91 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.200.5/28 brd 192.168.200.15 scope global dynamic ens192
        valid_lft 597sec preferred_lft 597sec
    inet6 fe80::20c:29ff:fe13:a691/64 scope link
        valid_lft forever preferred_lft forever

```

Рисунок 25 — Проверка выдачи ip-адреса

## 10. Настройте DNS-сервер на сервере HQ-SRV:

Вся настройка будет происходить на сервере HQ-SRV

Первым делом необходимо установить пакеты для dns командой

**apt install bind9 dnsutils**

где:

**bind9** — пакеты для создания dns сервера

**dnsutils** — дополнительные пакеты, которые помогут проверить работоспособность (команда host)

Следующим шагом необходимо создать зоны для прямого и обратного просмотра dns

Для этого переходим по пути **nano /etc/bind/named.conf.default-zones** и создаём зоны как показано на скриншотах ниже

```

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

zone "100.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/au-team.irpo_obr";
};

zone "200.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/au-team.irpo_hqobr";
};

```

Рисунок 26 — зоны для hq.work(На скриншоте указаны 2 обратные зоны, т. к. у HQ-CLI и HQ-SRV IP-адреса заканчиваются на одинаковые октеты и из-за этого DNS может не работать)

где:

**zone** — создаваемая зона

**type** — выбор между первичным и вторичным dns. (Master и Slave)

**file** — расположение конфигурационного файла зоны

**allow-update** — разрешение динамических обновлений

где zone:

**hq.work** — зона прямого просмотра

**in-addr.arpa** — зона обратного просмотра ipv4

Следующим шагом необходимо создать конфигурационные файлы для наших зон. Это можно сделать, скопировав стандартные шаблоны командой **cp**

Пример:

**cp /etc/bind/db.local /etc/bind/au-team.irpo** — создание файла для прямой зоны

**cp /etc/bind/db.127 /etc/bind/ au-team.irpo\_obr** — создание обратной зоны ipv4

Первым шагом сконфигурируем зону прямого просмотра, переходим по пути

**nano /etc/bind/au-team.irpo** и конфигурируем файл как показано на

скриншоте ниже

```
GNU nano 7.2 /etc/bind/au-team.irpo
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                        2      ; 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
hq-srv    IN      A        192.168.100.2
hq-cli    IN      A        192.168.200.2
br-rtr    IN      A        192.168.0.1
br-srv    IN      A        192.168.0.2
moodle    CNAME    hq-rtr.au-team.irpo
wiki      CNAME    hq-rtr.au-team.irpo
```

Рисунок 27 — зона прямого просмотра

Где:

**NS запись** — обозначение сервера ответственного за разрешение запросов к dns

**A запись** — основная запись для зоны прямого просмотра по протоколу ipv4

**CNAME** — необязательный параметр, для указания альтернативного имени записи

Вторым шагом настроим зону обратного просмотра как указано на скриншоте ниже

Зона находится по пути

**nano /etc/bind/au-team.irpo\_obr**



```
GNU nano 7.2 /etc/bind/au-team.irpo_obr
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                        1      ; 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.
```

Рисунок 28— настройка зоны обратного просмотра hq.work для ipv4

```
HQ-SRV
GNU nano 7.2 /etc/bind/au-team.irpo_hqobr
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                        1      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       au-team.irpo.
2         IN      PTR      hq-cli.au-team.irpo.
```

Рисунок 29— настройка второй зоны обратного просмотра hq.work для ipv4

Где:

**PTR запись** — основная запись для зоны обратного просмотра

**Проверка выполняется посредством команд**

**host IP-адрес**

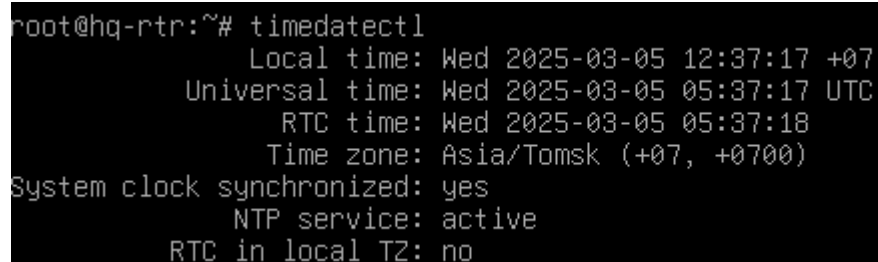
**host имя машины**

## Задание 11

**Настройка даты и времени согласно месту проведения экзамена**

**timedatectl set-timezone Asia/Tomsk**

**Команда для проверки: timedatectl**



```
root@hq-rtr:~# timedatectl
          Local time: Wed 2025-03-05 12:37:17 +07
          Universal time: Wed 2025-03-05 05:37:17 UTC
             RTC time: Wed 2025-03-05 05:37:18
            Time zone: Asia/Tomsk (+07, +0700)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

Рисунок 30 — Проверка Даты и времени