

Оглавление

<u>Модуль 1. Настройка сетевой инфраструктуры.....</u>	<u>2</u>
<u>Задание 1. Произведите базовую настройку устройств.....</u>	<u>3</u>
<u>Выполнение.....</u>	<u>3</u>
<u>Задание 2. Настройка ISP.....</u>	<u>6</u>
<u>Выполнение.....</u>	<u>6</u>
<u>Задание 3. Создание локальных учетных записей.....</u>	<u>7</u>
<u>Выполнение.....</u>	<u>7</u>
<u>Задание 4. Настройте на интерфейсе HQ-RTR в сторону офиса HQ виртуальный коммутатор.....</u>	<u>8</u>
<u>Выполнение.....</u>	<u>8</u>
<u>Задание 5. Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV.....</u>	<u>9</u>
<u>Выполнение.....</u>	<u>9</u>
<u>Задание 6. Между офисами HQ и BR необходимо сконфигурировать IP туннель.....</u>	<u>10</u>
<u>Выполнение.....</u>	<u>10</u>
<u>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.....</u>	<u>11</u>
<u>Выполнение.....</u>	<u>11</u>
<u>Задание 8. Настройка динамической трансляции адресов.....</u>	<u>14</u>
<u>Выполнение.....</u>	<u>14</u>
<u>Задание 9. Настройка протокола динамической конфигурации хостов.....</u>	<u>15</u>
<u>Выполнение.....</u>	<u>15</u>
<u>Задание 10 Настройка DNS для офисов HQ и BR.....</u>	<u>16</u>
<u>Выполнение.....</u>	<u>16</u>
<u>Задание 11 Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.....</u>	<u>20</u>
<u>Выполнение.....</u>	<u>20</u>

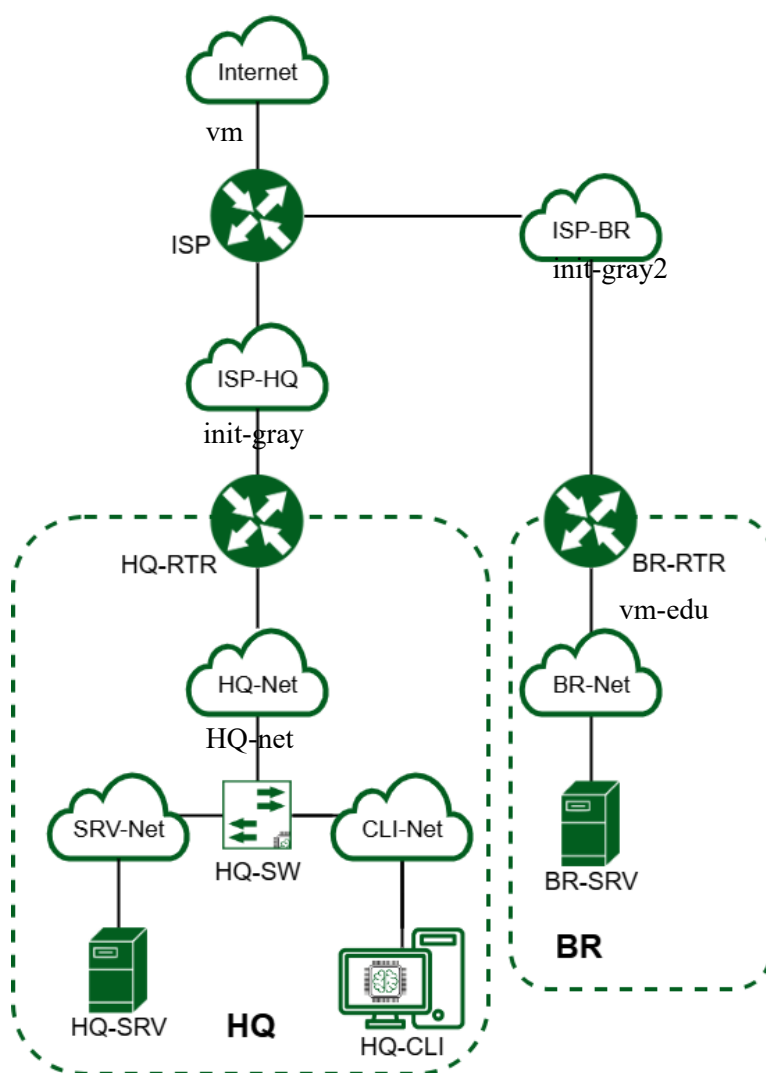
Модуль 1. Настройка сетевой инфраструктуры

Задание:

Необходимо разработать и настроить инфраструктуру информационно-коммуникационной системы согласно предложенной топологии. 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.



Задание 1. Произведите базовую настройку устройств

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

Выполнение

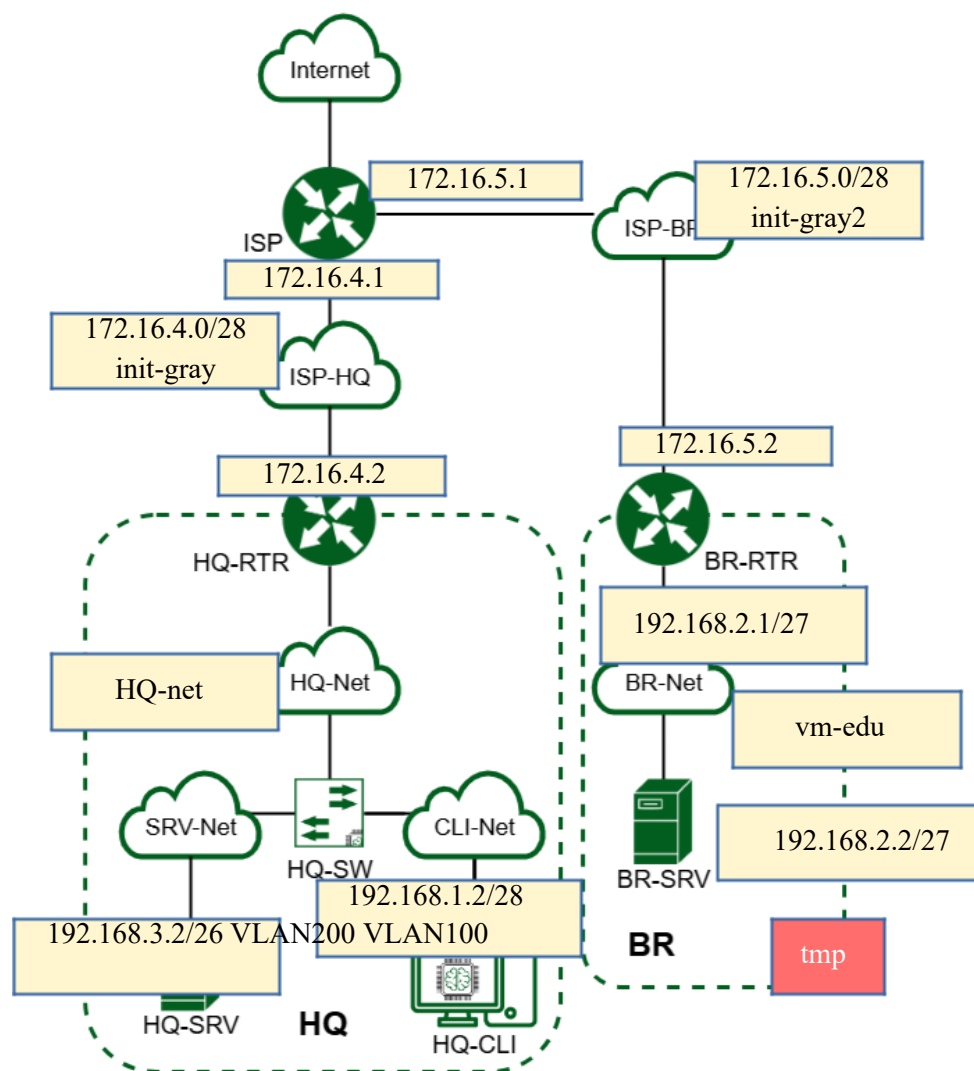
Имена устройств сведём в таблицу. Всего у нас 6 устройств

Название на схеме	FQDN
ISP	isp.au-team.irpo
HQ-RTR	hq-rtr.au-team.irpo
BR-RTR	br-rtr.au-team.irpo
HQ-SRV	hq-srv.au-team.irpo
HQ-CLI	hq-cli.au-team.irpo
BR-SRV	br-srv.au-team.irpo

Настройку имени устройств можно произвести несколькими способами самое простое использовать команду:

hostnamectl set-hostname <FQDN из таблицы выше> ; exec bash

команда **exec bash** перезапускает терминал и заданное имя будет отображаться



Сеть между HQ-RTR и HQ-SRV – VLAN100 не более 64 адресов. 64 это 2 в степени 6, значит маска сети $32-6=26$ сеть выберем 192.168.3.0/26

Сеть между HQ-RTR и HQ-CLI – VLAN200 не более 16 адресов. 16 это 2 в степени 4, значит маска сети $32-4=28$ сеть выберем 192.168.1.0/28

Сеть HQ-RTR для управления – VLAN999 не более 8 адресов. 8 это 2 в степени 3, значит маска сети $32-3=29$ сеть выберем 192.168.4.0/29

Сеть между BR-RTR и BR-SRV – не более 32 адресов. 32 это 2 в степени 5, значит маска сети $32-5=27$ сеть выберем 192.168.2.0/27

создадим таблицу IP-адресов сетей.

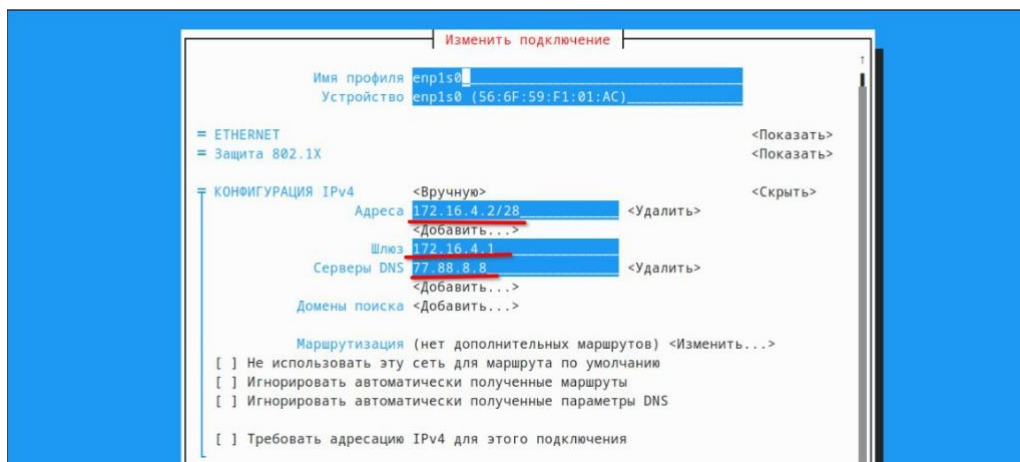
Имя	Количество адресов	IP адрес и префикс маски	Маска сети	Диапазон адресов
HQ-VLAN100	64	192.168.3.0/26	255.255.255.192	192.168.3.1-192.168.3.62
HQ-VLAN200	16	192.168.1.0/28	255.255.255.240	192.168.1.1-192.168.1.14
HQ-VLAN999	8	192.168.4.0/29	255.255.255.248	192.168.4.1-192.168.4.6
BR	32	192.168.2.0/27	255.255.255.224	192.168.2.1-192.168.2.30

Теперь определим IP-адреса на интерфейсах каждой машины

ISP	DHCP	—	Internet
	172.16.4.1/28	—	HQ-RTR
	172.16.5.1/28	—	BR-RTR
HQ-RTR	172.16.4.2/28	172.16.4.1	ISP
	192.168.1.1/28	—	управление
	192.168.3.1/26	—	HQ-SRV
	192.168.4.1/29	—	HQ-CLI
BR-RTR	172.16.5.2/28	172.16.5.1	ISP
	192.168.2.1/27	—	BR-SRV
HQ-SRV	192.168.3.2/26	192.168.3.1	HQ-RTR
HQ-CLI	192.168.1.2/28	192.168.1.1	HQ-RTR
BR-SRV	192.168.2.2/27	192.168.2.1	BR-RTR

Адресацию ISP берем из пункта 2 задания.

Настраивать IP адреса интерфейсов удобно через утилиту **nmtui**.



Проверить результат настройки IP-адресов можно с помощью команды:

ip -c -br a

На устройствах ISP, HQ-RTR, BR-RTR необходимо включить пересылку пакетов между интерфейсами - forwarding

sysctl net.ipv4.ip_forward=1 >> /etc/sysctl.conf

Для спокойствия применить параметры из файла

sysctl -p

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

Выполнение

Сетевые интерфейсы были настроены на предыдущем шаге

В РЕД ОС 8 по умолчанию используется nftables, разберём как настраивается сначала iptables.

Или iptables

Устанавливаем и активируем службу iptables

apt install iptables-services -y && systemctl enable --now iptables

Удаляем все правила, так как в РЕД ОС 8 существуют правила по умолчанию.

iptables -F

Добавляем правило NAT для внешнего интерфейса

iptables -t nat -A POSTROUTING -o enp1s0 -j MASQUERADE Сохраняем настройки
service iptables save

Или nftables

Создаем и открываем файл

nano /etc/nftables/isp.nft

Прописываем следующие строки

```
table inet nat {  
    chain POSTROUTING {  
        type nat hook postrouting priority srcnat; oifname "enp1s0"  
        masquerade  
    }  
}
```

где enp1s0 - интерфейс ISP (смотрящий в Интернет)

Включаем использование данного файла в sysconfig

nano /etc/sysconfig/nftables.conf

Ниже строки начинающейся на *include*, прописываем строку

include "/etc/nftables/isp.nft"

Запуск и добавление в автозагрузку сервиса nftables

systemctl enable --now nftables

Для проверки настроек нужно отправить пинг на любой внешний адрес с устройства HQ-RTR или BR-RTR.

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`
- При настройке на EcoRouter пользователь `net_admin` должен обладать максимальными привилегиями
- При настройке ОС на базе Linux, запускать `sudo` без дополнительной аутентификации

Выполнение

На HQ-SRV и BR-SRV

Добавить пользователя с уникальным ID в систему можно командой

`useradd -u 1010 sshuser`

Устанавливаем пароль пользователю `sshuser` **`passwd sshuser`**

Два раза вводим пароль `P@ssw0rd`

Для установки возможности запуска команды `sudo` без пароля достаточно в файл `/etc/sudoers` добавить следующую строчку

`sshuser ALL=(ALL) NOPASSWD: ALL` На маршрутизаторах HQ-RTR

и BR-RTR

Добавить пользователя в систему можно командой

`useradd net_admin`

Устанавливаем пароль пользователю `sshuser` **`passwd`**

`net_admin`

Два раза вводим пароль `P@$word`

Для установки возможности запуска команды `sudo` без пароля достаточно в файл `/etc/sudoers` добавить следующую строчку

`net_admin ALL=(ALL) NOPASSWD: ALL`

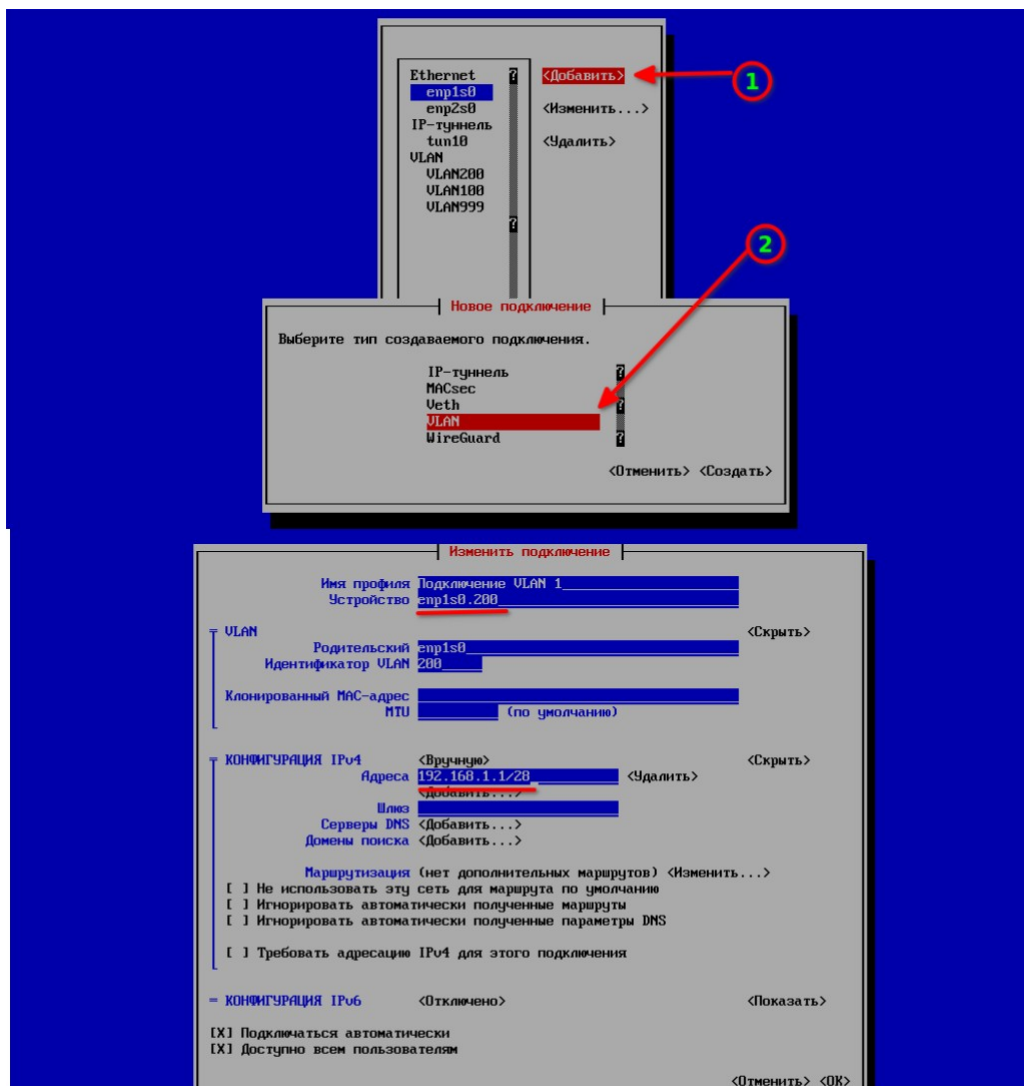
Нужно ли добавлять при этом пользователей в группу `wheel`? НЕТ!!!

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

Выполнение

Для настройки VLAN тоже удобно использовать nmtui



Главное правило не забыть какой интерфейс в какую сторону смотрит и обязательно проверять корректность настроек. В результате настроек на интерфейсе смотрящем в сторону сети HQ должно быть три подинтерфейса с различными VLAN.

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»

Выполнение

Все отключают SELinux. Зачем?

Так как все настройки которые мы будем изменять закомментированы, то воспользуемся отдельным файлом конфигурации ssh, который разместим в папке /etc/ssh/sshd_config.d/ Главное помнить, что имя файла должно содержать латинские символы и окончание .conf

Port 2024	#Изменение порта
AllowUsers net_admin	#Логин, которому можно подключаться
Banner /etc/ssh/baner.txt	#Указатель на файл банера
MaxAuthTries 2	#Количество попыток ввода пароля

Номер порта необходимо прописать в SELinux. Подсказка есть в конфигурационном файле sshd.

Создаём файл банера с текстом «Authorized access only»

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

Не забываем добавить порт в SELinux

semanage port -m -t ssh_port_t -p tcp 2024 Чтобы применить изменения, перезапускаем службу SSH

```
# systemctl restart sshd
```

Настройка на BR-SRV аналогичная Обязательно

проверяйте каждый шаг. Подключаемся и вводим

пароль P@\$Sword

```
[admin@tmp ~]$ ssh net_admin@172.16.4.2 -p 2024
#####
#      Authorized accass only      #
#####
net_admin@172.16.4.2's password:
Last login: Fri Feb 14 22:25:28 2025 from 172.16.4.3
[net_admin@HQ-RTR ~]$
```

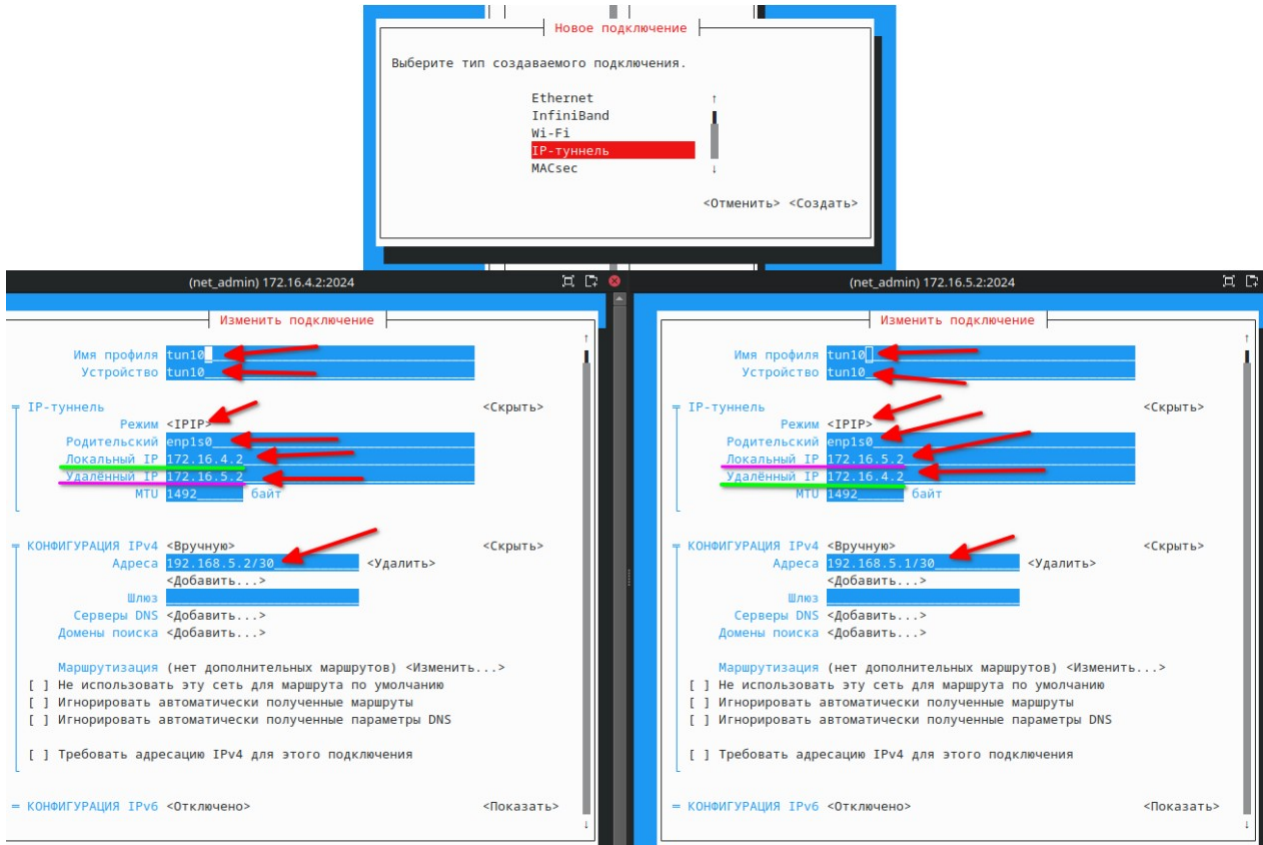
Задание 6. Между офисами HQ и BR необходимо сконфигурировать IP туннель

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

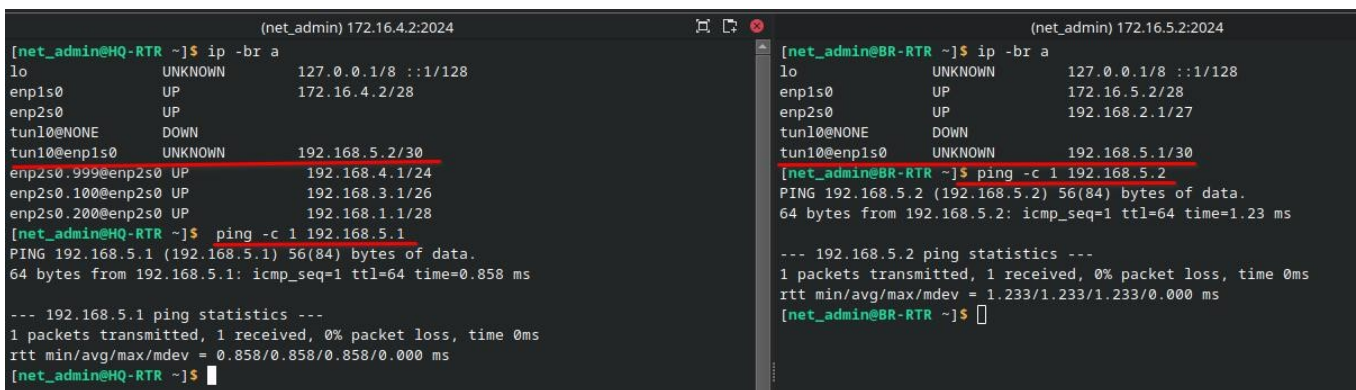
Выполнение

Имена tun0, gre0 и sit0 являются зарезервированными в iproute2 («base devices») и имеют особое поведение.

Мы выбрали технологию IPIP. Добавляем тоннель и настраиваем



Проверяем



Возможно что для корректной работы протокола динамической маршрутизации требуется увеличить параметр TTL на интерфейсе туннеля

GRE-туннеля между HQ-RTR и BR-RTR с использованием Netplan:
Для HQ-RTR (172.16.4.2/28):

Для работы с GRE и IPIP туннелями нам потребуется загрузить специальные модули ядра, для этого откроем файл **/etc/modules** и внесем в него строки:

```
ip_gre
```

```
ipip
```

```
# /etc/netplan/01-netcfg.yaml
```

```
network:
```

```
  version: 2
```

```
  renderer: networkd
```

```
  ethernets:
```

```
    ens33:
```

```
      addresses:
```

```
        - 172.16.4.2/28
```

```
      nameservers:
```

```
        addresses: [77.88.8.8, 8.8.4.4]
```

```
  tunnels:
```

```
    gre0:
```

```
      mode: gre
```

```
      local: 172.16.4.2 # Замените на реальный внешний IP HQ-RTR
```

```
      remote: 172.16.4.2 # Замените на реальный внешний IP BR-RTR
```

```
      addresses: [10.10.10.1/30]
```

```
#    routes:
```

```
#      - to: 172.16.5.0/28
```

```
#      via: 10.10.10.2
```

Для BR-RTR (172.16.5.2/28):

```
# /etc/netplan/01-netcfg.yaml
```

```
network:
```

```
  version: 2
```

```
  renderer: networkd
```

```
  ethernets:
```

```
    ens33:
```

```
      addresses:
```

```
        - 172.16.5.2/28
```

```
      nameservers:
```

```
        addresses: [77.88.8.8, 8.8.4.4]
```

```
  tunnels:
```

```
    gre0:
```

```
      mode: gre
```

```
      local: 172.16.5.2 # Замените на реальный внешний IP BR-RTR
```

```
      remote: 172.16.4.2 # Замените на реальный внешний IP HQ-RTR
```

```
      addresses: [10.10.10.2/30]
```

```
#    routes:
```

```
#      - to: 172.16.4.0/28
```

```
#      via: 10.10.10.1
```

Дополнительные настройки:

После настройки примените изменения:

```
sudo netplan apply
```

Проверьте туннель:

```
ip tunnel show
```

```
ping 10.10.10.2 # с HQ-RTR должен пинговать BR-RTR и наоборот
```

Для маршрутизации между сетями добавьте соответствующие правила маршрутизации в конфигурацию Netplan или используйте динамическую маршрутизацию (OSPF, BGP и т.д.)

Не забудьте настроить форвардинг пакетов на обоих маршрутизаторах:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Для постоянного включения форвардинга добавьте в **/etc/sysctl.conf**:

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

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 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

Выполнение

Для динамической маршрутизации выберем протокол OSPF. Такой протокол реализован в пакете frr.

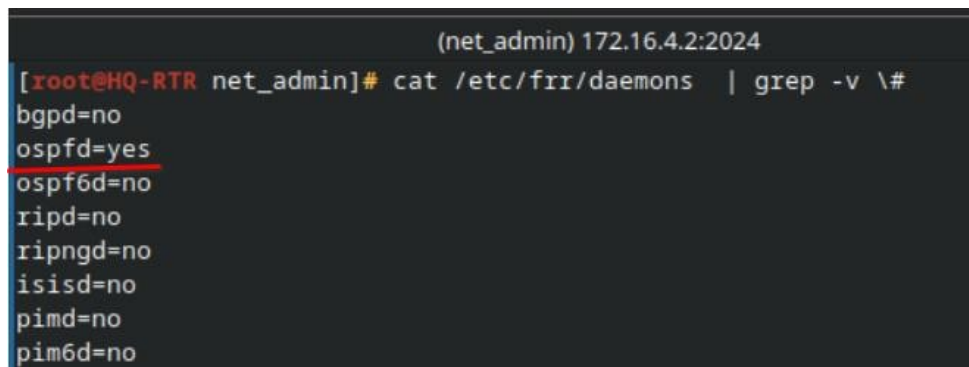
Устанавливаем пакет frr

apt install -y frr

Включаем соответствующий демон в конфигурационном файле

/etc/frr/daemons

Находим строчку с нужным протоколом и меняем **no** на **yes**.



```
(net_admin) 172.16.4.2:2024
[root@HQ-RTR net_admin]# cat /etc/frr/daemons | grep -v \#
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
pim6d=no
```

Включаем и добавляем в автозагрузку службу FRR

systemctl enable --now frr

Переходим в терминал управления FRR командой vtysh (аналог cisco) **# vtysh**

Далее выполняем команды как и в циско 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**

Переводим все интерфейсы в пассивный режим

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

Объявляем все сети кроме внешних соответствующенго RTR, например для HQ-RTR

hq-rtr.au-team.irpo(config-router)# **network 192.168.1.0/28 area 0** hq-rtr.au-team.irpo(config-router)# **network 192.168.3.0/26 area 0** hq-rtr.au-team.irpo(config-router)# **network 192.168.4.0/24 area 0** hq-rtr.au-team.irpo(config-router)# **network 192.168.5.0/30 area 0**

Настройка аутентификации

hq-rtr.au-team.irpo(config-router)# **area 0 authentication**

Выходим из режима конфигурации OSPFv2

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

Теперь важный момент, настраиваем активный интерфейс **tun10** Переходим в режим конфигурирования интерфейса tun1

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

tun10 делаем активным, для установления соседства с BR-RTR и обмена внутренними маршрутами

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

Переводим интерфейс tun1 в активный режим

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

Настройка аутентификации с открытым паролем password

```
hq-rtr.au-team.irpo(config-if)# ip ospf authentication
```

```
hq-rtr.au-team.irpo(config-if)# ip ospf authentication-key password
```

Выходим из конфигурации и tun1

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

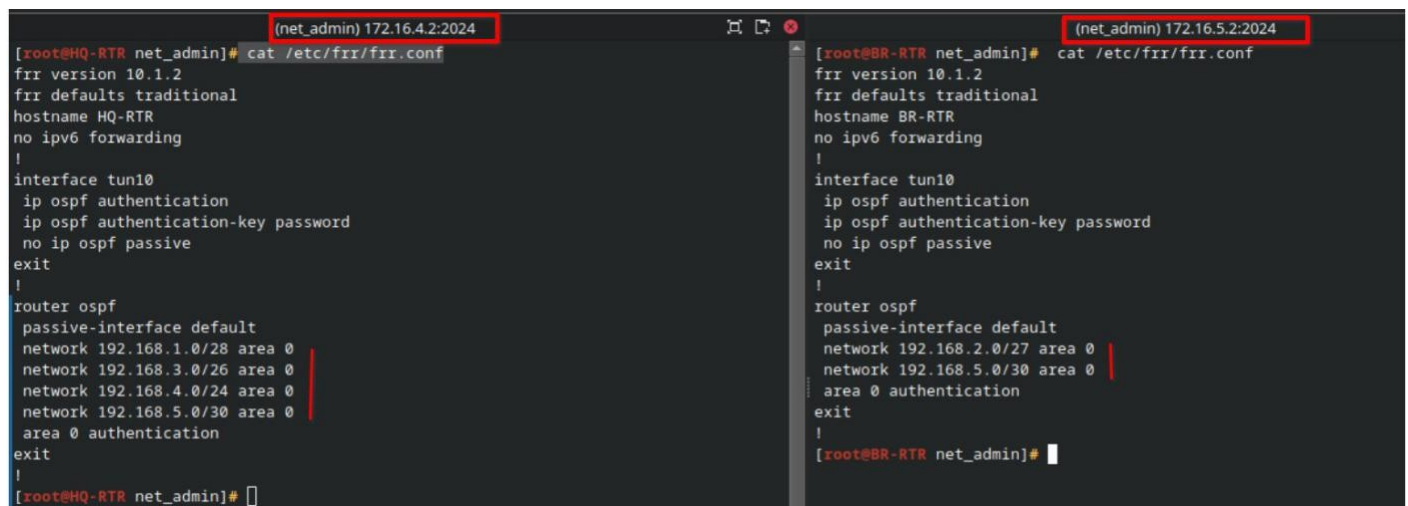
Выходим из режима конфигурации hq-

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

Сохраняем текущую конфигурацию hq-rtr.au-team.irpo# **write** Перезапускаем frr

```
systemctl restart frr
```

Проверяем конфигурационный файл.



The screenshot shows two terminal windows side-by-side. The left window is titled '(net_admin) 172.16.4.2:2024' and shows the configuration for HQ-RTR. The right window is titled '(net_admin) 172.16.5.2:2024' and shows the configuration for BR-RTR. Both configurations include OSPF settings for area 0 and authentication using the password 'password'.

```
[root@HQ-RTR net_admin]# cat /etc/frr/frr.conf
frr version 10.1.2
frr defaults traditional
hostname HQ-RTR
no ipv6 forwarding
!
interface tun10
 ip ospf authentication
 ip ospf authentication-key password
 no ip ospf passive
exit
!
router ospf
 passive-interface default
 network 192.168.1.0/28 area 0
 network 192.168.3.0/26 area 0
 network 192.168.4.0/24 area 0
 network 192.168.5.0/30 area 0
 area 0 authentication
exit
!
[root@HQ-RTR net_admin]#
```

```
[root@BR-RTR net_admin]# cat /etc/frr/frr.conf
frr version 10.1.2
frr defaults traditional
hostname BR-RTR
no ipv6 forwarding
!
interface tun10
 ip ospf authentication
 ip ospf authentication-key password
 no ip ospf passive
exit
!
router ospf
 passive-interface default
 network 192.168.2.0/27 area 0
 network 192.168.5.0/30 area 0
 area 0 authentication
exit
!
[root@BR-RTR net_admin]#
```

На BR-RTR настраиваем OSPF аналогично, не забываем что пассивные сети другие. Когда настроили BR-RTR, можно проверить работу протокола.

Проверяем получены ли маршруты

```
(net_admin) 172.16.4.2:2024
[root@HQ-RTR net_admin]# ip r
default via 172.16.4.1 dev enp1s0 proto static metric 100
172.16.4.0/28 dev enp1s0 proto kernel scope link src 172.16.4.2 metric 100
192.168.1.0/28 dev enp2s0.200 proto kernel scope link src 192.168.1.1 metric 402
192.168.2.0/27 nhid 22 via 192.168.5.1 dev tun10 proto ospf metric 20
192.168.3.0/26 dev enp2s0.100 proto kernel scope link src 192.168.3.1 metric 401
192.168.4.0/24 dev enp2s0.999 proto kernel scope link src 192.168.4.1 metric 400
192.168.5.0/30 dev tun10 proto kernel scope link src 192.168.5.2 metric 675
[root@HQ-RTR net_admin]#

(net_admin) 172.16.5.2:2024
[root@BR-RTR net_admin]# ip r
default via 172.16.5.1 dev enp1s0 proto static metric 100
172.16.5.0/28 dev enp1s0 proto kernel scope link src 172.16.5.2 metric 100
192.168.1.0/28 nhid 14 via 192.168.5.2 dev tun10 proto ospf metric 20
192.168.2.0/27 dev enp2s0 proto kernel scope link src 192.168.2.1 metric 101
192.168.3.0/26 nhid 14 via 192.168.5.2 dev tun10 proto ospf metric 20
192.168.4.0/24 nhid 14 via 192.168.5.2 dev tun10 proto ospf metric 20
192.168.5.0/30 dev tun10 proto kernel scope link src 192.168.5.1 metric 675
[root@BR-RTR net_admin]#
```

Для проверки работы дополнительно в vtysh можно использовать некоторые команды

Получить информацию о соседях и установленных отношениях соседства.

show ip ospf neighbor

```
[root@BR-RTR net_admin]# vtysh
Hello, this is FRRouting (version 10.1.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

BR-RTR# show ip ospf neighbor

Neighbor ID      Pri State           Up Time           Dead Time Address          Interface          RXmtL RqstL DBsmL
192.168.5.2      1 Full/-          22h23m36s        35.610s 192.168.5.2      tun10:192.168.5.1 0      0      0

BR-RTR#
```

Показать маршруты, полученные от процесса OSPF.

show ip route ospf

```
[root@BR-RTR net_admin]# vtysh
Hello, this is FRRouting (version 10.1.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

BR-RTR# show ip route ospf
Codes: K - kernel route, C - connected, L - local, S - static,
R - RIP, O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, F - PBR,
f - OpenFabric, t - Table-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure

O>* 192.168.1.0/28 [110/20] via 192.168.5.2, tun10, weight 1, 22:24:25
O 192.168.2.0/27 [110/10] is directly connected, enp2s0, weight 1, 22:24:36
O>* 192.168.3.0/26 [110/20] via 192.168.5.2, tun10, weight 1, 22:24:25
O>* 192.168.4.0/24 [110/20] via 192.168.5.2, tun10, weight 1, 22:24:25
O 192.168.5.0/30 [110/10] is directly connected, tun10, weight 1, 22:24:36
BR-RTR#
```

Задание 8. Настройка динамической трансляции адресов.

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

Выполнение

В задании 2 мы настраивали динамическую трансляцию для ISP. Повторяем те же действия, но для RTR устройств

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.

Выполнение

Установка DHCP сервера

apt install isc-dhcp-server -y

Настройки для диапазона адресов IPv4 производятся в файле **/etc/dhcp/dhcpd.conf**.

Пример данного файла можно посмотреть в файле

/usr/share/doc/dhcp-server/dhcpd.conf.example

Приводим файл к виду:

```
subnet 192.168.1.0 netmask 255.255.255.240 { range 192.168.1.2
    192.168.1.14;
    option domain-name-servers 192.168.3.2;
    option domain-name "au-team.irpo";
    option routers 192.168.1.1;
    option broadcast-address 192.168.1.15;
}
```

где

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.

Запускаем и добавляем в автозагрузку службу dhcpd:

systemctl enable --now dhcpd

Проверка на HQ-CLI перезагружаем сетевой интерфейс и убеждаемся в работоспособности DHCP сервера

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.

Выполнение

Дополним выданную таблицу

Таблица 2

Устройство	Запись	Тип	ИП
HQ-RTR	hq-rtr.au-team.irpo	A,PTR	192.168.1.1
BR-RTR	br-rtr.au-team.irpo	A	
HQ-SRV	hq-srv.au-team.irpo	A,PTR	192.168.3.2
HQ-CLI	hq-cli.au-team.irpo	A,PTR	192.168.1.2
BR-SRV	br-srv.au-team.irpo	A	
HQ-RTR	moodle.au-team.irpo	CNAME	
HQ-RTR	wiki.au-team.irpo	CNAME	

ИП адрес на HQ-SRV настраиваем статический.

Устанавливаем пакет bind

```
apt install bind9 dnsutils
```

Редактируем конфигурационный файл /etc/named.conf. В данном файле

необходимо изменить следующие строки, содержащие

```
listen-on port 53 { any; };  
listen-on-v6 port 53 { none; };  
allow-query { any; };;  
forwarders { 77.88.8.8; };
```

Объявляем зоны, дописываем в конец файла /etc/named.conf строки **zone "au-team.irpo" {**

```
type master;  
file "master/au-team.irpo";  
};  
zone "1.168.192.in-addr.arpa" {  
type master;  
file "master/au-team1.ptr";  
};  
zone "3.168.192.in-addr.arpa" {  
type master;file "master/au-team3.ptr";  
};
```

```

zone "." IN {
    type hint;
    file "named.ca";
};

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

zone "1.168.192.in-addr.arpa" {
    type master;
    file "master/au-team1.ptr";
};

zone "3.168.192.in-addr.arpa" {
    type master;
    file "master/au-team3.ptr";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

```

где:

zone "au-team.irpo">{ ... }; определения зоны au-team.irpo . В кавычках указывается имя зоны, которое следует разрешать на этом сервере. zone "1.168.192.in-addr.arpa">{ ... } и zone "3.168.192.in-addr.arpa">{ ... } определения обратной зоны au-team.irpo .

Файлов обратной зоны мы создали 2 для удобства и простоты по адресам адресов обратных зон

Создаём файлы описания зон

В системе есть примеры файлов обратной и прямой зоны, можно использовать эти примеры для создания нужных файлов

```

[root@HQ-SRV sshuser]# ls -l /var/named/
итого 32
drwxrwx---. 2 named named 4096 фев  6 21:19 data
drwxrwx---. 2 named named 4096 апр  1 15:50 dynamic
drwxr-xr-x. 2 root  root  4096 апр  1 14:25 master
-rw-r-----. 1 root  named 3317 июл 29  2024 named.ca
-rw-r-----. 1 root  named  152 июл 29  2024 named.empty
-rw-r-----. 1 root  named  152 июл 29  2024 named.localhost
-rw-r-----. 1 root  named  168 июл 29  2024 named.loopback
drwxrwx---. 2 named named 4096 июл 29  2024 slaves
[root@HQ-SRV sshuser]#

```

```

[root@HQ-SRV sshuser]# ls /var/named/master/
au-team1.ptr  au-team3.ptr  au-team.irpo

```

Приводим созданные файлы к виду:

```
[root@HQ-SRV sshuser]# cat /var/named/master/au-team.irpo
$TTL 604800
;
au-team.irpo. IN SOA hq-srv.au-team.irpo. root.au-team.irpo. (
    1 ; Serial
    600 ; Refresh
    3600 ; Retry
    1w ; Expire
    360 ; Minimum TTL
)
IN NS au-team.irpo.
IN A 192.168.3.2
hq-rtr IN A 192.168.3.1
br-rtr IN A 192.168.2.1
hq-srv IN A 192.168.3.2
hq-cli IN A 192.168.1.2
br-srv IN A 192.168.2.2
moodle IN CNAME hq-rtr.au-team.irpo.
wiki IN CNAME hq-rtr.au-team.irpo.
```

```
[root@HQ-SRV sshuser]# cat /var/named/master/au-team1.ptr
$TTL 604800
;
@ IN SOA au-team.irpo. root.au-team.irpo. (
    1 ; Serial
    600 ; Refresh
    3600 ; Retry
    1w ; Expire
    360 ; Minimum TTL
)
IN NS au-team.irpo.
1 IN PTR hq-rtr.au-team.irpo.
2 IN PTR hq-cli.au-team.irpo.
```

```
[root@HQ-SRV sshuser]# cat /var/named/master/au-team3.ptr
$TTL 604800
;
@ IN SOA au-team.irpo. root.au-team.irpo. (
    1 ; Serial
    600 ; Refresh
    3600 ; Retry
    1w ; Expire
    360 ; Minimum TTL
)
IN NS au-team.irpo.
2 IN PTR hq-srv.au-team.irpo.
```

named-checkconf -z

Если есть ошибки исправляем

ПРОВЕРЯЕМ работает ли прямая и обратная зоны

```
[root@HQ-SRV sshuser]# nslookup moodle.au-team.irpo
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
moodle.au-team.irpo      canonical name = hq-rtr.au-team.irpo.
Name:   hq-rtr.au-team.irpo
Address: 192.168.3.1
```

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

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

Выполнение

Проверяем часовой пояс
timedatectl

Список доступных часовых поясов можно посмотреть командой

ls /usr/share/zoneinfo/

Посмотреть список регионов и городов

ls /usr/share/zoneinfo/Europe/

Настроим Московский часовой пояс (UTC +3):

timedatectl set-timezone Europe/Moscow

Изменение даты и времени при необходимости

Для изменения даты и времени используется команда: **imedatectl set-**

time "<дата> <время>

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

Проверка:

timedatectl