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.

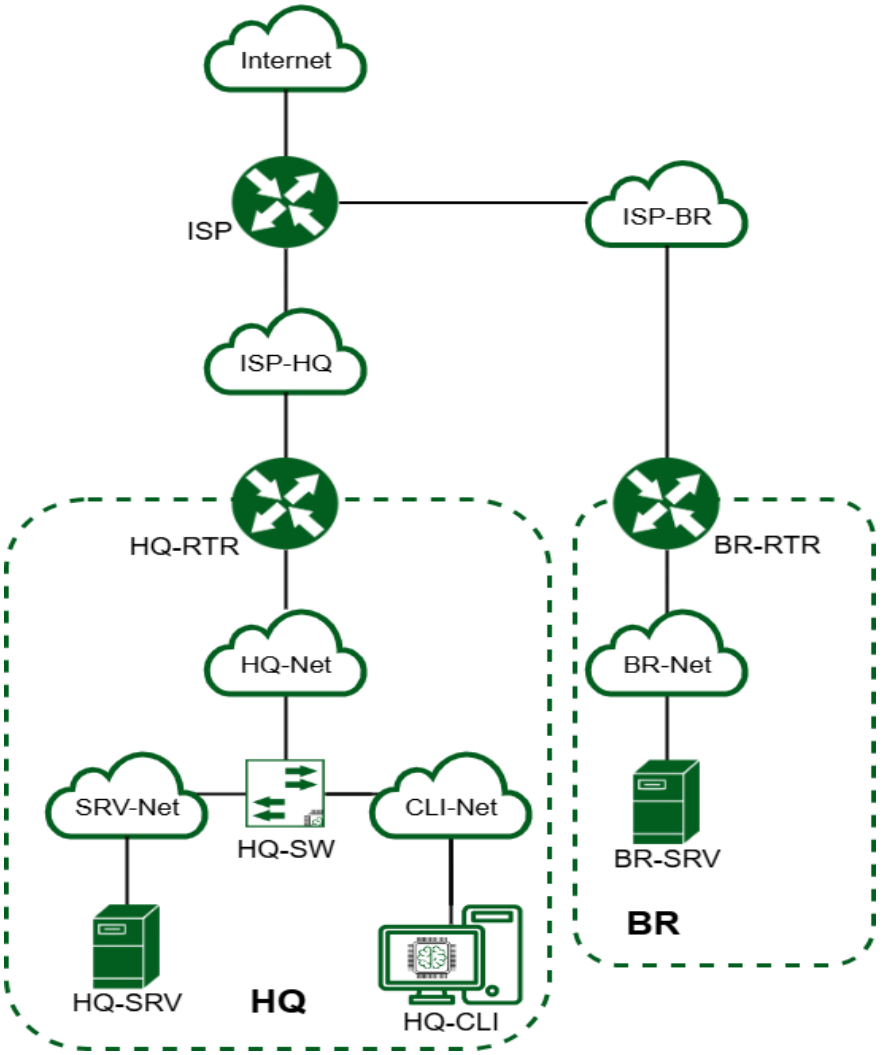


Рисунок 1. Топология сети

1. Произведите базовую настройку устройств

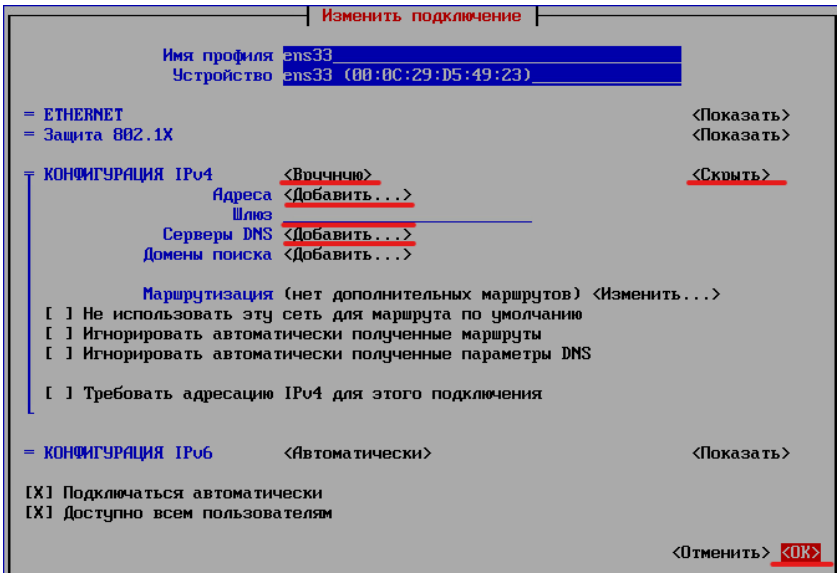
- Настройте имена устройств согласно топологии. Используйте полное доменное имя

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 ens34: 172.16.4.1 /28 ens35: 172.16.5.1 /28	
HQ-RTR	ens33: 172.16.4.2/28 ens.34.vlan100: 192.168.100.1/26 ens34.vlan200: 192.168.200.1/28 ens34.vlan999: 192.168.99.1/29	172.16.4.1
BR-RTR	ens33: 172.16.5.2/28 ens34: 172.30.100.1/27	172.16.5.1
HQ-SRV	ens33.vlan100: 192.168.100.10/26	192.168.100.1
BR-SRV	ens33: 172.30.100.10/27	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@$$word
  - 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

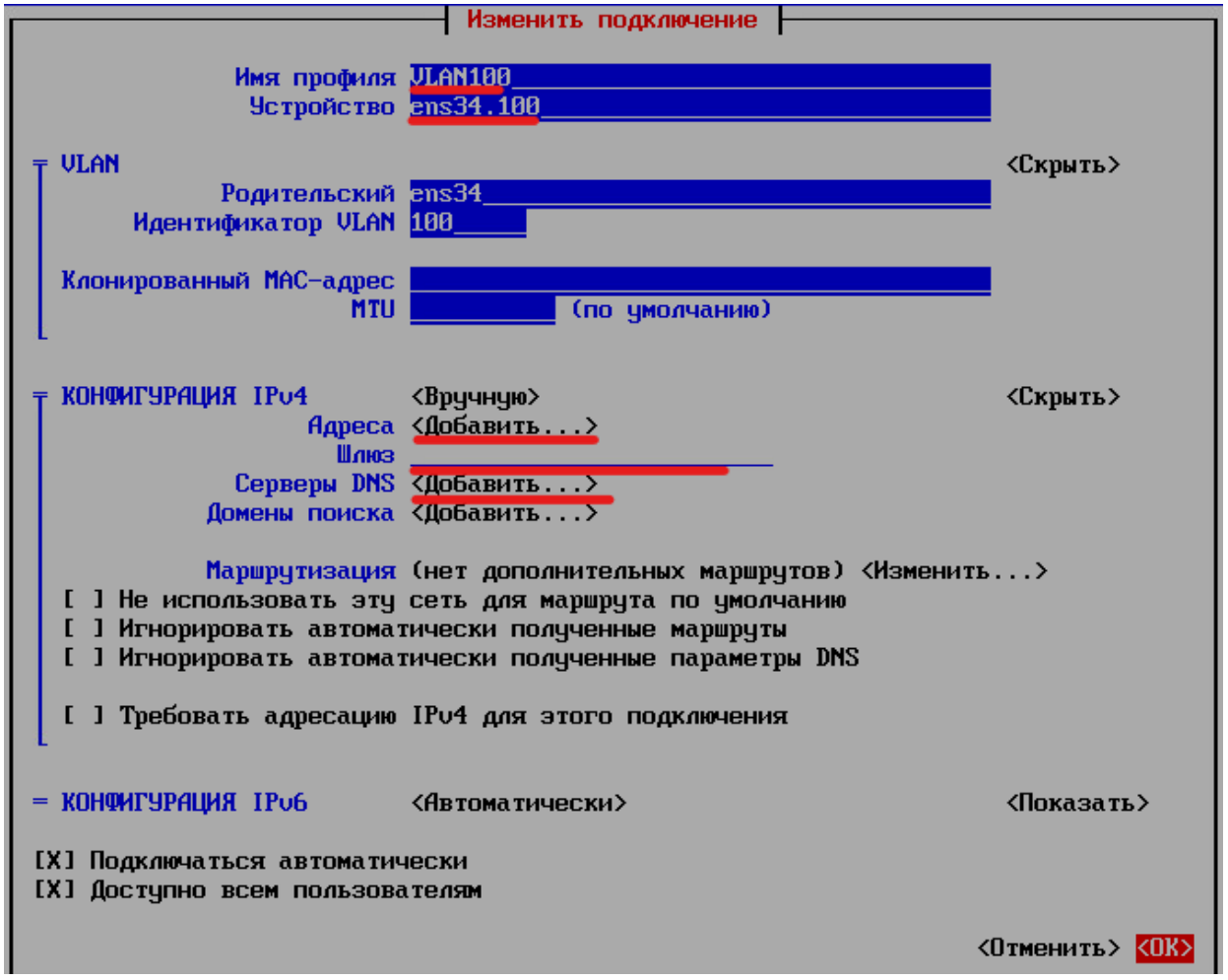
P@$$w0rd

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.



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

Перезапускаем ssh

systemctl restart sshd

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

ssh -l sshuser 172.30.100.1 -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

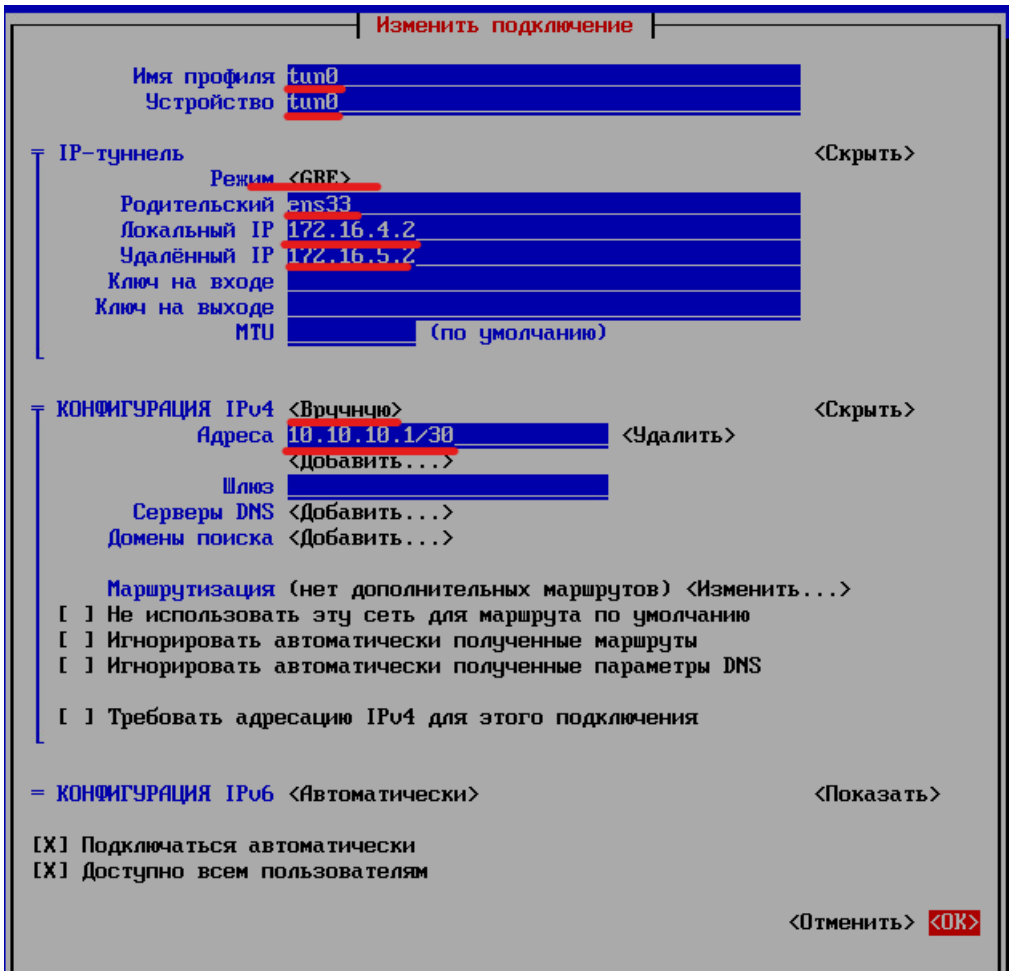
Заходим в nmtui

Стрелочка вправо – добавить

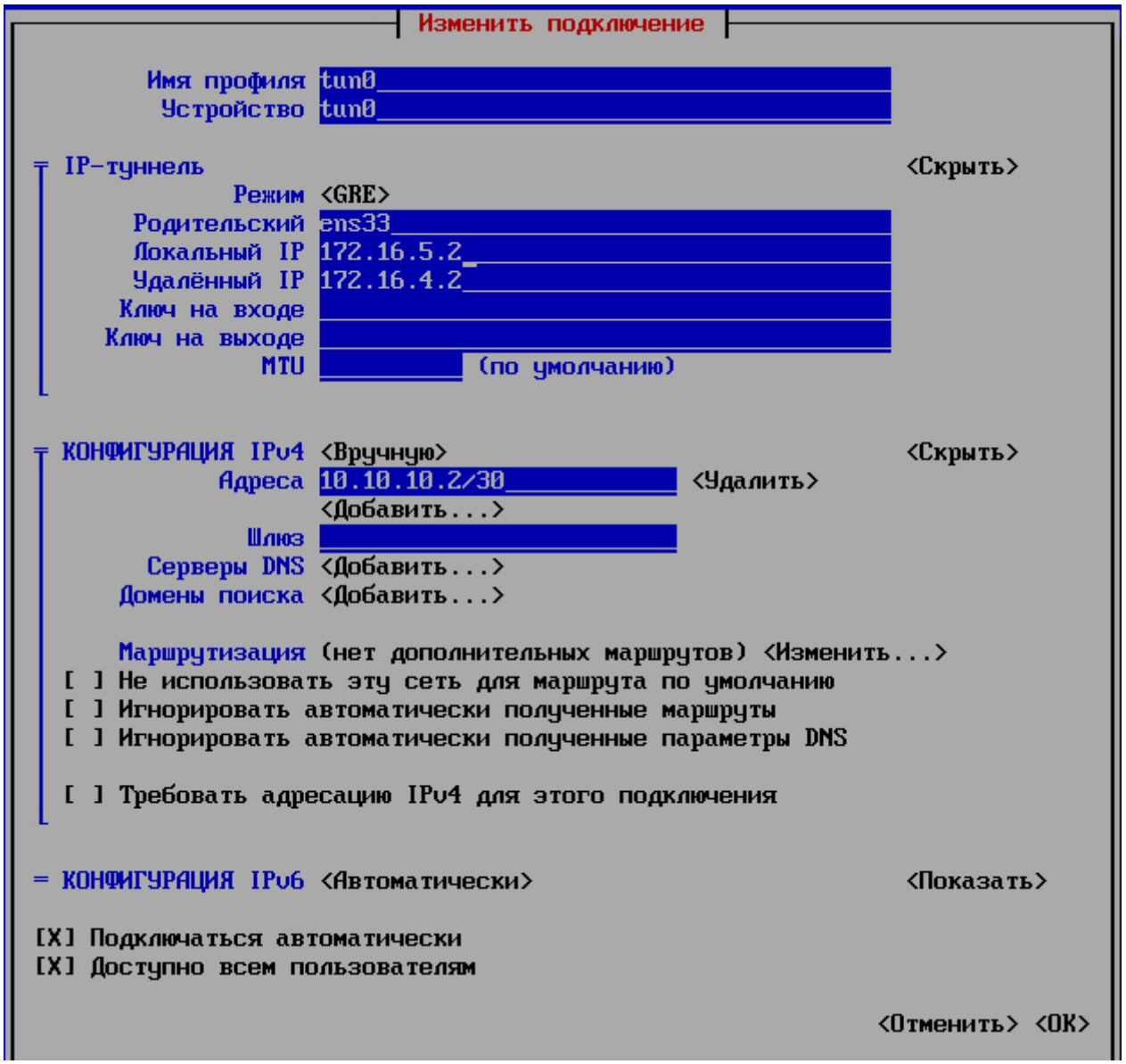
Выбираем IP-Туннель

Конфигурируем дальше по скринам, не забыв изменить режим на GRE

HQ-RTR:



BR-RTR:



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 172.30.100.10/27 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

192.168.200.0/28 – нужная подсеть

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 192.168.100.1;
        option domain-name “au-team.irpo”;
}
```

```
systemctl enable --now dhcpd
dhcpd
```

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

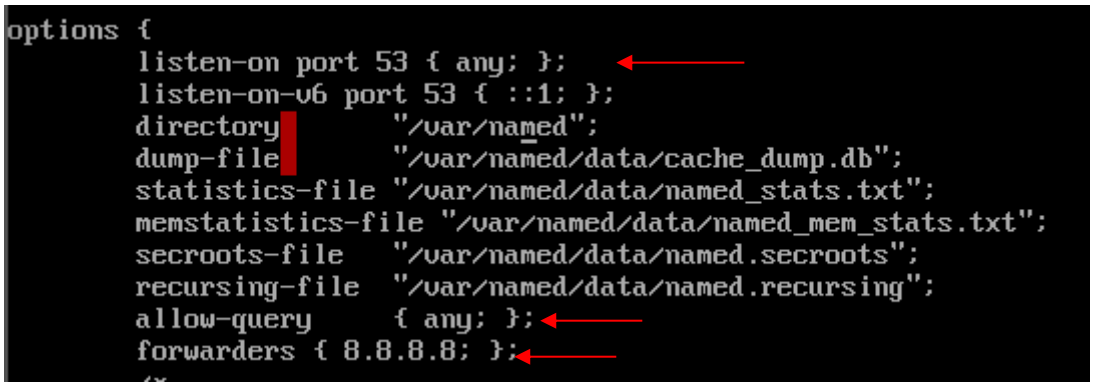
Таблица 2

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

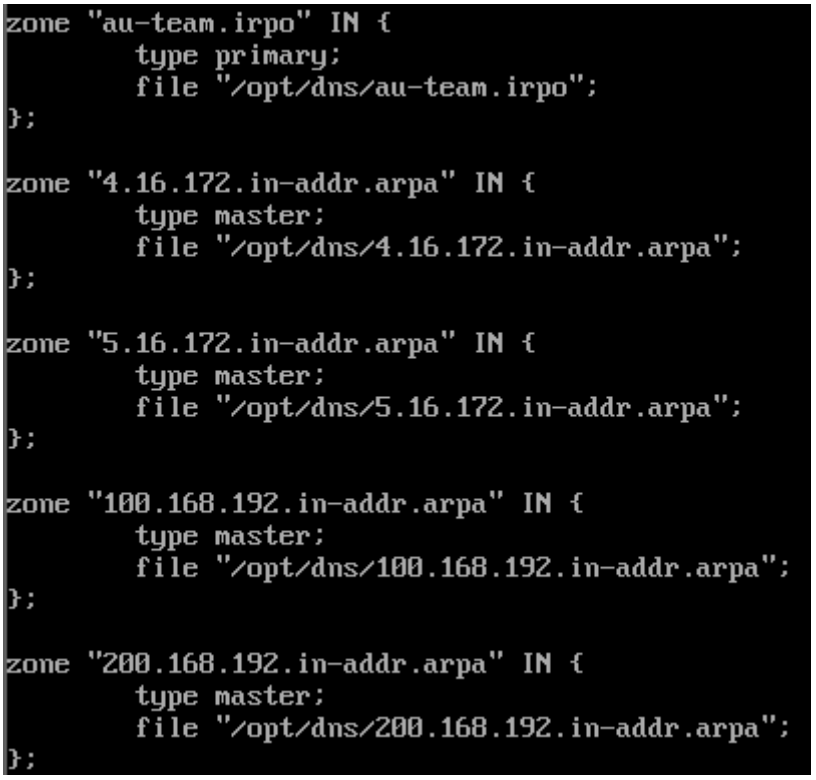
dnf install bind

nano /etc/named.conf

Изменить строчки, на которые указывают стрелочки:



И в конец добавить:



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

```
$TTL 3H         ;
au-team.irpo.   IN      SOA     au-team.irpo. au-team.irpo. (
                                        1       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum


        NS      @
        A       127.0.0.1
        AAAA    ::1

hq-rtr  IN      A       172.16.4.1
br-rtr  IN      A       172.16.5.1
hq-srv  IN      A       192.168.100.1
hq-cli  IN      A       192.168.200.2
br-srv  IN      A       172.30.100.1
wiki    CNAME           172.16.4.1
moodle  CNAME           172.16.4.1
```

cp /var/named/named.empty /opt/dns/4.16.172.in-addr.arpa

nano 4.16.172.in-addr.arpa

```
 GNU nano 7.2
$TTL    3600 ;
@  IN      SOA     au-team.irpo. au-team.irpo. (
                    1               ; Serial
                    3600            ; Refresh
                    900             ; Retry
                    3600000         ; Expire
                    3600 )          ; Minimum

        NS      au-team.irpo.
1       IN      PTR     hq-rtr.au-team.irpo.
```

cp /opt/dns/4.16.172.in-addr.arpa /opt/dns/5.16.172.in-addr.arpa

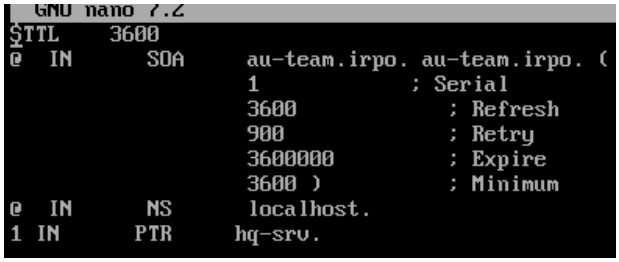
nano 5.16.172.in-addr.arpa

```
 GNU nano 7.2
$TTL    3600 ;
@  IN      SOA     au-team.irpo. au-team.irpo. (
                    1               ; Serial
                    3600            ; Refresh
                    900             ; Retry
                    3600000         ; Expire
                    3600 )          ; Minimum

        NS      au-team.irpo.
1       IN      PTR     br-rtr.au-team.irpo.
```

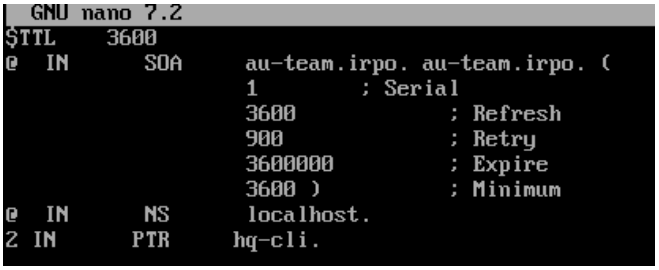
cp /var/named/named.empty 100.168.192.in-addr.arpa

nano 100.168.192.in-addr.arpa



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

nano 200.168.192.in-addr.arpa



chmod -R 777 /opt/dns

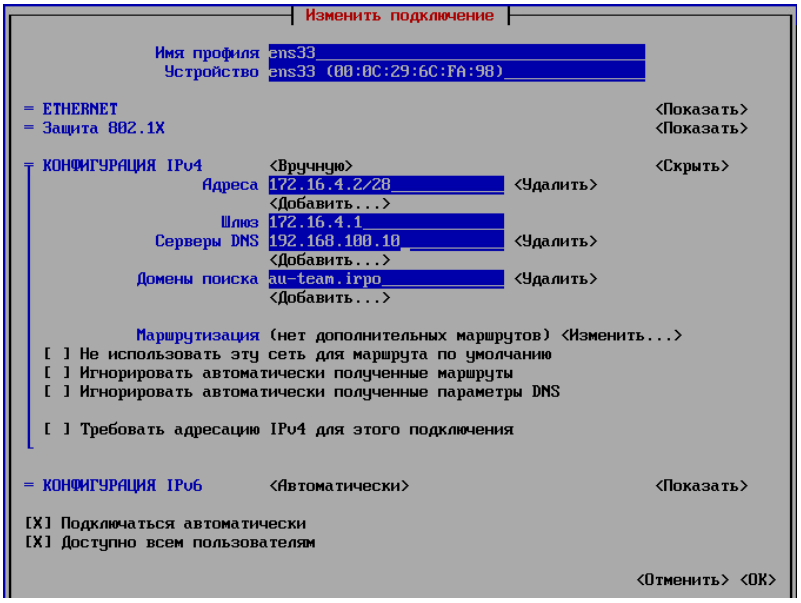
ПРОВЕРЯЕМ КОНФИГУРАЦИЮ И ИСПРАВЛЯЕМ ОШИБКИ ЕСЛИ ЕСТЬ

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)