

## Модуль № 1:

### Настройка сетевой инфраструктуры

Задание:

Необходимо разработать и настроить инфраструктуру информационно-коммуникационной системы согласно предложенной топологии (см. Рисунок 1). Задание включает базовую настройку устройств:

- присвоение имен устройствам,
- расчет IP-адресации,
- настройку коммутации и маршрутизации.

В ходе проектирования и настройки сетевой инфраструктуры следует вести отчет о своих действиях, включая таблицы и схемы, предусмотренные в задании. Итоговый отчет должен содержать одну таблицу и пять отчетов о ходе работы. Итоговый отчет по окончании работы следует сохранить на диске рабочего места.

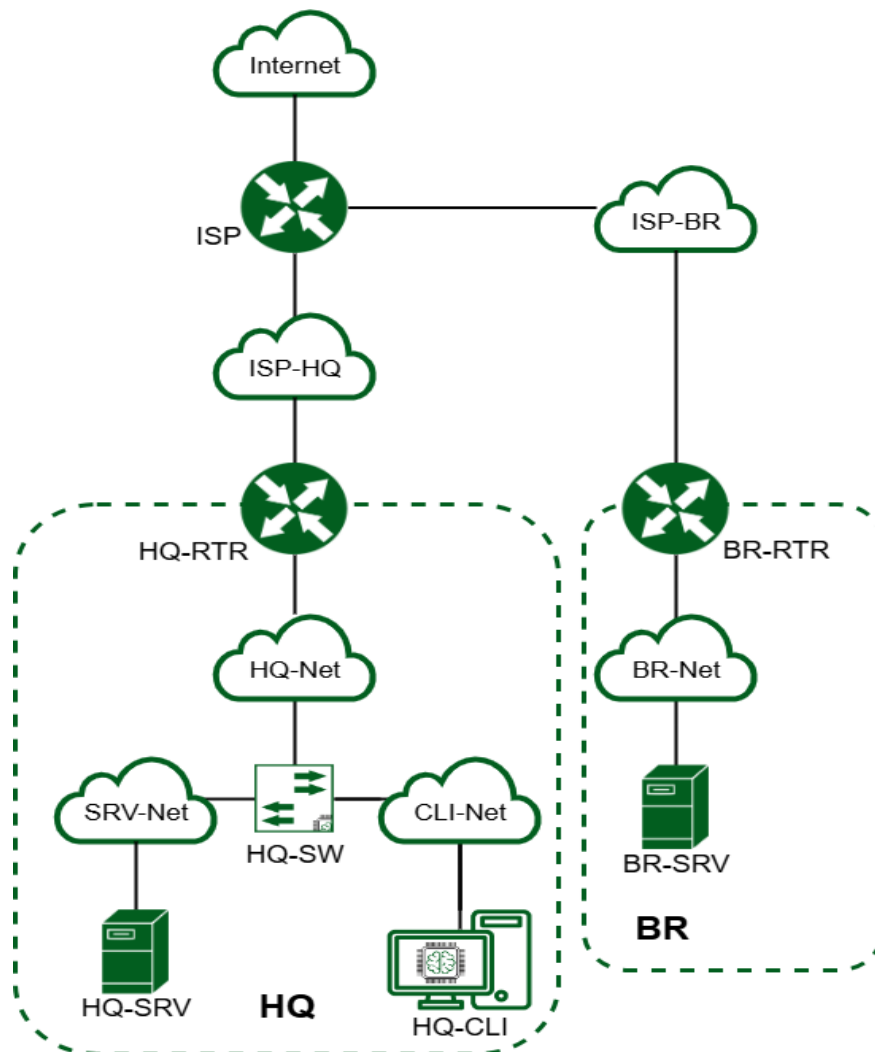


Рисунок 1. Топология сети

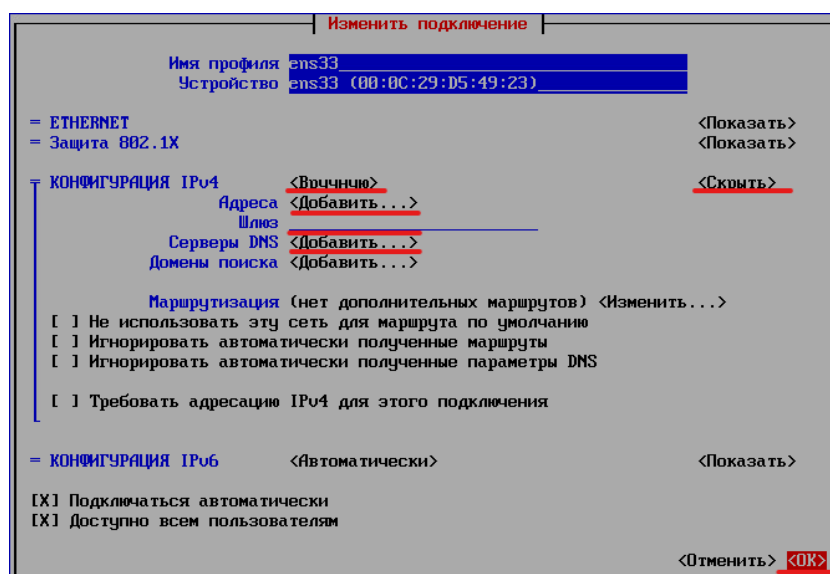
## 1. Произведите базовую настройку устройств

- Настройте имена устройств согласно топологии. Используйте полное доменное имя

`hostnamectl hostname host-name.au-team.irpo`, где **host-name** имя вашего устройства, например (hq-srv, br-rtr, isp).

- На всех устройствах необходимо сконфигурировать IPv4
  - `nmtui` > Изменить подключение > Выбираем нужный интерфейс > Стрелочка вправо > Изменить > Конфигурация IPv4: Изменить с Автоматически на вручную и нажать > Показать > Адреса > Добавить, после чего задаём IP-адрес и при необходимости шлюз и серверы DNS, после чего сохраняем изменения с помощью ОК.

На этом пункте настраиваем все интерфейсы на устройствах – ISP, BR-RTR, BR-SRV. На HQ-RTR настраиваем интерфейс в сторону ISP. Интерфейсы на устройствах HQ-RTR, HQ-SRV и HQ-CLI находящиеся в локальной сети HQ будут настраиваться в пункте №4.



Для применения изменений выходим в командную строку и прописываем команду:

`nmcli connection up INTERFACE`, где **INTERFACE** – название вашего интерфейса, настройки которого необходимо обновить (например, ens33).

На маршрутизаторах (ISP/BR-RTR/HQ-RTR) включаем параметр, отвечающий за пересылку пакетов:

```
echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
sysctl -p
```

- IP-адрес должен быть из приватного диапазона в случае, если сеть локальная, согласно RFC1918 (10.0.0.0-10.255.255.255; 172.16.0.0 – 172.32.255.255; 192.168.0.0 – 192.168.255.255)

- Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов (255.255.255.192 /26)

192.168.100.0/26

- Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 16 адресов (255.255.255.240 /28)

192.168.200.0/28

- Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов (255.255.255.224 /27)

172.30.100.0/27

- Локальная сеть для управления(VLAN999) должна вмещать не более 8 адресов (255.255.255.248 /29)

192.168.99.0/29

- Сведения об адресах занесите в отчёт, в качестве примера используйте Таблицу 3

Таблица 3. Таблица адресации

| Имя устройства | IP-адрес  | Шлюз по умолчанию   |
|----------------|---|---------------------|
| ISP            | ens33: DHCP<br>ens34: 172.16.4.1 /28<br>ens35: 172.16.5.1 /28   |                     |
| HQ-RTR         | ens33: 172.16.4.2/28<br>ens34.vlan100:<br>192.168.100.1/26<br>ens34.vlan200:<br>192.168.200.1/28<br>ens34.vlan999:<br>192.168.99.1/29 | ens33:172.16.4.1    |
| BR-RTR         | ens33: 172.16.5.2/28<br>ens34: 172.30.100.1/27  | ens:33.172.16.5.1   |
| HQ-SRV         | ens33.vlan100:<br>192.168.100.10/26   | ens33:192.168.100.1 |
| BR-SRV         | ens33: 172.30.100.10/27   | ens33:172.30.100.1  |
| HQ-CLI         | ens33.vlan200: DHCP   | DHCP                |

## 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

### НА ISP

```
dnf install iptables-services -y
systemctl enable --now iptables
iptables -F
iptables -A FORWARD -s 172.16.0.0/16 -j ACCEPT
iptables -A FORWARD -d 172.16.0.0/16 -j ACCEPT
iptables -t nat -A POSTROUTING -o ens33 -s 172.16.0.0/16 -j MASQUERADE
systemctl stop firewalld
systemctl disable firewalld
iptables-save > /etc/sysconfig/iptables
```

ПРОВЕРЯЕМ ПИНГИ НА 8.8.8.8 С HQ-RTR И BR-RTR

### 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.

```
useradd -m -U -s /bin/bash -u 1010 sshuser
```

```
passwd sshuser
```

```
P@ssw0rd
```

```
P@ssw0rd
```

```
echo "sshuser ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers
```

- Создайте пользователя net\_admin на маршрутизаторах HQ-RTR и BR-RTR

- Пароль пользователя net\_admin с паролем P@\$w0rd
- При настройке на EcoRouter пользователь net\_admin должен обладать максимальными привилегиями
- При настройке ОС на базе Linux, запускать sudo без дополнительной аутентификации

```
useradd -m -U -s /bin/bash net_admin
```

```
passwd net_admin
```

```
P@$w0rd
```

```
P@$w0rd
```

```
echo "net_admin ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers
```

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

nmtui > Изменить подключение > Добавить > VLAN и настраиваем VLAN. Данный шаг выполняем на HQ-RTR – ens34, HQ-SRV – ens33, HQ-CLI – ens33.

(Шлюз и Серверы DNS для HQ-CLI и HQ-SRV)

The screenshot shows the 'Изменить подключение' (Edit connection) window in nmtui. The 'VLAN' section is expanded, showing fields for 'Имя профиля' (Profile name) set to 'VLAN100', 'Устройство' (Device) set to 'ens34.100', 'Родительский Идентификатор VLAN' (Parent VLAN ID) set to '100', 'Клонированный MAC-адрес' (Cloned MAC address) as an empty field, and 'MTU' set to '(по умолчанию)' (default). The 'КОНФИГУРАЦИЯ IPv4' (IPv4 configuration) section is also expanded, showing 'Метод' (Method) as '<Вручную>' (Manual), 'Адреса' (Addresses) as '<Добавить...>', 'Шлюз' (Gateway) as an empty field, 'Серверы DNS' (DNS servers) as '<Добавить...>', and 'Домены поиска' (Search domains) as '<Добавить...>'. Below this, the 'Маршрутизация' (Routing) section shows 'Маршрутизация (нет дополнительных маршрутов)' (Routing (no additional routes)) with '<Изменить...>' (Change...), and four checkboxes: 'Не использовать эту сеть для маршрута по умолчанию' (Do not use this network for the default route), 'Игнорировать автоматически полученные маршруты' (Ignore automatically obtained routes), 'Игнорировать автоматически полученные параметры DNS' (Ignore automatically obtained DNS parameters), and 'Требовать адресацию IPv4 для этого подключения' (Require IPv4 addressing for this connection). The 'КОНФИГУРАЦИЯ IPv6' (IPv6 configuration) section is collapsed, showing 'Метод' (Method) as '<Автоматически>' (Automatic) and '<Показать>' (Show). At the bottom, there are two checked checkboxes: 'Подключаться автоматически' (Connect automatically) and 'Доступно всем пользователям' (Available to all users). The window has '<Отменить>' (Cancel) and '<ОК>' (OK) buttons at the bottom right.

Изменить подключение

Имя профиля VLAN100

Устройство ens34.100

VLAN <Скрыть>

Родительский Идентификатор VLAN ens34  
100

Клонированный MAC-адрес

MTU  (по умолчанию)

КОНФИГУРАЦИЯ IPv4 <Скрыть>

Метод <Вручную>

Адреса <Добавить...>

Шлюз

Серверы DNS <Добавить...>

Домены поиска <Добавить...>

Маршрутизация (нет дополнительных маршрутов) <Изменить...>

☐ Не использовать эту сеть для маршрута по умолчанию

☐ Игнорировать автоматически полученные маршруты

☐ Игнорировать автоматически полученные параметры DNS

☐ Требовать адресацию IPv4 для этого подключения

= КОНФИГУРАЦИЯ IPv6 <Автоматически> <Показать>

☒ Подключаться автоматически

☒ Доступно всем пользователям

<Отменить> <ОК>

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»

#### Создаём баннер

```
echo "Authorized access only" > /etc/ssh/banner.txt
```

#### Настраиваем SSH

```
nano /etc/ssh/sshd_config
```

```
Port 2024
```

```
AllowUsers sshuser
```

```
MaxAuthTries 2
```

```
Banner /etc/ssh/banner.txt
```

#### Разрешаем подключение по порту 2024

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

(либо выключаем SELinux и перезапускаем сервер)

#### Перезапускаем ssh

```
systemctl restart sshd
```

Далее с HQ-RTR и BR-RTR проверяем доступ до соответствующих серверов в своей локальной сети:

```
ssh -l sshuser 172.30.100.10 -p 2024
```

```
ssh -l sshuser 192.168.100.10 -p 2024
```

6. Между офисами HQ и BR необходимо сконфигурировать ip туннель

- Сведения о туннеле занесите в отчёт
- На выбор технологии GRE или IP in IP

Заходим в nmtui

Стрелочка вправо – добавить

Выбираем IP-Туннель

Конфигурируем дальше по скринам, не забыв изменить режим на GRE  
HQ-RTR:

The screenshot shows the 'Изменить подключение' (Edit connection) window in nmtui. The profile name is 'tun0' and the device is 'tun0'. The 'IP-туннель' (IP tunnel) section is expanded, showing the mode set to 'GRE'. The parent interface is 'ens33', the local IP is '172.16.4.2', and the remote IP is '172.16.5.2'. The 'Ключ на входе' (Pre-shared key) and 'Ключ на выходе' (Post-shared key) fields are empty. The MTU is set to '(по умолчанию)' (default). Below the tunnel section, the 'КОНФИГУРАЦИЯ IPv4' (IPv4 configuration) section is expanded, showing the interface name 'Врччню' and the address '10.10.10.1/30'. There are buttons for '<Удалить>' (Delete) and '<Добавить...>' (Add...). The 'Шлюз' (Gateway) field is empty. The 'Серверы DNS' (DNS servers) and 'Домены поиска' (Search domains) fields are also empty. The 'Маршрутизация' (Routing) section shows options for using the network for default routing, ignoring automatically received routes, and ignoring automatically received DNS parameters. The 'КОНФИГУРАЦИЯ IPv6' (IPv6 configuration) section is collapsed, showing 'Автоматически' (Automatic) and a button to '<Показать>' (Show). At the bottom, there are checkboxes for 'Подключаться автоматически' (Connect automatically) and 'Доступно всем пользователям' (Available to all users), both of which are checked. The window has '<Отменить>' (Cancel) and '<ОК>' (OK) buttons at the bottom right.

Изменить подключение

Имя профиля **tun0**

Устройство **tun0**

IP-туннель <Скрыть>

Режим **<GRE>**

Родительский **ens33**

Локальный IP **172.16.4.2**

Удалённый IP **172.16.5.2**

Ключ на входе

Ключ на выходе

MTU (по умолчанию)

КОНФИГУРАЦИЯ IPv4 **<Врччню>** <Скрыть>

Адреса **10.10.10.1/30** <Удалить>

<Добавить...>

Шлюз

Серверы DNS <Добавить...>

Домены поиска <Добавить...>

Маршрутизация (нет дополнительных маршрутов) <Изменить...>

☐ Не использовать эту сеть для маршрута по умолчанию

☐ Игнорировать автоматически полученные маршруты

☐ Игнорировать автоматически полученные параметры DNS

☐ Требовать адресацию IPv4 для этого подключения

= КОНФИГУРАЦИЯ IPv6 **<Автоматически>** <Показать>

☒ Подключаться автоматически

☒ Доступно всем пользователям

<Отменить> **<ОК>**



BR-RTR:

Изменить подключение

Имя профиля

tun0

Устройство

tun0

IP-туннель

<Скрыть>

Режим

<GRE>

Родительский

ens33

Локальный IP

172.16.5.2

Удалённый IP

172.16.4.2

Ключ на входе

Ключ на выходе

MTU

(по умолчанию)

КОНФИГУРАЦИЯ IPv4

<Вручную>

<Скрыть>

Адреса

10.10.10.2/30

<Удалить>

<Добавить...>

Шлюз

Серверы DNS

<Добавить...>

Домены поиска

<Добавить...>

Маршрутизация (нет дополнительных маршрутов) <Изменить...>

☐

 Не использовать эту сеть для маршрута по умолчанию

☐

 Игнорировать автоматически полученные маршруты

☐

 Игнорировать автоматически полученные параметры DNS

☐

 Требовать адресацию IPv4 для этого подключения

= КОНФИГУРАЦИЯ IPv6

<Автоматически>

<Показать>

☒

 Подключаться автоматически

☒

 Доступно всем пользователям

<Отменить>

<ОК>

ПОСЛЕ ЭТОГО НА ОБОИХ РОУТЕРАХ ПИШЕМ:

```
nmcli connection modify tun0 ip-tunnel.ttl 64
```

И перезапускаем tunnel через nmtui (выключаем и включаем интерфейс)

Проверяем пинги с двух роутеров на 10.10.10.1 и 10.10.10.2

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 ip 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

### HQ-RTR И BR-RTR

```
dnf install frr
```

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

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

```
заменить no на yes в ospfd=yes
```

```
systemctl restart frr
```

```
vtysh
```

ДАЛЕЕ РАБОТА КАК В CISCO

```
conf t
```

```
router ospf
```

| Команды для HQ-RTR              | Команды для BR-RTR             |
|---------------------------------|--------------------------------|
| network 192.168.100.0/26 area 0 | network 172.30.100.0/27 area 0 |
| network 192.168.200.0/28 area 0 | network 10.10.10.0/30 area 0   |
| network 192.168.99.0/29 area 0  |                                |
| network 10.10.10.0/30 area 0    |                                |
| ospf router-id 172.16.4.2       | ospf router-id 172.16.5.2      |
| passive-interface ens33         | passive-interface ens33        |
| passive-interface ens34         | passive-interface ens34        |
| passive-interface ens35         |                                |

```
area 0 authentication
exit
interface tun0
ip ospf authentication
ip ospf authentication-key P@ssw0rd
do wr
exit
exit
exit
```

## 8. Настройка динамической трансляции адресов.

- Настройте динамическую трансляцию адресов для обоих офисов.

- Все устройства в офисах должны иметь доступ к сети Интернет  
НА HQ-RTR И BR-RTR:

```
systemctl --now enable firewalld
firewall-cmd --set-default-zone=trusted
firewall-cmd --zone=trusted --add-masquerade --permanent
systemctl restart firewalld
```

## 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

```
dnf install dhcp-server
nano /etc/dhcp/dhcpd.conf
```

Пишем это в файле:

```
subnet 192.168.200.0 netmask 255.255.255.240 {  
range 192.168.200.2 192.168.200.14;  
option routers 192.168.200.1;  
option broadcast-address 192.168.200.15;  
option domain-name-servers 192.168.100.10;  
option domain-name "au-team.irpo";  
}
```

```
systemctl enable --now dhcpcd  
dhcpcd
```

Получаем адрес на HQ-CLI путём отключения и включения интерфейса ens33.vlan200.

ПРОВЕРЯЕМ НА HQ-RTR, ЧТО ЕСТЬ ЗАПИСЬ В ФАЙЛЕ, УКАЗЫВАЮЩАЯ НА ПОЛУЧЕНИЕ АДРЕС КЛИЕНТОМ:

```
cat /var/lib/dhcpd/dhcpd.leases
```

## 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

Таблица 2

| Устройство | Запись              | Тип   |
|------------|---------------------|-------|
| HQ-RTR     | hq-rtr.au-team.irpo | A,PTR |
| BR-RTR     | br-rtr.au-team.irpo | A     |
| HQ-SRV     | hq-srv.au-team.irpo | A,PTR |
| HQ-CLI     | hq-cli.au-team.irpo | A,PTR |
| BR-SRV     | br-srv.au-team.irpo | A     |
| HQ-RTR     | moodle.au-team.irpo | CNAME |
| HQ-RTR     | wiki.au-team.irpo   | CNAME |

dnf install bind

nano /etc/named.conf

Изменить строчки, на которые указывают стрелочки:

```
options {  
    listen-on port 53 { any; };  
    listen-on-v6 port 53 { ::1; };  
    directory "/var/named";  
    dump-file "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    memstatistics-file "/var/named/data/named_mem_stats.txt";  
    secroots-file "/var/named/data/named.secroots";  
    recursing-file "/var/named/data/named.recursing";  
    allow-query { any; };  
    forwarders { 8.8.8.8; };  
}
```

(Вместо 8.8.8.8 ставим 10.39.0.1)

И в конец добавить:

```
zone "au-team.irpo" IN {  
    type master;  
    file "/opt/dns/au-team.irpo";  
};  
  
zone "100.168.192.in-addr.arpa" IN {  
    type master;  
    file "/opt/dns/100.168.192.in-addr.arpa";  
};  
  
zone "200.168.192.in-addr.arpa" IN {  
    type master;  
    file "/opt/dns/200.168.192.in-addr.arpa";  
};  
  
include "/etc/named.rfc1912.zones";  
include "/etc/named.root.key";
```

Далее копируем файл шаблона и заполняем по скринам.

mkdir /opt/dns

cd /opt/dns

cp /var/named/named.empty au-team.irpo

nano au-team.irpo

```

GNU nano 7.2 /opt/dns/au-team.irpo
$TTL 3H
au-team.irpo. IN SOA au-team.irpo. au-team.irpo. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

    NS      hq-srv.au-team.irpo.
hq-rtr A    192.168.100.1
hq-rtr A    192.168.200.1
br-rtr A    172.30.100.1
hq-srv A    192.168.100.10
hq-cli A    192.168.200.2
br-srv A    172.30.100.10
wiki CNAME  hq-rtr.au-team.irpo.
moodle CNAME hq-rtr.au-team.irpo.

```

cp /var/named/named.empty 100.168.192.in-addr.arpa

nano 100.168.192.in-addr.arpa

```

GNU nano 7.2 /opt/dns/100.168.192.in-addr.arpa
$TTL 3H
@ IN SOA au-team.irpo. au-team.irpo. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

    NS      hq-srv.au-team.irpo.
1 PTR      hq-rtr
10 PTR     hq-srv

```

cp /var/named/named.empty 200.168.192.in-addr.arpa

nano 200.168.192.in-addr.arpa

```

GNU nano 7.2 /opt/dns/200.168.192.in-addr.arpa
$TTL 3H
@ IN SOA au-team.irpo. au-team.irpo. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

    NS      hq-srv.au-team.irpo.
1 PTR      hq-rtr
2 PTR      hq-cli

```

chmod -R 777 /opt/dns

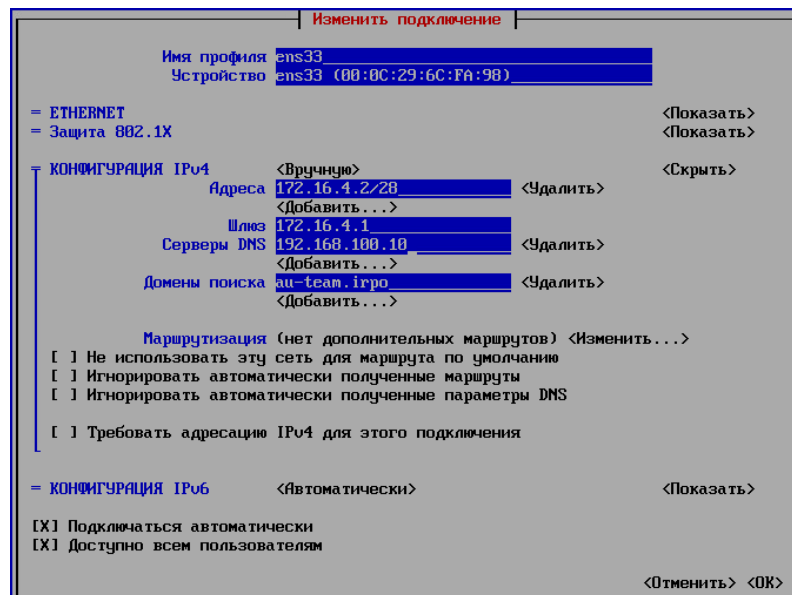
ПРОВЕРЯЕМ КОНФИГУРАЦИЮ И ИСПРАВЛЯЕМ ОШИБКИ ЕСЛИ ЕСТЬ

named-checkconf -z

systemctl restart named

Далее заходим в nmtui и меняем ДНС сервер с 8.8.8.8 (10.39.0.1) на 192.168.100.10. Так же указываем домен поиска au-team.irpo.

После этого в nmtui переходим на вкладку «Активировать подключение». Выключаем и включаем интерфейс, на который ставили ДНС.



Проверяем

НА HQ-CLI И ПРОВЕРЯЕМ РАБОТОСПОБНОСТЬ

ping br-rtr

ping br-srv

ping hq-rtr

ping hq-srv

ping ya.ru

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

timedatectl set-timezone Europe/Moscow

timedatectl (ПРОВЕРИТЬ ЗОНУ, ПО ЗАДАНИЮ ВРЕМЯ МЕНЯТЬ НЕ ПРОСЯТ)