



Разбор демонстрационного экзамена 2026 по специальности 09.02.06 Сетевое
и системное администрирование, адаптированный под ОС Debian 13

АННОТАЦИЯ

На Debian 13 некоторые пакеты отсутствуют и их придется устанавливать вручную (в гайде описаны какие).

Рекомендации по заданиям:

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

Все остальное можно делать по порядку.

СПИСОК ИЗМЕНЕНИЙ

В силу развития Debian 13 были изменены некоторые пакеты и их версии, соответственно изменились методы и принципы использования данного программного обеспечения:

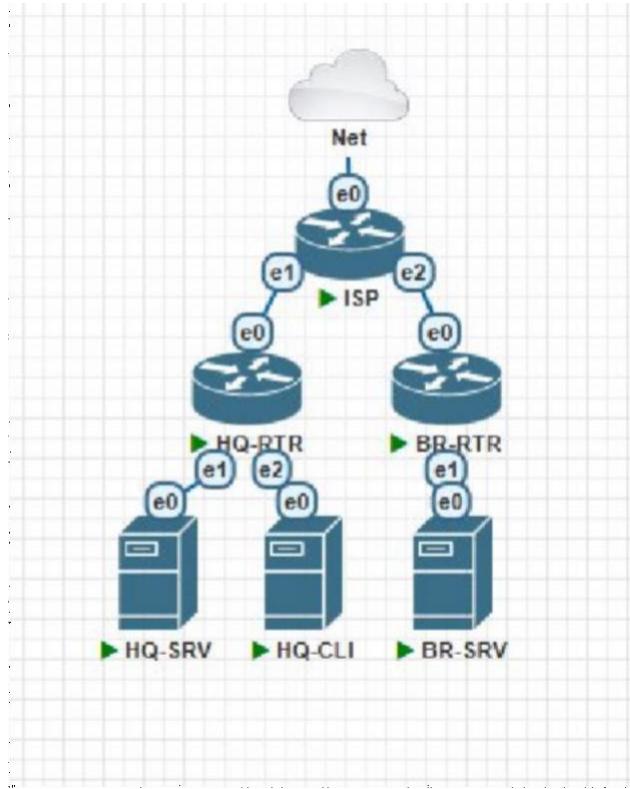
1. В разборе nmtui был заменен на ifupdown (networking)
(исключением является GRE-туннель, он по прежнему на nmtui)
2. iptables был заменен на nftables
3. Файл /etc/sysctl.conf переехал в /etc/sysctl.d/sysctl.conf
(примечание: файл по умолчанию пустой, правила теперь придется писать самостоятельно)
4. login заменен на su
5. bind усложнили удалением комментариев и стандартных файлов

Комментарий от автора

Debian 13 претерпел колоссальное количество изменений, добавилось много новых усложнений — теперь придется отказаться от старых принципов работы... Нужно адаптироваться к новому ПО, ведь «хороший сисадмин тот, который может быстро разобраться с тем, с чем никогда не имел дела» =)

РАЗВЕРТЫВАНИЕ СТЕНДА

Создадим в PNetLab такую схему:

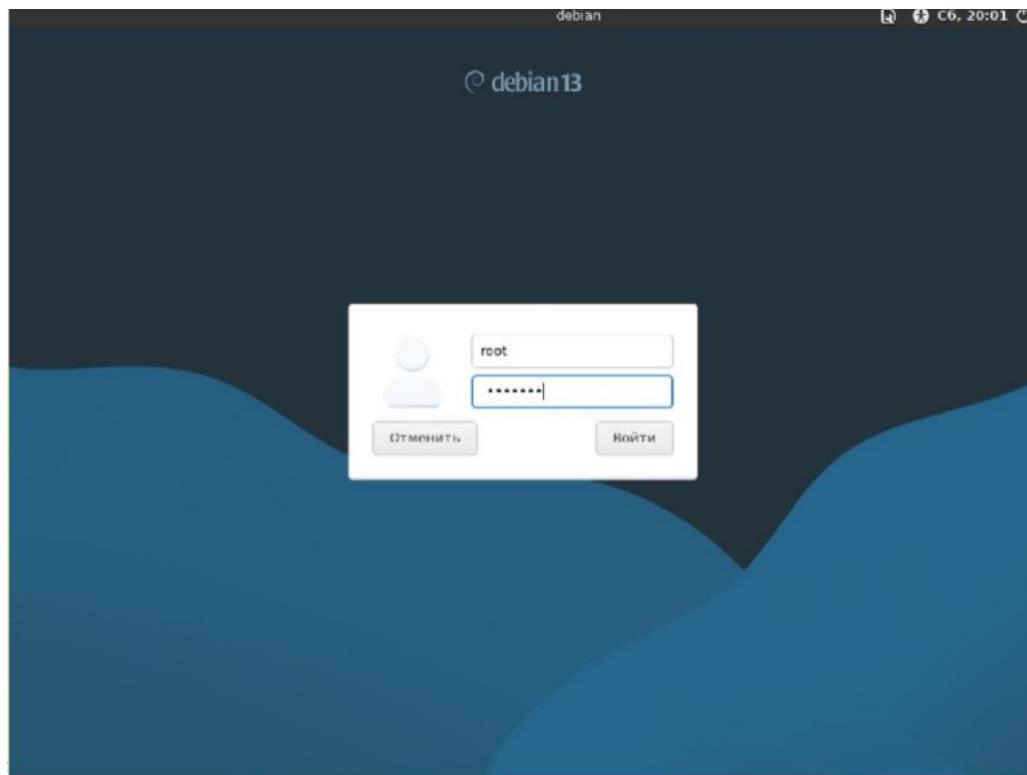


1. Net: cloud_nat
2. ISP: 1 CPU, 1024 RAM, 3 Ethernet
3. HQ-RTR: 1 CPU, 1024 RAM, 4 Ethernet
4. BR-RTR: 1 CPU, 1024 RAM, 2 Ethernet
5. HQ-SRV: 1 CPU, 1024 RAM, 1 Ethernet
6. HQ-CLI: 1 CPU, 1024 RAM, 1 Ethernet
7. BR-SRV: 1 CPU, 1024 RAM, 1 Ethernet

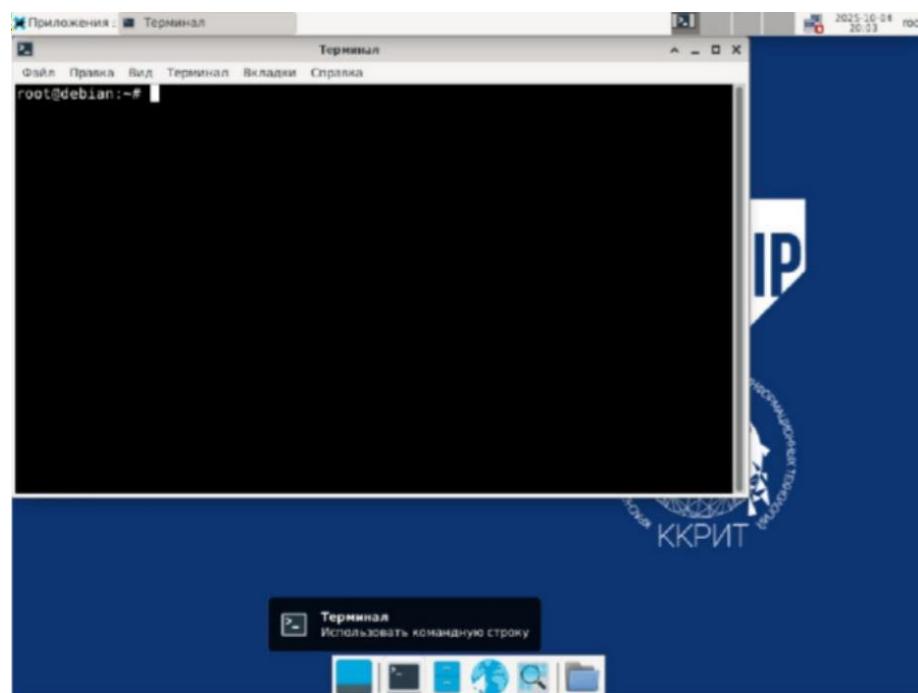
Все устройства на базе Linux Debian 13.

ВНИМАНИЕ!!! ТО ЧТО ОПИСАНО НИЖЕ ОЧЕНЬ ВАЖНО!!!
ПРОДЕЛАТЬ НА ВСЕХ УСТРОЙСТВАХ!!!

На экране входа в пользователя вводим стандартные данные учетной записи root. Пароль Test123.



Первым делом открываем терминал



И редактируем репозиторий через редактор nano

```
root@debian:~# nano /etc/apt/sources.list
```

Для тех у кого не работает инет в пинете надо открыть конфиг nano

/etc/resolv.conf и nameserver поменять на 8.8.8.8 или если стоит search полностью стереть строку и вписать nameserver 8.8.8.8

НА 10 ПУНКТЕ МОЖЕТ ВЫЛЕЗТИ ОШИБКА ПРИ СКАЧИВАНИИ bind9, ЕСЛИ ЭТО ПРОИЗОЙДЕТ, ПИШЕМ sudo apt-get update

Ставим комментарий на первой строчке символом #

```
GNU nano 8.4                               /etc/apt/sources.list *
#deb cdrom:[Debian GNU/Linux 13.1.0 _Trixie_ - Official amd64 DVD Binary-1 with>
      deb http://deb.debian.org/debian/ trixie main non-free-firmware
      deb-src http://deb.debian.org/debian/ trixie main non-free-firmware

      deb http://security.debian.org/debian-security trixie-security main non-free-fi>
      deb-src http://security.debian.org/debian-security trixie-security main non-fre>

      # trixie-updates, to get updates before a point release is made;
      # see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates>
      deb http://deb.debian.org/debian/ trixie-updates main non-free-firmware
      deb-src http://deb.debian.org/debian/ trixie-updates main non-free-firmware
```

Выходим Ctrl+X, y, Enter.

! Почему это важно?

— Это важно, потому что Debian по умолчанию использует репозиторий с локального .iso образа (CD-ROM). Так как Debian уже установлен и CD-ROM извлечен, установщик пакетов apt будет ждать образ Debian в виртуальном дисководе и брать оттуда пакеты. Но он его не дождется, и пакеты устанавливаться не начнут. Поэтому отключаем этот репозиторий на всех устройствах, чтобы установка производилась через Интернет.

МОДУЛЬ 1

+ 1

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(VLAN 100) должна вмещать не более 32 адресов
 - Локальная сеть в сторону HQ-CLI(VLAN 200) должна вмещать не менее 16 адресов
 - Локальная сеть для управления(VLAN 999) должна вмещать не более 8 адресов
 - Локальная сеть в сторону BR-SRV должна вмещать не более 16 адресов

Зададим имена устройствам полным доменным именем:

На ISP:

```
root@debian:~# hostnamectl set-hostname isp.au-team.irpo; exec bash
```

На HQ-RTR:

```
root@debian:~# hostnamectl set-hostname hq-rtr.au-team.irpo; exec bash
```

На BR-RTR:

```
root@debian:~# hostnamectl set-hostname br-rtr.au-team.irpo; exec bash
```

На HQ-SRV:

```
root@debian:~# hostnamectl set-hostname hq-srv.au-team.irpo; exec bash
```

На HQ-CLI:

```
root@debian:~# hostnamectl set-hostname hq-cli.au-team.irpo; exec bash
```

На BR-SRV:

```
root@debian:~# hostnamectl set-hostname br-srv.au-team.irpo; exec bash
```

Сконфигурируем IPv4.

Руководствуясь требованиями задания составим таблицу IP-адресации.

Имя устройства	IP-адрес	Шлюз по умолчанию	Сеть
ISP	DHCP		Интернет
	172.16.1.1/28	-	От ISP к HQ-RTR
	172.16.2.1/28	-	От ISP к BR-RTR
HQ-RTR	172.16.1.2/28	172.16.1.1	От ISP к HQ-RTR
	192.168.100.1/27	-	От HQ-RTR к HQ-SRV (VLAN100)
	192.168.100.33/28	-	От HQ-RTR к HQ-CLI (VLAN200)
	192.168.100.49/29	-	VLAN999
HQ-SRV	192.168.100.2/27	192.168.100.1	От HQ-RTR к HQ-SRV
HQ-CLI	DHCP	192.168.100.33 (DHCP)	От HQ-RTR к HQ-CLI
BR-RTR	172.16.2.2/28	172.16.2.1	От ISP к BR-RTR
	192.168.200.1/28	-	От BR-RTR к BR-SRV
BR-SRV	192.168.200.2/28	192.168.200.1	От BR-RTR к 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.*.*



2. Настройте доступ к сети Интернет, на маршрутизаторе ISP:

Настройте адресацию на интерфейсах:

- Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP
- Настройте маршрут по умолчанию, если это необходимо
- Настройте интерфейс, в сторону HQ-RTR, интерфейс подключен к сети 172.16.1.0/28
- Настройте интерфейс, в сторону BR-RTR, интерфейс подключен к сети 172.16.2.0/28
- На ISP настройте динамическую сетевую трансляцию портов для доступа к сети Интернет HQ-RTR и BR-RTR.

P.S. В данном задании мы сразу сделаем задание 8, чтобы не терять время.

8. Настройка динамической трансляции адресов маршрутизаторах HQ-RTR и BR-RTR:

- Настройте динамическую трансляцию адресов для обоих офисов в сторону ISP, все устройства в офисах должны иметь доступ к сети Интернет

Проведем базовую настройку сети через конфигурационный файл /etc/network/interfaces.

На ISP:

```
root@isp:~# nano /etc/network/interfaces
```

```
GNU nano 8.4 /etc/network/interfaces
# and how to activate them. For more information see the manual page for interfaces(5).
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet dhcp

auto ens4
iface ens4 inet static
address 172.16.1.1/28

auto ens5
iface ens5 inet static
address 172.16.2.1/28

post-up nft -f /etc/nftables.conf
```

^G Справка ^O Записать ^F Поиск ^K Выр
^X Выход ^R ЧитФайл ^\ Замена ^U Вст

- auto ens3 – автоматическое включение интерфейса
- iface ens3 inet dhcp/static – тип интерфейса (динамический/статический)
- address 172.16.1.1/28 – задание IP-адреса на интерфейс
- post-up nft -f /etc/nftables.conf – исполнение команды после загрузки конфигурационного файла (в данном случае это применение настроек файла nftables)

Выходим с файла: Ctrl+X, y, Enter.

СДЕЛАТЬ НА ISP, HQ-RTR И BR-RTR СТРОГО, ИНАЧЕ ИНЕТ НЕ БУДЕТ РАБОТАТЬ

Редактируем sysctl.conf

```
root@isp:~# nano /etc/sysctl.d/sysctl.conf
```

```
GNU nano 8.4
net.ipv4.ip_forward=1
```

Выходим с файла: Ctrl+X, y, Enter.

Применяем правила sysctl

```
root@isp:~# sysctl --system
```

Сделаем динамическую трансляцию адресов (**проделать также на HQ- RTR, BR-RTR!**)

```
root@isp:~# nano /etc/nftables.conf
```

```
GNU nano 8.4                               /etc/nftables.conf
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority filter;
    }
    chain forward {
        type filter hook forward priority filter;
    }
    chain output {
        type filter hook output priority filter;
    }
}
```

[Прочитано 15 строк]
^G Справка ^O Записать ^F Поиск ^K Вырезать ^T Выполнить
^X Выход ^R ЧитФайл ^\ Замена ^U Вставить ^J Выровнять



Приводим файл к такому виду (делаем маскарадинг)

```
GNU nano 8.4                               /etc/nftables.conf *
#!/usr/sbin/nft -f

flush ruleset

table ip nat {
    chain postrouting {
        type nat hook postrouting priority 100; policy accept
        meta l4proto { gre, ipip, ospf } counter return
        masquerade
    }
}

table inet filter {
    chain input {
        type filter hook input priority filter;
    }
    chain forward {
        type filter hook forward priority filter;
    }
    chain output {
}

^G Справка      ^O Записать      ^F Поиск      ^K Вырезать      ^T Выполнить      ^C Пози
^X Выход      ^R ЧитФайл      ^\ Замена      ^U Вставить      ^J Выровнять      ^/ К ст
```

**ОБЯЗАТЕЛЬНО ПРОВЕРИТЬ ПРАВИЛЬНОСТЬ
НАПИСАНИЯ!!! ОДНА ОШИБКА И ТЫ ОШИБСЯ**

Перезагружаем службу сети (делать рекомендую **почаще** на

Всех устройствах, если какие-то проблемы)

```
root@isp:~# systemctl restart networking
```

Проверяем IP-адреса

```
root@isp:~# ip -br a
lo          UNKNOWN      127.0.0.1/8 brd 1/128
ens3         UP          10.0.137.96/24 brd fe80::b4e:4cc3:6d1e:csan/64
ens4         UP          172.16.1.1/28
ens5         UP          172.16.2.1/28 brd fe80::52fc:52ff:fe00:302/64
```

В случае, если какие-то IP-адреса пропадают — перезагружаем службы NetworkManager и networking по очереди:

```
root@isp:~# systemctl restart NetworkManager
```

```
root@isp:~# systemctl restart networking
```

На HQ-RTR:

```
root@hq-rtr:~# nano /etc/network/interfaces
```

```
GNU nano 8.4 /etc/network/interfaces
# This file describes the network interfaces
# and how to activate them. For more information,
# see /etc/network/interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet static
    address 172.16.1.2/28
    gateway 172.16.1.1
    post-up nft -f /etc/nftables.conf

^G Справка ^O Записать ^F Поиск ^
^X Выход ^R ЧитФайл ^\ Замена ^
```

- gateway 172.16.1.1 – указание шлюза (IP-адрес предыдущего устройства, к которому подключено устройство по сети. В нашем случае это ISP.)

Выходим с файла: Ctrl+X, y, Enter.

Перезагружаем службу сети

```
root@hq-rtr:~# systemctl restart networking
```

Проверяем IP-адреса

```
root@hq-rtr:~# ip -br a
lo          UNKNOWN      127.0.0.1/8 brd::1/128
ens3         UP          172.16.1.2/28
ens4         UP
ens5         UP
ens6         DOWN
```

Попробуем пингануть с ISP HQ-RTR

```
root@isp:~# ping 172.16.1.2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.
64 bytes from 172.16.1.2: icmp_seq=1 ttl=64 time=0.968 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=64 time=0.750 ms
64 bytes from 172.16.1.2: icmp_seq=3 ttl=64 time=0.698 ms
^C
--- 172.16.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.698/0.805/0.968/0.116 ms
```

А также в обратную сторону

```
root@hq-rtr:~# ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=0.815 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.613 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=0.885 ms
^C
--- 172.16.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2023ms
rtt min/avg/max/mdev = 0.613/0.771/0.885/0.115 ms
root@hq-rtr:~#
```

Проверим также и Интернет

```
root@hq-rtr:~# ping ya.ru
PING ya.ru (5.255.255.242) 56(84) bytes of data.
64 bytes from ya.ru (5.255.255.242): icmp_seq=1 ttl=53 time=59.4 ms
64 bytes from ya.ru (5.255.255.242): icmp_seq=2 ttl=53 time=58.7 ms
64 bytes from ya.ru (5.255.255.242): icmp_seq=3 ttl=53 time=58.6 ms
64 bytes from ya.ru (5.255.255.242): icmp_seq=4 ttl=53 time=58.6 ms
^C
--- ya.ru ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 58.597/58.833/59.377/0.317 ms
root@hq-rtr:~#
```

На BR-RTR:

```
root@br-rtr:~# nano /etc/network/interfaces
```

```
GNU nano 8.4 /etc/network/interfaces
# This file describes the network interfaces
# and how to activate them. For more information
# see /etc/network/interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet static
address 172.16.2.2/28
gateway 172.16.2.1

auto ens4
iface ens4 inet static
address 192.168.200.1/28

post-up nft -f /etc/nftables.conf

^G Справка ^O Записать ^F Поиск ^K
^X Выход ^R ЧитФайл ^\ Замена ^U
```

Перезагружаем службу сети

```
root@br-rtr:~# systemctl restart networking
```

Проверяем IP-адреса

```
root@br-rtr:~# ip -br a
lo          UNKNOWN    127.0.0.1/8 brd ::/128
ens3        UP         172.16.2.2/28 brd 0.0.0.0
ens4        UP         192.168.200.1/28 brd fe80::5293:deff:fe00:501/64
```

На HQ-SRV:

```
root@hq-srv:~# nano /etc/network/interfaces
```

```
GNU nano 8.4 /etc/net
# This file describes the network inter
# and how to activate them. For more in
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet static
address 192.168.100.2/27
gateway 192.168.100.1
```

**^G Справка ^O Записать ^F Поиск
^X Выход ^R ЧитФайл ^\ Замена**

Перезагружаем службу сети

```
root@hq-srv:~# systemctl restart networking
```

Проверяем IP-адреса

```
root@hq-srv:~# ip -br a
lo          UNKNOWN      127.0.0.1/8 brd 128
ens3        UP           192.168.100.2/27 brd fe80::521b:22ff:fe00:600/64
```

На HQ-CLI (временно, до 9 задания, позже он IP будет получать по DHCP):

```
root@hq-cli:~# nano /etc/network/interfaces
```

```
GNU nano 8.4 /etc/network/interfaces
# This file describes the network interfaces
# and how to activate them. For more information
# see /etc/network/interfaces(5).
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet static
address 192.168.100.34/28
gateway 192.168.100.33
```

```
^G Справка ^O Записать ^F Поиск
^X Выход ^R ЧитФайл ^\ Замена
```

Перезагружаем службу сети

```
root@hq-cli:~# systemctl restart networking
```

Проверяем IP-адреса

```
root@hq-cli:~# ip -br a
lo                  UNKNOWN      127.0.0.1/8 brd 127.0.0.1/128
ens3                UP          192.168.100.34/28 brd fe80::52d5:9bff:fe00:700/64
```

На BR-SRV:

```
root@br-srv:~# nano /etc/network/interfaces
```

```
GNU nano 8.4 /etc/network/interfaces
# This file describes the network interfaces
# and how to activate them. For more info
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet static
address 192.168.200.2/28
gateway 192.168.200.1
```

```
^G Справка ^O Записать ^F Поиск ^K
^X Выход ^R ЧитФайл ^\ Замена ^L
```

Перезагружаем службу сети

```
root@br-srv:~# systemctl restart networking
```

Проверяем IP-адреса

```
root@br-srv:~# ip -br a
lo          UNKNOWN      127.0.0.1/8 ::1/128
ens3        UP          192.168.200.2/28
root@br-srv:~#
```

Рекомендую повторно проверить везде IP-адреса. Если что-то отвалилось:

```
systemctl restart networking
```



3. Создайте локальные учетные записи на серверах HQ-SRV и BR-SRV:

- Создайте пользователя sshuser
- Пароль пользователя sshuser с паролем P@ssw0rd
- Идентификатор пользователя 2026
- Пользователь sshuser должен иметь возможность запускать sudo без ввода пароля
- Создайте пользователя net_admin на маршрутизаторах HQ-RTR и BR-RTR
- Пароль пользователя net_admin с паролем P@ssw0rd
- При настройке ОС на базе Linux, запускать sudo без ввода пароля
- При настройке ОС отличных от Linux пользователь должен обладать максимальными привилегиями.

ЕСЛИ СЛУЧАЙНО ДОПУСТИЛИ ОШИБКУ В СОЗДАНИИ ПОЛЬЗОВАТЕЛЯ, МОЖНО ЕГО УДАЛИТЬ С ПОМОЩЬЮ ЭТИХ КОМАНД:

rm -r /home/имя пользователя

userdel имя пользователя

После этого уже внимательно можно создать снова

Создаем пользователей sshuser на HQ-SRV и BR-SRV

```
root@hq-srv:~# useradd -m -s /bin/bash sshuser -u 2026 -U
```

```
root@br-srv:~# useradd -m -s /bin/bash sshuser -u 2026 -U
```

Даем привилегии sudo

```
root@hq-srv:~# usermod -aG sudo sshuser
```

```
root@br-srv:~# usermod -aG sudo sshuser
```

Ставим пароль P@\$Word на пользователя sshuser

```
root@hq-srv:~# passwd sshuser
Новый пароль:
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
```

Заходим в visudo

```
root@hq-srv:~# visudo
root@br-srv:~# visudo
```

И на HQ-SRV и на BR-SRV **ОБЯЗАТЕЛЬНО** в конце файла visudo добавляем строчку

```
sshuser ALL=(ALL:ALL) NOPASSWD:ALL
```

После слова sshuser нажимаем TAB, пишем ALL=(ALL:ALL), затем жмем пробел и пишем NOPASSWD:ALL

```
GNU nano 8.4                               /etc/sudoers.tmp
# User alias specification

# Cmnd alias specification

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

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

sshuser ALL=(ALL:ALL) NOPASSWD:ALL
# See sudoers(5) for more information on "@include"

@include /etc/sudoers.d

^G Справка      ^O Записать      ^F Поиск      ^K Вырезать
^X Выход       ^R ЧитФайл      ^\ Замена      ^U Вставить
```

Проверяем наших пользователей sshuser

```
root@hq-srv:~# su - sshuser
```

Обратим внимание, что при логине пароль не требуется

```
sshuser@hq-srv:~$
```

Повышаем права через sudo -i, видим что также все работает без пароля

```
sshuser@hq-srv:~$ sudo -i
sudo: не удаётся определить
решении имен
root@hq-srv:~#
```

Создаем пользователей net_admin на HQ-RTR и BR-RTR

```
root@hq-rtr:~# useradd -m -s /bin/bash net_admin -U  
root@br-rtr:~# useradd -m -s /bin/bash net_admin -U
```

Даем привилегии sudo

```
root@hq-rtr:~# usermod -aG sudo net_admin  
root@br-rtr:~# usermod -aG sudo net_admin
```

Ставим пароль P@ssw0rd на пользователя net_admin

```
root@hq-rtr:~# usermod -aG sudo net_admin  
root@hq-rtr:~# passwd net_admin  
Новый пароль:  
Повторите ввод нового пароля:  
passwd: пароль успешно обновлён
```

Заходим в visudo

```
root@hq-rtr:~# visudo  
root@br-rtr:~# visudo
```

И на HQ-RTR и на BR-RTR **ОБЯЗАТЕЛЬНО** в конце файла visudo добавляем строчку

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

```
GNU nano 8.4                               /etc/sudoer
# User alias specification

# Cmnd alias specification

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

# Allow members of group sudo to execute any
%sudo   ALL=(ALL:ALL) ALL

net_admin      ALL=(ALL:ALL) NOPASSWD:ALL
# See sudoers(5) for more information on "@includ
@includedir /etc/sudoers.d

^G Справка      ^O Записать      ^F Поиск      ^K Выр
^X Выход        ^R ЧитФайл      ^\ Замена      ^U Всё
```

Также все работает без пароля

```
root@br-rtr:~# su - net_admin
net_admin@br-rtr:~$ sudo -i
sudo: не удаётся определить адрес
служба
root@br-rtr:~#
```

(4)

4. Настройте коммутацию в сегменте HQ следующим образом:

- Трафик HQ-SRV должен принадлежать VLAN 100
- Трафик HQ-CLI должен принадлежать VLAN 200
- Предусмотреть возможность передачи трафика управления в VLAN 999
- Реализовать на HQ-RTR маршрутизацию трафика всех указанных VLAN с использованием одного сетевого адаптера ВМ/физического порта
- Сведения о настройке коммутации внесите в отчёт

На HQ-RTR установим OpenvSwitch:

- Если не скачивается, выдает Игн... Проверяем интернет.

```
root@hq-rtr:~# apt install openvswitch-switch

Установка:
  openvswitch-switch

Установка зависимостей:
  ieee-data      python3-markdown-it  python3-pyparsing
  libunbound8    python3-mdurl       python3-rich
  libxdp1        python3-netaddr     python3-sortedcontainers
  openvswitch-common  python3-netifaces  python3-uc-micro
  python3-click   python3-openvswitch  uuid-runtime
  python3-linkify-it  python3-pygments

Предлагаемые пакеты:
  ethtool          python3-graphviz    python-pyparsing-doc
  openvswitch-doc   python3-unbound    python-sortedcontainers-doc
  ipython3         python-pygments-doc
  python-netaddr-doc  ttf-bitstream-vera

Сводка:
  Обновление: 0, Установка: 18, Удаление: 0, Пропуск обновления: 0
  Объём загрузки: 9 460 kB
  Требуемое пространство: 52,1 MB / 19,4 GB доступно

Продолжить? [Д/Н] у
```

Создаем мост на виртуальном коммутаторе

```
root@hq-rtr:~# ovs-vsctl add-br hq-sw
```

Добавляем физические интерфейсы на виртуальный коммутатор с тегами

```
root@hq-rtr:~# ovs-vsctl add-port hq-sw ens4 tag=100
root@hq-rtr:~# ovs-vsctl add-port hq-sw ens5 tag=200
root@hq-rtr:~# ovs-vsctl add-port hq-sw ens6 tag=999
```

Добавляем VLAN-интерфейсы

```
root@hq-rtr:~# ovs-vsctl add-port hq-sw vlan100 tag=100 -- set interface vlan100 type=internal
root@hq-rtr:~# ovs-vsctl add-port hq-sw vlan200 tag=200 -- set interface vlan200 type=internal
root@hq-rtr:~# ovs-vsctl add-port hq-sw vlan999 tag=999 -- set interface vlan999 type=internal
```

Отредактируем файл /etc/network/interfaces. В нем нужно будет поднять VLAN-интерфейсы, назначить им IP-адреса, а также поднять мост

```
root@hq-rtr:~# nano /etc/network/interfaces
```

Модифицируем файл таким образом:

```
GNU nano 8.4          /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see
# the per-interface manual pages for details.

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet static
address 172.16.1.2/28
gateway 172.16.1.1

auto vlan100
iface vlan100 inet static
address 192.168.100.1/27

auto vlan200
iface vlan200 inet static
address 192.168.100.33/28

auto vlan999
iface vlan999 inet static
address 192.168.100.49/29

post-up nft -f /etc/nftables.conf
post-up ip link set hq-sw up

^K Справка ^O Записать ^F Поиск ^K Вырезать
^X Выход    ^R ЧитФайл  ^\ Замена   ^U Вставить
```

Перезагружаем сеть

```
root@hq-rtr:~# systemctl restart networking
```

Проверяем адресацию

```
root@hq-rtr:~# ip -br a
lo                  UNKNOWN      127.0.0.1/8 brd 127.0.0.1/128
ens3                UP          172.16.1.2/28 brd fe80::52a0:91ff:fe00:400/64
ens4                UP          fe80::52a0:91ff:fe00:402/64
ens5                UP          fe80::52a0:91ff:fe00:403/64
ens6                DOWN
ovs-system          DOWN
hq-sw               UNKNOWN      fe80::52a0:91ff:fe00:401/64
vlan100              UNKNOWN      192.168.100.1/27 brd fe80::943e:2aff:fe58:4c3/64
vlan200              UNKNOWN      192.168.100.33/28 brd fe80::587e:17ff:fe41:edb6/64
vlan999              UNKNOWN      192.168.100.49/29 brd fe80::3484:34ff:feb7:79d0/64
```

Теперь попробуем пингануть HQ-SRV и HQ-CLI с HQ-RTR

```
root@hq-rtr:~# 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=64 time=206 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=41.1 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=0.698 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=0.748 ms
^C
--- 192.168.100.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/mdev = 0.698/62.205/206.301/84.808 ms
root@hq-rtr:~# ping 192.168.100.34
PING 192.168.100.34 (192.168.100.34) 56(84) bytes of data.
64 bytes from 192.168.100.34: icmp_seq=1 ttl=64 time=1.76 ms
64 bytes from 192.168.100.34: icmp_seq=2 ttl=64 time=0.814 ms
64 bytes from 192.168.100.34: icmp_seq=3 ttl=64 time=0.759 ms
64 bytes from 192.168.100.34: icmp_seq=4 ttl=64 time=0.604 ms
^C
```

Также на HQ-SRV и на HQ-CLI теперь появился интернет

```
root@hq-srv:~# ping ya.ru
PING ya.ru (77.88.55.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=244 time=65.4 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=2 ttl=244 time=62.8 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=3 ttl=244 time=62.8 ms
^C
--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 62.774/63.675/65.416/1.230 ms
root@hq-srv:~#
```



5. Настройте безопасный удаленный доступ на серверах HQ-SRV и BR-SRV:

- Для подключения используйте порт 2026
- Разрешите подключения исключительно пользователю sshuser
- Ограничьте количество попыток входа до двух
- Настройте баннер «Authorized access only».

Устанавливаем SSH-сервер на HQ-SRV и BR-SRV

```
root@hq-srv:~# apt install openssh-server
```

```
root@br-srv:~# apt install openssh-server
```

Редактируем конфигурацию

```
root@hq-srv:~# nano /etc/ssh/sshd_config
```

```
GNU nano 8.4                               /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/t

# The strategy used for options in the default sshd_config sh
# OpenSSH is to specify options with their default value whe
# possible, but leave them commented.  Uncommented options ov
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key

^G Справка    ^O Записать   ^F Поиск      ^K Вырезать   ^T Выполн
^X Выход      ^R ЧитФайл    ^\ Замена     ^U Вставить   ^J Выровн
```

Раскомментируем строчку Port 22, и изменим порт на 2026

```
GNU nano 8.4                               /etc/ssh/sshd_config

# This is the sshd server system-wide configuration
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/u

# The strategy used for options in the default sshd
# OpenSSH is to specify options with their default
# possible, but leave them commented. Uncommented o
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2026■
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key

^G Справка    ^O Записать    ^F Поиск    ^K Вырезать
^X Выход    ^R ЧитФайл    ^\ Замена    ^U Вставить
```

Разрешим вход только пользователем sshuser

```
Port 2026
AllowUsers sshuser■
#AddressFamily any
#ListenAddress 0.0.0.0
```

Ограничиваем на две попытки входа

```
Port 2026
AllowUsers sshuser
MaxAuthTries 2■
#AddressFamily any
```

Зададим также баннер

```
Port 2026
AllowUsers sshuser
MaxAuthTries 2
Banner /etc/ssh_banner
#AddressFamily any
```

Выходим с файла

Создадим баннер по пути /etc/ssh_banner

```
root@hq-srv:~# nano /etc/ssh_banner
```

В баннере звездочками делаем рамку, и вписываем туда «Authorized access only»

The screenshot shows the terminal window for the nano editor. The title bar says "GNU nano 8.4" and the file path is "/etc/ssh_banner". The main area contains the following text:

```
*****  
*  
* Authorized access only *  
*  
*****
```

At the bottom of the screen, there is a menu bar with Russian labels and keyboard shortcuts:

- Справка (Ctrl+G)
- Выход (Ctrl+X)
- Записать (Ctrl+O)
- ЧитФайл (Ctrl+R)
- Поиск (Ctrl+F)
- Замена (Ctrl+V)
- Выре (Ctrl+K)
- Вста (Ctrl+U)

Тоже самое делаем и на BR-SRV.

Перезагружаем SSH

```
root@hq-srv:~# systemctl restart ssh
```

```
root@br-srv:~# systemctl restart ssh
```

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

```
root@hq-cli:~# ssh sshuser@192.168.100.2 -p 2026
```

Пишем «yes»

```
ED25519 key fingerprint is SHA256:W5BS8uz3Rtnsewkq5UneuAI1/EDz7Pzc3371NIJpv2U.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Баннер отображается корректно. Вводим пароль

```
Hosts:  
*****  
*          *  
* Authorized access only *  
*          *  
*****  
sshuser@192.168.100.2's password:
```

Как видим, все работает

```
sshuser@192.168.100.2's password:  
Linux hq-srv.au-team.irpo 6.12.43+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1  
.43-1 (2025-08-27) 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.  
sshuser@hq-srv:~$
```

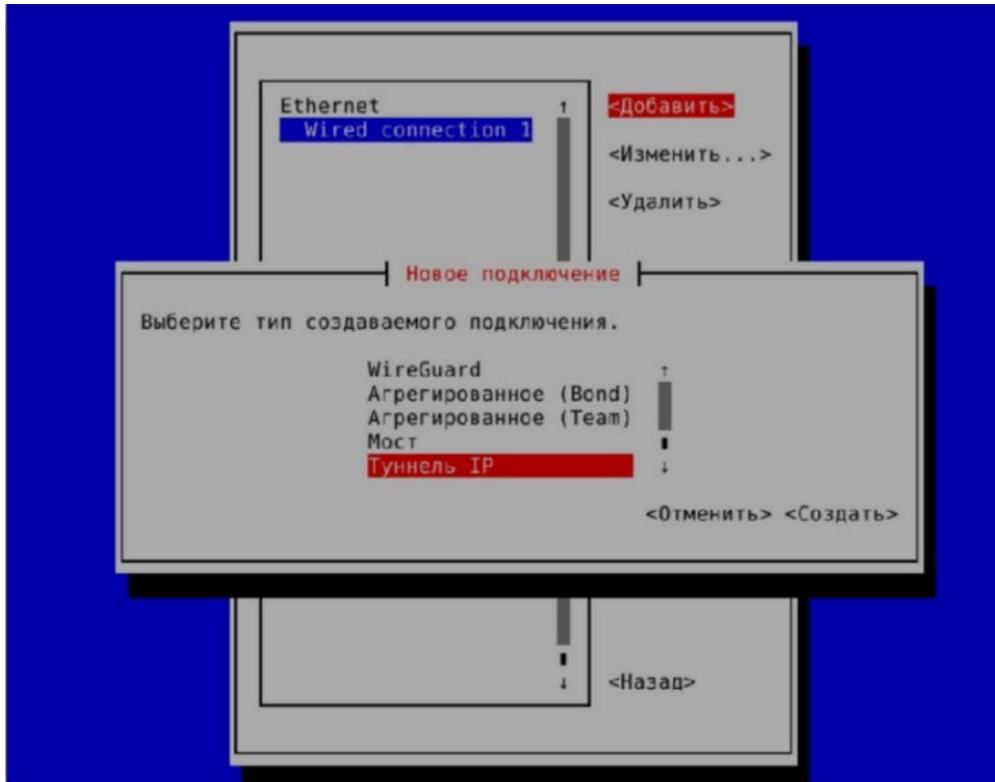


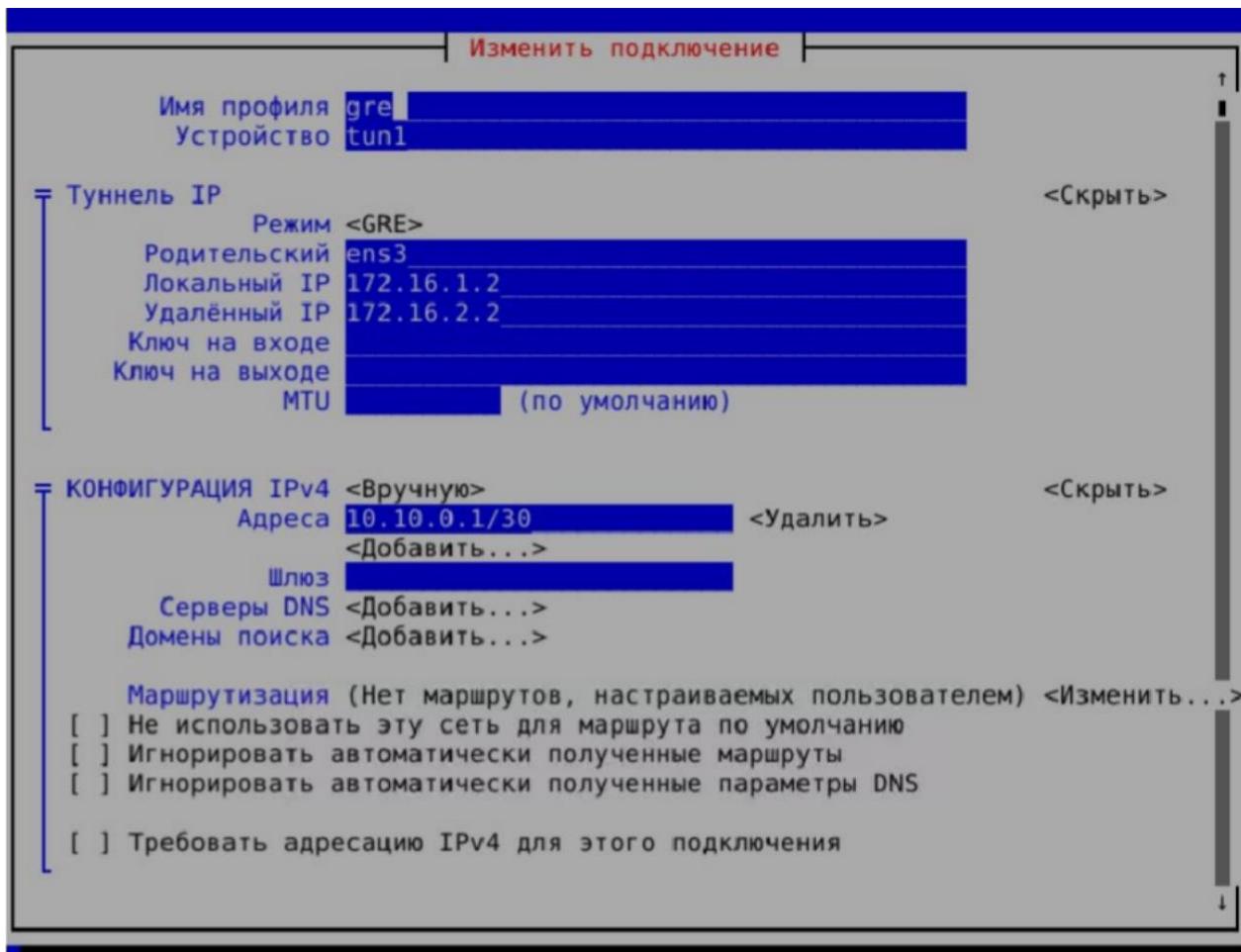
6. Между офисами HQ и BR, на маршрутизаторах HQ-RTR и BR-RTR необходимо сконфигурировать ip туннель:

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

Производим настройку на HQ-RTR.

- Выбираем «Редактировать подключения»
- Выбираем «Добавить»
- Выбираем «Туннель IP»
- Задаём понятные имена «Имя профиля» и «Устройство»
- «Режим» выбираем «GRE»
- «Родительский» указываем интерфейс в сторону ISP (ens3)
- Задаём «Локальный IP» (IP на интерфейсе HQ-RTR в сторону ISP 172.16.1.2)
- Задаём «Удаленный IP» (IP на интерфейсе BR-RTR в сторону ISP 172.16.2.2)
- Переходим к «КОНФИГУРАЦИЯ IPv4», переключаем на «Вручную»
- Задаём адрес IPv4 для туннеля (10.10.0.1/30)





Выходим

Заходим в файл /etc/network/interfaces

```
root@hq-rtr:~# nano /etc/network/interfaces
```

В самом конце файла добавляем строчку для поднятия интерфейса GRE

```
post-up ip link set gre0 up
```

Перезапускаем службу сети

```
root@hq-rtr:~# systemctl restart networking
```

Проверяем, что gre0 перешел в статус UNKNOWN и tun1 приобрел IP-адрес

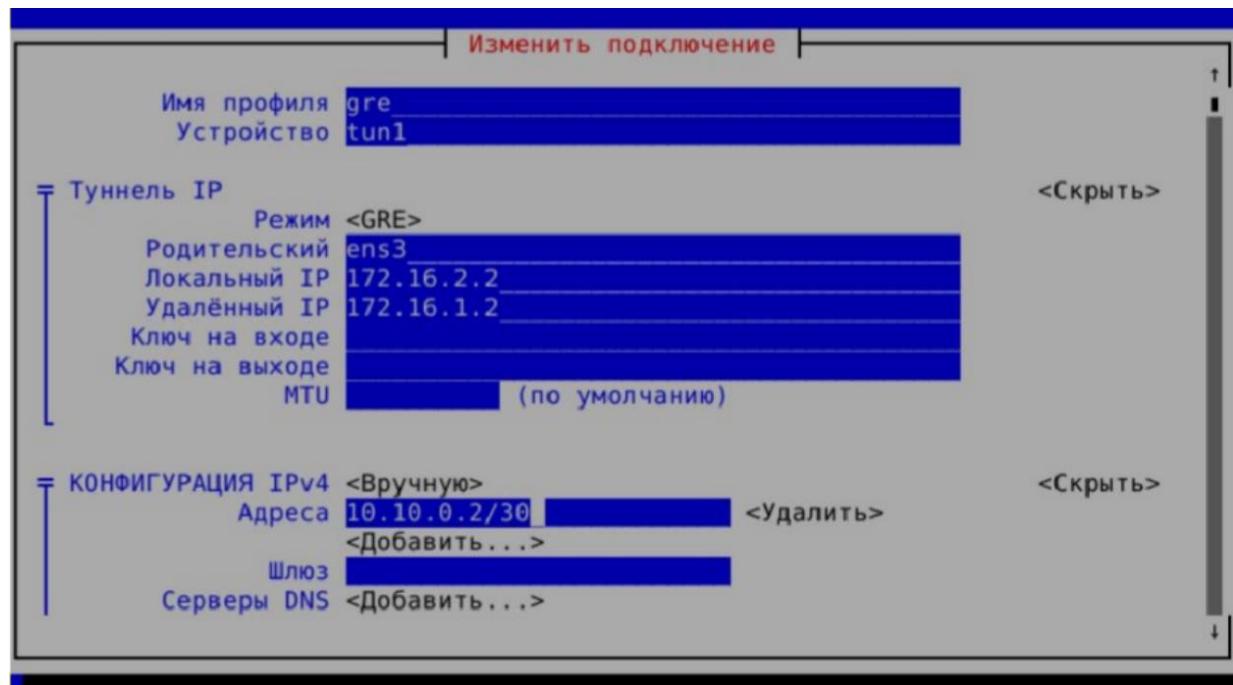
```
gre@NONE      UNKNOWN      fe80::1%ens3/64 fe80::1%ens3/64 fe80::1%ens3/64  
1/64 fe80::c0a8:64ff/64 fe80::ac10:102/64 fe80::7f00:1/64  
gretap@NONE   DOWN  
erspan@NONE   DOWN  
tun1@ens3     UNKNOWN      10.10.0.1/30 fe80::30f1:be14:51fa:39dc/64
```

Изменяем TTL интерфейса GRE на 64

```
root@hq-rtr:~# nmcli connection modify gre ip-tunnel.ttl 64
```

Производим настройку на BR-RTR.

- Выбираем «Редактировать подключения»
- Выбираем «Добавить»
- Выбираем «Туннель IP»
- Задаём понятные имена «Имя профиля» и «Устройство»
- «Режим» выбираем «GRE»
- «Родительский» указываем интерфейс в сторону ISP (ens3)
- Задаём «Локальный IP» (IP на интерфейсе BR-RTR в сторону ISP 172.16.2.2)
- Задаём «Удаленный IP» (IP на интерфейсе HQ-RTR в сторону ISP 172.16.1.2)
- Переходим к «КОНФИГУРАЦИЯ IPv4», переключаем на «Вручную»
- Задаём адрес IPv4 для туннеля (10.10.0.2/30)



Выходим

Заходим в файл /etc/network/interfaces

```
root@br-rtr:~# nano /etc/network/interfaces
```

В самом конце файла добавляем строчку для поднятия интерфейса GRE

```
post-up ip link set gre0 up
```

Перезапускаем службу сети

```
root@br-rtr:~# systemctl restart networking
```

Проверяем, что gre0 перешел в статус UNKNOWN и tun1 приобрел IP-адрес

gre0@NONE	UNKNOWN	fe80::964:2/64 fe80::c808:c88/64 fe80::ac18:284/64
/64 fe80::7f80:1/64		
gretap0@NONE	DOWN	
erspan0@NONE	DOWN	
tun1@ens3	UNKNOWN	10.10.0.2/30 fe80::9d5c:5fd4:c37f:b00/64

Изменяем TTL интерфейса GRE на 64

```
root@br-rtr:~# nmcli connection modify gre ip-tunnel.ttl 64
```

Если тут вылезает ошибка, проверьте внимательно nmtui, не должно стоять после gre пробела

Попробуем пингануть с BR-RTR HQ-RTR по IP-адресу 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=1.92 ms
64 bytes from 10.10.0.1: icmp_seq=2 ttl=64 time=1.29 ms
64 bytes from 10.10.0.1: icmp_seq=3 ttl=64 time=1.31 ms
64 bytes from 10.10.0.1: icmp_seq=4 ttl=64 time=1.26 ms
^C
--- 10.10.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.255/1.445/1.921/0.275 ms
root@br-rtr:~#
```

Попробуем пингануть с HQ-RTR BR-RTR по IP-адресу 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=3.84 ms
64 bytes from 10.10.0.2: icmp_seq=2 ttl=64 time=1.69 ms
64 bytes from 10.10.0.2: icmp_seq=3 ttl=64 time=1.28 ms
64 bytes from 10.10.0.2: icmp_seq=4 ttl=64 time=1.36 ms
^C
--- 10.10.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.284/2.044/3.840/1.047 ms
```

5

7. Обеспечьте динамическую маршрутизацию на маршрутизаторах HQ-RTR и BR-RTR: сети одного офиса должны быть доступны из другого офиса и наоборот. Для обеспечения динамической маршрутизации используйте link state протокол на усмотрение участника:

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

Устанавливаем FRR на HQ-RTR и BR-RTR

```
root@hq-rtr:~# apt install frr
```

```
root@br-rtr:~# apt install frr
```

Сначала настроим HQ-RTR

Зайдем в конфигурационный файл модулей FRR

```
root@hq-rtr:~# nano /etc/frr/daemons
```

Ищем строчку ospfd=no и меняем на ospfd=yes

```
GNU nano 8.4
# This file tells the frr package what daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activating a daemon for the first time, if the configuration
# file, has to be present *and* be readable by the user. If the
# configuration file is not present or is not readable by the user,
# the daemon will not be started by the init script. To change
# permissions, use "chmod u=rw,g=r,o=". If you want to run the
# daemon as root, use "u=root".
#
# When using "vtysh" such a configuration file must be present
# in the group "frrvty" and set to ug=rw,o=r.
#
# The watchfrr, zebra and staticd daemons do not require
# configuration files.
#
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
```

Перезапускаем FRR

```
root@hq-rtr:~# systemctl restart frr
```

Входим в эмуляцию интерфейса FRR (аналог Cisco)

```
root@hq-rtr:~# vtysh
```

Входим в режим конфигурации терминала

```
hq-rtr.au-team.irpo# conf t
```

Входим в режим конфигурации OSPF

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

Задаем ID для маршрутизатора (1.1.1.1)

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

```
hq-rtr.au-team.irpo(config-router)# no passive-interface default
```

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

```
hq-rtr.au-team.irpo(config-router)# network 192.168.100.0/27 area 0  
hq-rtr.au-team.irpo(config-router)# network 192.168.100.32/28 area 0  
hq-rtr.au-team.irpo(config-router)# network 10.10.0.0/30 area 0
```

Настройка аутентификации для области

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

Переходим к конфигурированию интерфейса tun1

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

Выводим интерфейс из пассивного режима

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

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

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

Выходим и записываем изменения

```
hq-rtr.au-team.irpo(config-if)# exit
hq-rtr.au-team.irpo(config)# exit
hq-rtr.au-team.irpo# wr
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
```

Настроим BR-RTR

Зайдем в конфигурационный файл модулей FRR

```
root@br-rtr:~# nano /etc/frr/daemons
```

Ищем строчку ospfd=no и меняем на ospfd=yes

```
GNU nano 8.4                               /etc/frr/daemons
# ATTENTION:
#
# When activating a daemon for the first time, a
# empty, has to be present *and* be owned by the
# the daemon will not be started by /etc/init.d/
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also
# group "frrvty" and set to ug=rw,o= though. Che
#
# The watchfrr, zebra and staticd daemons are al
#
bgpd=no
ospfd=yes■
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
pim6d=no
ldpd=no

^G Справка   ^O Записать   ^F Поиск   ^K Выреза
^X Выход    ^R ЧитФайл   ^\ Замена   ^U Встави
```

Перезапускаем FRR

```
root@br-rtr:~# systemctl restart frr
```

Входим в эмуляцию интерфейса FRR (аналог Cisco)

```
root@br-rtr:~# vtysh
```

Входим в режим конфигурации терминала

```
br-rtr.au-team.irpo# conf t
```

Входим в режим конфигурации OSPF

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

Задаем ID для маршрутизатора (2.2.2.2)

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

```
br-rtr.au-team.irpo(config-router)# no passive-interface default
```

Объявляем локальную сеть офиса BR и сеть GRE-туннеля

```
br-rtr.au-team.irpo(config-router)# network 192.168.200.0/28 area 0  
br-rtr.au-team.irpo(config-router)# network 10.10.0.0/30 area 0
```

Настройка аутентификации для области

```
br-rtr.au-team.irpo(config-router)# area 0 authentication
```

Переходим к конфигурированию интерфейса tun1

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

Выходим из пассивного режима

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

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

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

Выходим и записываем изменения

```
br-rtr.au-team.irpo(config-if)# exit  
br-rtr.au-team.irpo(config)# exit  
br-rtr.au-team.irpo# wr  
Note: this version of vtysh never writes vtysh.conf  
Building Configuration...  
Integrated configuration saved to /etc/frr/frr.conf  
[OK]
```

После этого перезагружаем HQ-RTR и BR-RTR

```
root@hq-rtr:~# reboot
```

```
root@br-rtr:~# reboot
```

Входим в эмуляцию интерфейса FRR

```
root@hq-rtr:~# vtysh
```

```
root@br-rtr:~# vtysh
```

Проверяем соседство маршрутизаторов

```
hq-rtr.au-team.irpo# show ip ospf neighbor  
  
Neighbor ID      Pri State          Up Time      Dead Time Address      In  
terface  
2.2.2.2          1 Full/-          3m02s       34.268s   10.10.0.2      tu  
n1:10.10.0.1
```

```
br-rtr.au-team.irpo# show ip ospf neighbor  
  
Neighbor ID      Pri State          Up Time      Dead Time Address      In  
terface  
1.1.1.1          1 Full/-          2m23s       33.965s   10.10.0.1      tu  
n1:10.10.0.2
```

Все работает, можно с HQ-SRV пингануть BR-SRV

**ЕСЛИ СЕРВЕРА НЕ ВИДЯТ ДРУГ ДРУГА, ТО
ПРОПИСЫВАЕМ НА HQ-RTR И BR-RTR systemctl restart frr**

```
root@hq-srv:~# ping 192.168.200.2  
PING 192.168.200.2 (192.168.200.2) 56(84) bytes of data.  
64 bytes from 192.168.200.2: icmp_seq=1 ttl=62 time=6.54 ms  
64 bytes from 192.168.200.2: icmp_seq=2 ttl=62 time=2.58 ms  
64 bytes from 192.168.200.2: icmp_seq=3 ttl=62 time=3.27 ms  
64 bytes from 192.168.200.2: icmp_seq=4 ttl=62 time=3.34 ms  
64 bytes from 192.168.200.2: icmp_seq=5 ttl=62 time=2.95 ms  
^C  
--- 192.168.200.2 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4008ms  
rtt min/avg/max/mdev = 2.579/3.735/6.542/1.428 ms
```

(4)

9. Настройте протокол динамической конфигурации хостов для сети в сторону HQ-CLI:

- Настройте нужную подсеть
- 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 – au-team.irpo
- Сведения о настройке протокола занесите в отчёт.

Установим DHCP-сервер на HQ-RTR

```
root@hq-rtr:~# apt install isc-dhcp-server
```

Зайдем в настройки интерфейсов DHCP

```
root@hq-rtr:~# nano /etc/default/isc-dhcp-server
```

Вписываем в INTERFACESv4 значение vlan200 (это HQ-CLI)

```
# On what interfaces should
#      Separate multiple i
INTERFACESv4="vlan200"
INTERFACESv6=""
```

Настроим сам DHCP

```
root@hq-rtr:~# nano /etc/dhcp/dhcpd.conf
```

```
GNU nano 8.4                               /etc/dhcp/dhcpd.conf
# dhcpd.conf
#
# Sample configuration file for ISC dhcpcd
#
# 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
# attempt to do a DNS update when a lease is confirmed. We default to
# 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
# network, the authoritative directive should be uncommented.
[ Прочитано 107 строк ]
^G Справка    ^O Записать   ^F Поиск      ^K Вырезать   ^T Выполнить ^C
^X Выход      ^R Читать файл ^\ Замена      ^U Вставить   ^] Выровнять ^/
```

Нужно изменить эти две строчки

```
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;
```

На

```
# option definitions common to all supported networks.
option domain-name "au-team.irpo";
option domain-name-servers 192.168.100.2;■
```

Перемещаемся к концу файла

```
GNU nano 8.4 /etc/dhcp/dhcpd.conf *
# match if substring (option vendor-class-identifier, 0, 4) = "S
#}

#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}

^G Справка ^O Записать ^F Поиск ^K Вырезать ^T Выполнить
^X Выход ^R ЧитФайл ^\ Замена ^U Вставить ^J Выровнять
```

Добавляем в конец настройку DHCP

```
#      deny members of "foo";
#      range 10.0.29.10 10.0.29.230;
#    }
#}

subnet 192.168.100.32 netmask 255.255.255.240 {
  range 192.168.100.34 192.168.100.47;
  option routers 192.168.100.33;
}
```

Тут 2 пробела перед range и option

- 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 192.168.100.32 с маской 255.255.255.240 (/28), выдавать диапазоны адресов от 192.168.100.34 до 192.168.100.47 от нашего шлюза VLAN200 (192.168.100.33).

Перезагружаем службу DHCP

```
root@hq-rtr:~# systemctl restart isc-dhcp-server
```

Теперь на HQ-CLI изменим файл /etc/network/interfaces

```
root@hq-cli:~# nano /etc/network/interfaces
```

Меняем настройку со статики

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see
# /usr/share/doc/networking-guide/html/introduction.html

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet static
address 192.168.100.34/28
gateway 192.168.100.33
```

На DHCP

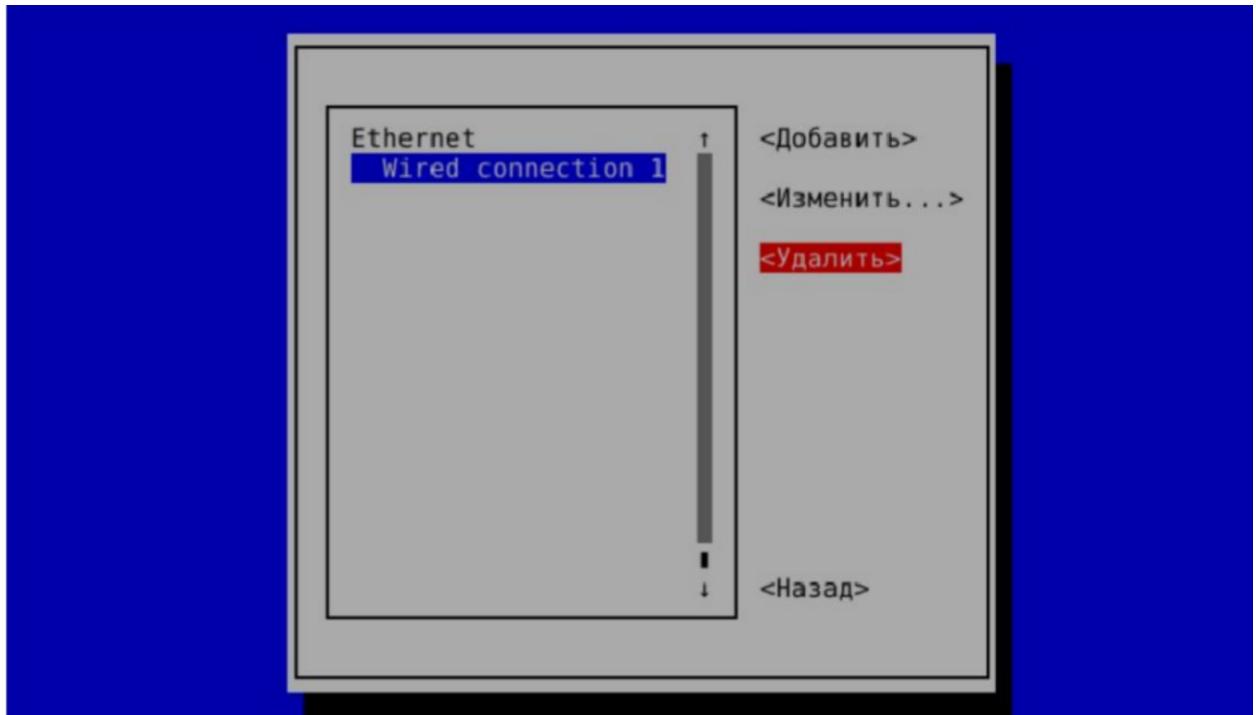
```
GNU nano 8.4                               /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see
# /usr/share/doc/networking-guide/html/introduction.html

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto ens3
iface ens3 inet dhcp
```

P.S. В nmtui рекомендую удалить Wired connection 1, иначе интерфейс получит два IP-адреса



```
root@hq-cli:~# ip -br a
lo          UNKNOWN      127.0.0.1/8 :/128
ens3        UP           192.168.100.34/28 192.168.100.35/28 fe80::e447:
            198.57.5.1/64
```

Перезапускаем службу сети

```
root@hq-cli:~# systemctl restart networking
```

Проверяем выдачу IP-адреса

```
root@hq-cli:~# ip -br a
lo          UNKNOWN      127.0.0.1/8 :/12
ens3        UP           192.168.100.34/28
```

Может выдаться и 192.168.100.35 (это если забыть удалить из nmtui подключение), но ничего страшного

```
root@hq-cli:~# ip -br a
lo          UNKNOWN      127.0.0.1/8 :/128
ens3        UP           192.168.100.35/28
```



10. Настройте инфраструктуру разрешения доменных имён 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 3
- В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер(77.88.8.7, 77.88.8.3 или другие)

P.S. здесь начинаются страдания, в BIND удалили подсказки, комментарии и стандартные файлы (на подобии db.local), поэтому придется очень хорошо развивать память, или гуглить содержимое файлов (или смириться)...

МОЖЕТ ВЫЛЕЗТИ ОШИБКА ПРИ СКАЧИВАНИИ bind9, ЕСЛИ ЭТО ПРОИЗОЙДЕТ, ПИШЕМ sudo apt-get update

Заходим на HQ-SRV, скачиваем DNS-сервер

```
root@hq-srv:~# apt install bind9
```

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

```
root@hq-srv:~# nano /etc/bind/named.conf.options
```

```
GNU nano 8.4          /etc/bind/named.conf.options *
options {
    directory "/var/cache/bind";
};

[ Прочитано 3 строки ]
^G Справка ^O Записать ^F Поиск ^K Вырезать ^T Выполнить ^C Позиция
^X Выход ^R ЧитФайл ^\ Замена ^U Вставить ^J Выровнять ^/ К строке
```

Приводим файл к такому виду

```
GNU nano 8.4                               /etc/bind/named.conf.options *
options {
    directory "/var/cache/bind";

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

    dnssec-validation no;

    listen-on-v6 port 53 { none; };
    listen-on port 53 { 127.0.0.1; 192.168.100.0/27; 192.168.100.32/28; 192.168.200.0/28; };
};
```



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

```
GNU nano 8.4                               /etc/bind/named.conf.local
// // Do any local configuration here
//
```

Приводим его к такому виду

```
GNU nano 8.4 /etc/bind/
// 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";
};■
```



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 auteam.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

```
root@hq-srv:~# named-checkconf
root@hq-srv:~#
```

Если вывод пустой, значит все ок. **Если**

нет, то проверьте правильность

написания.

Создаем папку с зонами

```
root@hq-srv:~# mkdir /etc/bind/zones
```

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

Одно но... Файла больше нет. Скачиваем через git.

```
root@hq-srv:~# apt install git
```

Клонируем репозиторий

```
root@hq-srv:~# git clone https://github.com/zalisfer/db-bind
```

Копируем db.local в /etc/bind/zones под название au-team.db

```
root@hq-srv:~# cp /root/db-bind/db.local /etc/bind/zones/au-team.db
```

Открываем в редакторе

```
root@hq-srv:~# nano /etc/bind/zones/au-team.db
```

Приводим файл к такому виду

```
GNU nano 8.4                               /etc/bind/zones/au-team.db *
```

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA    localhost. root.localhost. (
                      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
br-rtr  IN      A      192.168.200.1
hq-srv  IN      A      192.168.100.2
hq-cli   IN      A      192.168.100.35
br-srv   IN      A      192.168.200.2
moodle  CNAME   hq-rtr.au-team.irpo.
wiki    CNAME   hq-rtr.au-team.irpo.
```

Создадим зону обратного просмотра

```
root@hq-srv:~# cp /root/db-bind/db.127 /etc/bind/zones/au-team_rev.db
```

Отредактируем ее

```
root@hq-srv:~# nano /etc/bind/zones/au-team_rev.db
```

```
GNU nano 8.4                               /etc/bind/zones/au-team_rev.db
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA    localhost. root.localhost. (
                      1           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@       IN      NS     localhost.
1.0.0  IN      PTR    localhost.
```

Приводим к такому виду

```
GNU nano 8.4                               /etc/bind/zones/au-team_rev.db
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA    localhost. root.localhost. (
                      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.
66      IN      PTR    hq-cli.au-team.irpo.

^G Справка   ^O Записать   ^F Поиск   ^K Вырезать
^X Выход     ^R ЧитФайл   ^\ Замена   ^U Вставить
```

Назначаем владельца и права

```
root@hq-srv:~# chown -R root /etc/bind/zones
```

```
root@hq-srv:~# chown 0640 /etc/bind/zones/*
```

Также создаем папку master

```
root@hq-srv:~# mkdir /var/cache/bind/master
```

И копируем туда наши зоны

```
root@hq-srv:~# cp /etc/bind/zones/au-team.db /var/cache/bind/master  
root@hq-srv:~# cp /etc/bind/zones/au-team_rev.db /var/cache/bind/master
```

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

```
root@hq-srv:~# named-checkconf -z  
zone au-team.irpo/IN: loaded serial 2  
zone 100.168.192-in.addr.arpa/IN: loaded serial 1
```

Теперь в DNS-сервере HQ-SRV укажем 192.168.100.2.

```
root@hq-srv:~# nano /etc/resolv.conf
```

```
GNU nano 0.4  
# Generated by NetworkManager  
nameserver 192.168.100.2
```

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

```
root@br-srv:~# nano /etc/resolv.conf
```

```
GNU nano 8.4  
# Generated by NetworkManager  
nameserver 192.168.100.2  
  
/e
```

Перезапускаем BIND9 на HQ-SRV

```
root@hq-srv:~# systemctl restart bind9
```

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: icmp_seq=1 ttl=62 time=6.04 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=62 time=2.43 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=62 time=2.47 ms
^C
--- au-team.irpo ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.427/3.643/6.036/1.692 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 192.168.100.35
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
root@br-srv:~#
```

Также можно воспользоваться командой lookup или пингануть по доменному имени.



11. Настройте часовой пояс на всех устройствах (за исключением виртуального коммутатора, в случае его использования) согласно месту проведения экзамена

Проверяем часовой пояс.

```
root@isp:~# timedatectl
          Local time: Вс 2025-10-05 11:50:55 MSK
          Universal time: Вс 2025-10-05 08:50:55 UTC
                  RTC time: Вс 2025-10-05 08:50:55
                 Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
      NTP service: active
     RTC in local TZ: no
```

Список доступных часовых поясов можно посмотреть командой.

```
root@isp:~# ls /usr/share/zoneinfo/
Africa      Asia       Europe    iso3166.tab      Pacific    zone1970.tab
America     Atlantic   Factory   leapseconds      posixrules  zonenow.tab
Antarctica Australia  GMT       leap-seconds.list tzdata.zi   zone.tab
Arctic      Etc        Indian   localtime      UTC
root@isp:~#
```

Посмотреть список регионов и городов.

```
root@isp:~# ls /usr/share/zoneinfo/Asia
Aden        Brunei     Hovd      Kuching      Qatar      Thimphu
Almaty      Chita      Irkutsk   Kuwait      Qostanay   Tokyo
Amman      Chongqing  Istanbul  Macau       Qyzylorda Tomsk
Anadyr      Colombo    Jakarta   Magadan   Riyadh     Ulaanbaatar
Aqtau       Damascus   Jayapura  Makassar   Sakhalin   Urumqi
Aqtobe      Dhaka     Jerusalem Manila    Samarkand Ust-Nera
Ashgabat   Dili       Kabul     Muscat     Seoul     Vientiane
Atyrau      Dubai     Kamchatka Nicosia   Shanghai   Vladivostok
Baghdad     Dushanbe  Karachi   Novokuznetsk Singapore Yakutsk
Bahrain    Famagusta  Kashgar   Novosibirsk Srednekolymsk Yangon
Baku        Gaza       Kathmandu Omsk      Taipei     Yekaterinburg
Bangkok     Harbin    Khandyga Oral      Tashkent   Yerevan
Barnaul    Hebron    Kolkata   Phnom_Penh  Tbilisi
Beirut     Ho_Chi_Minh Krasnoyarsk Pontianak Tehran
Bishkek    Hong_Kong  Kuala_Lumpur Pyongyang Tel_Aviv
root@isp:~#
```

Выберем Красноярск.

```
root@isp:~# timedatectl set-timezone Asia/Krasnoyarsk
root@isp:~#
```

Изменение даты и времени при необходимости.

```
root@isp:~# timedatectl set-time "2025-05-10 15:53:00"
```

Проверяем изменения.

```
root@isp:~# timedatectl
          Local time: Вс 2025-10-05 15:52:52 +07
          Universal time: Вс 2025-10-05 08:52:52 UTC
                  RTC time: Вс 2025-10-05 08:52:52
                 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.