

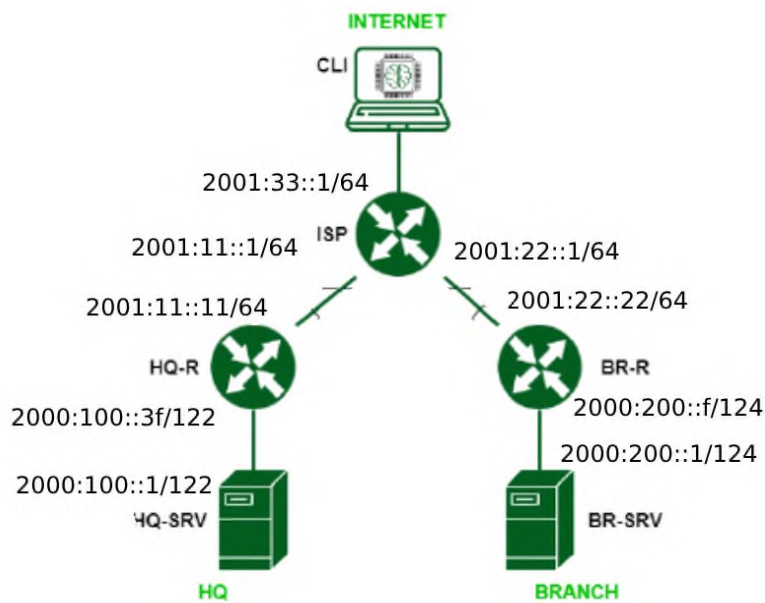
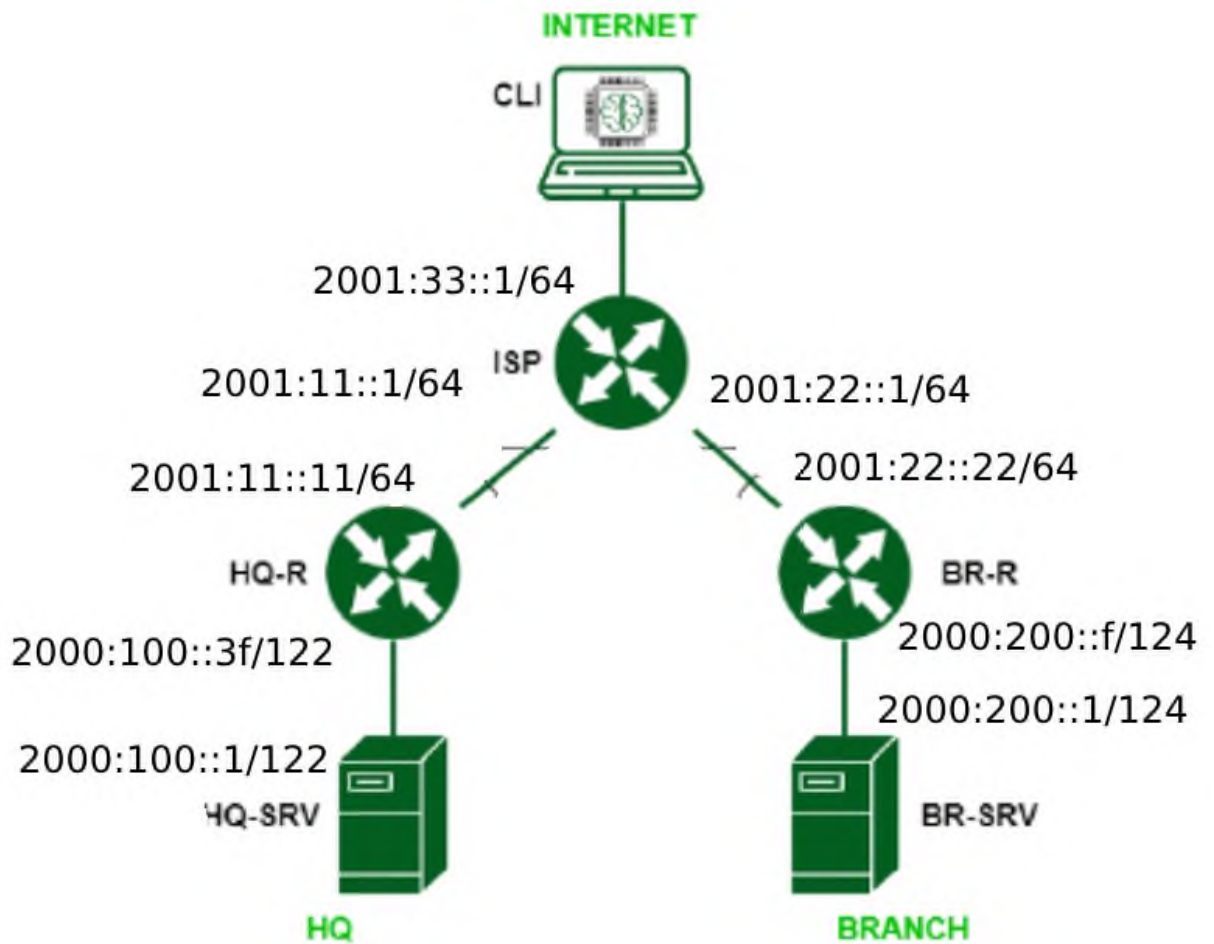
# ДЭ

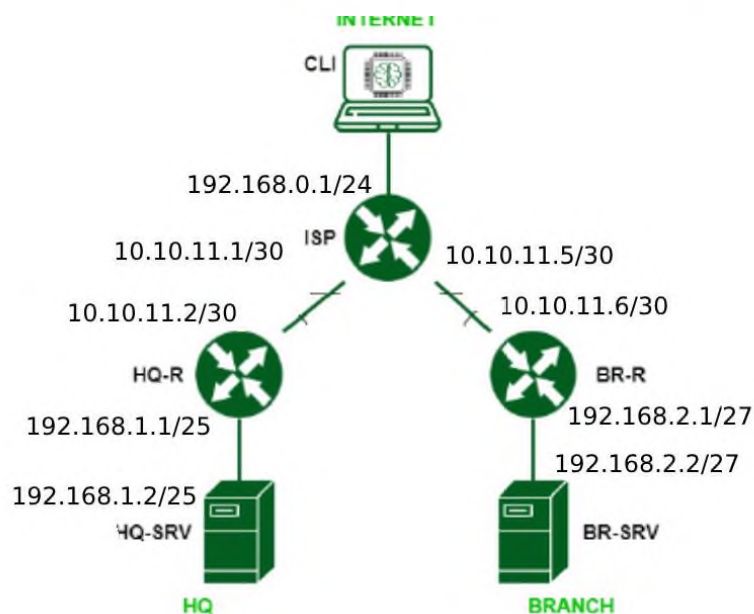
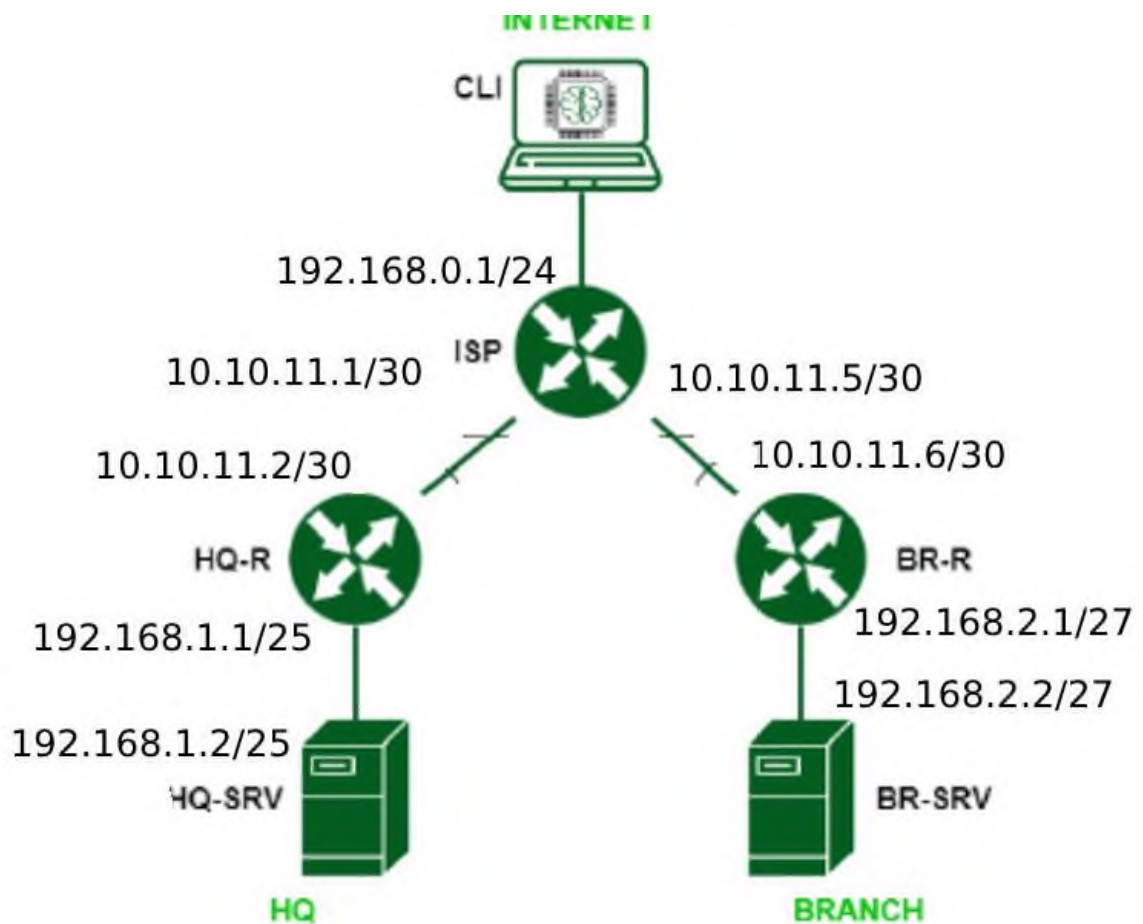
**Логин: adminer**

**пароль : qwerty2022!**

- [Логин: adminer](#)
- [пароль : qwerty2022!](#)
- [1 модуль 2 задание](#)
- [BR-R](#)
- [HQ-R](#)
- [ISP](#)
- [BR-SRV \(192.168.2.2\) и CLI \(192.168.0.2\)](#)
- [HQ-SRV не трогаем](#)
- [Не забудьте составить топологию сети L3. и заполнить таблицу адресов](#)
- [1 модуль 3 задание](#)
- [1 модуль 4 задание](#)
- [1 модуль 5 задание](#)
- [Модуль 1 задание 6](#)
- [Модуль 1 задание 7](#)
- [Модуль 1 задание 8](#)
- [Проверяем](#)

1 модуль 1 задание





## 1 модуль 2 задание

### BR-R

Команды для настройки

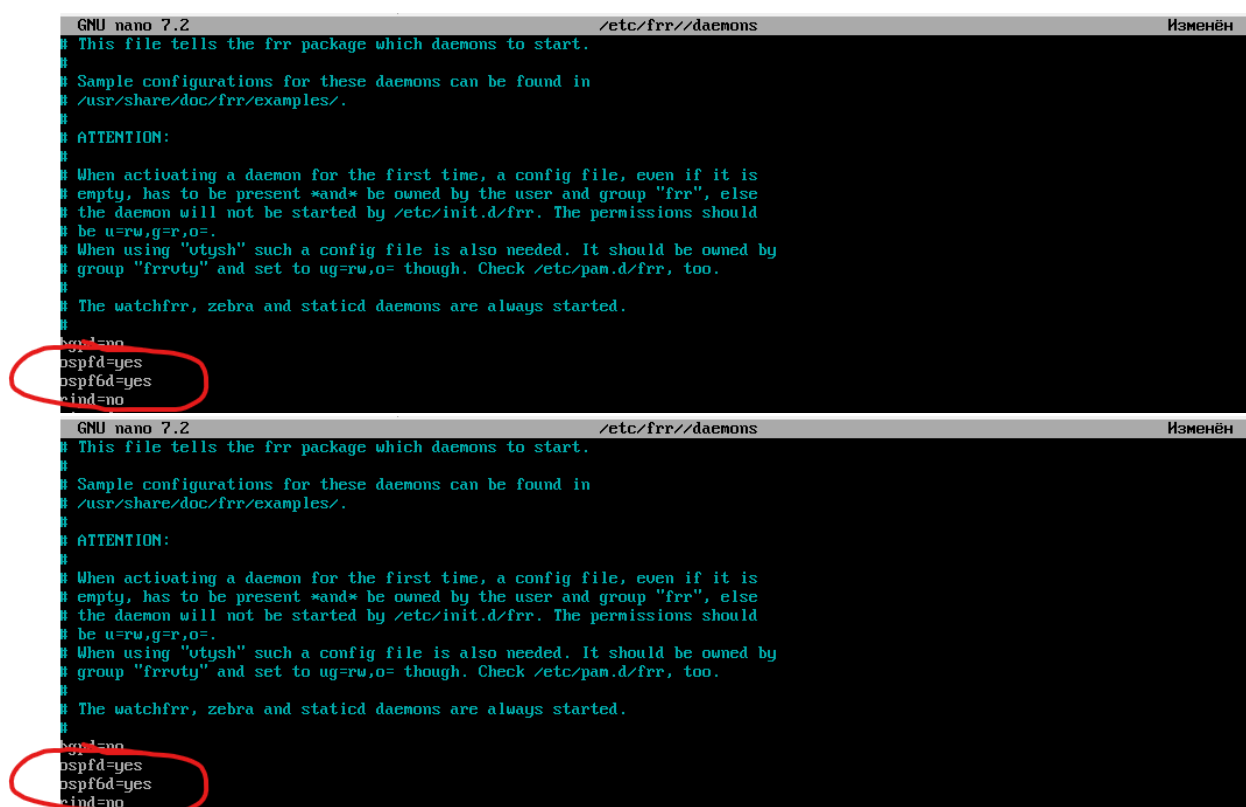
```
nano /etc/frr/daemons
ospfd=yes
```

```

ospf6d=yes
systemctl start frr.service
vtysh
conf t
ip forwarding
ipv6 forwarding
int eth0
ip address 10.10.11.6/30
no shutdown
int eth1
ip address 192.168.2.1/27
no shutdown
ex
router ospf
network 10.10.11.4/30 a 0
network 192.168.2.0/27 a 0
end
do wri
ex
systemctl restart frr.service

```

1) После входа в устройства пишем `su -` и переходим для редакции файла командой `nano /etc/frr/daemons` и меняем 2 параметра `ospfd` и `ospf6d`, с `no` на `yes` (рисунок 1). После изменения нажимаем `Ctrl + o > Enter > Ctrl + x`



2) Запускаем службу `systemctl start frr.service`. И заходим в службу для редакции апи адресов `vtysh`. После входа переходим в конфигурации `conf t`. Выключаем фигню командными `ip forwarding` и `ipv6 forwarding`.

```
[root@br-r ~]# vtysh
Hello, this is FRRouting (version 9.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

br-r# conf t
br-r(config)# ip forwarding
br-r(config)# ipv6 forwarding
br-r(config)#
```

### 3) Задаем апи командами

Я не знаю нужно ли настраивать ipv6. Я буду делать без. тг для инфы @swka32

```
int eth0
ip address 10.10.11.6/30
no shutdown
int eth1
ip address 192.168.2.1/27
no shutdown
ex
```

```
br-r(config)# int eth0
br-r(config-if)# ip address 10.10.11.6/30
br-r(config-if)# no shutdown
br-r(config-if)# int eth1
br-r(config-if)# ip address 192.168.2.1/27
br-r(config-if)# no shutdown
br-r(config-if)#
br-r(config)# int eth0
br-r(config-if)# ip address 10.10.11.6/30
br-r(config-if)# no shutdown
br-r(config-if)# int eth1
br-r(config-if)# ip address 192.168.2.1/27
br-r(config-if)# no shutdown
```

### 4) Настройка ОСПФ

```
router ospf
network 10.10.11.4/30 a 0
network 192.168.2.0/27 a 0
end
```

### 5) Сохранение и перезапуск фррр

```
do wri
ex
systemctl restart frr.service
```

```
br-r# do wri
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
br-r# ex
[root@br-r ~]# systemctl restaert frr
Unknown command verb restaert.
[root@br-r ~]# systemctl restart frr
[root@br-r ~]#

br-r# do wri
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
br-r# ex
[root@br-r ~]# systemctl restaert frr
Unknown command verb restaert.
[root@br-r ~]# systemctl restart frr
[root@br-r ~]#
```

## HQ-R

Аналогично BR-R настраиваем и HQ-R

```
nano /etc/frr/daemons
ospfd=yes
ospf6d=yes
systemctl start frr.service
vtysh
conf t
ip forwarding
ipv6 forwarding
int eth0
ip address 10.10.11.2/30
no shutdown
int eth1
ip address 192.168.1.1/25
no shutdown
ex
router ospf
network 10.10.11.0/30 a 0
network 192.168.1.0/25 a 0
do wri
end
ex
systemctl restart frr.service
```

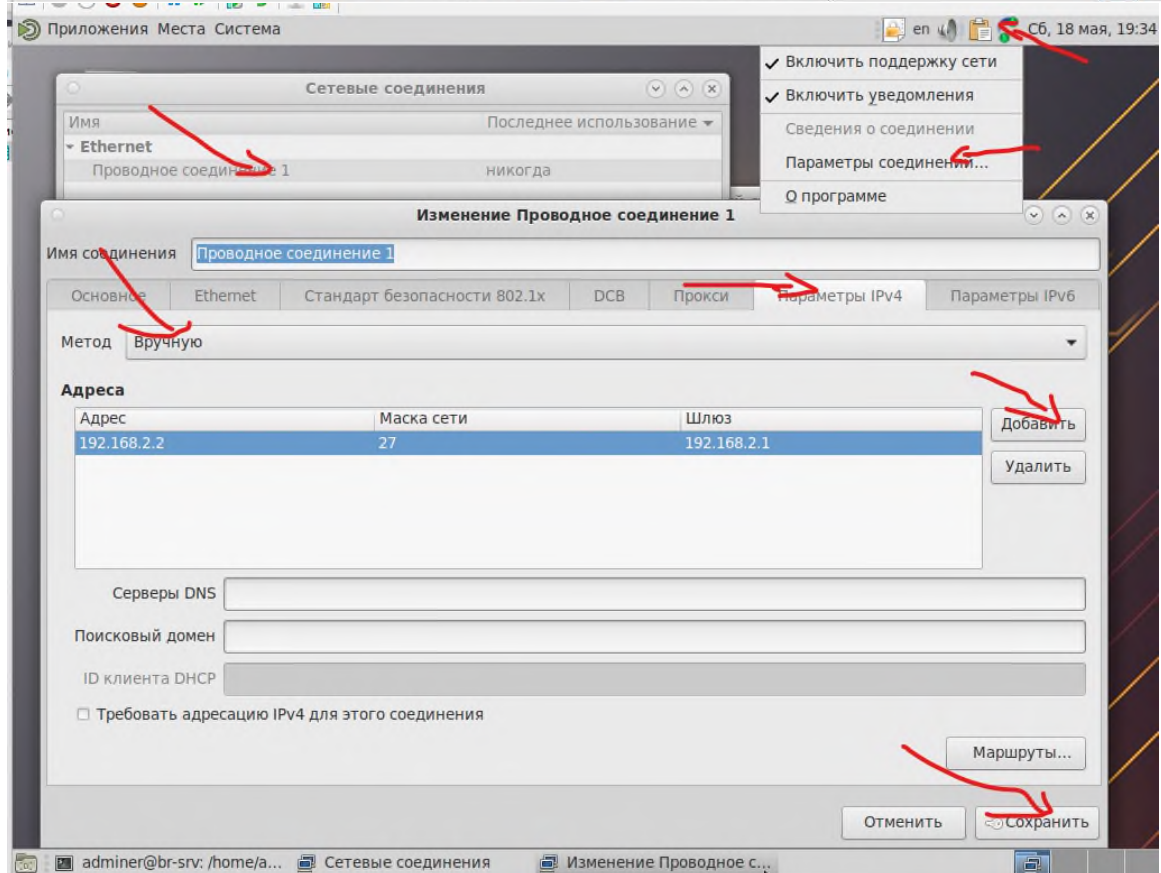
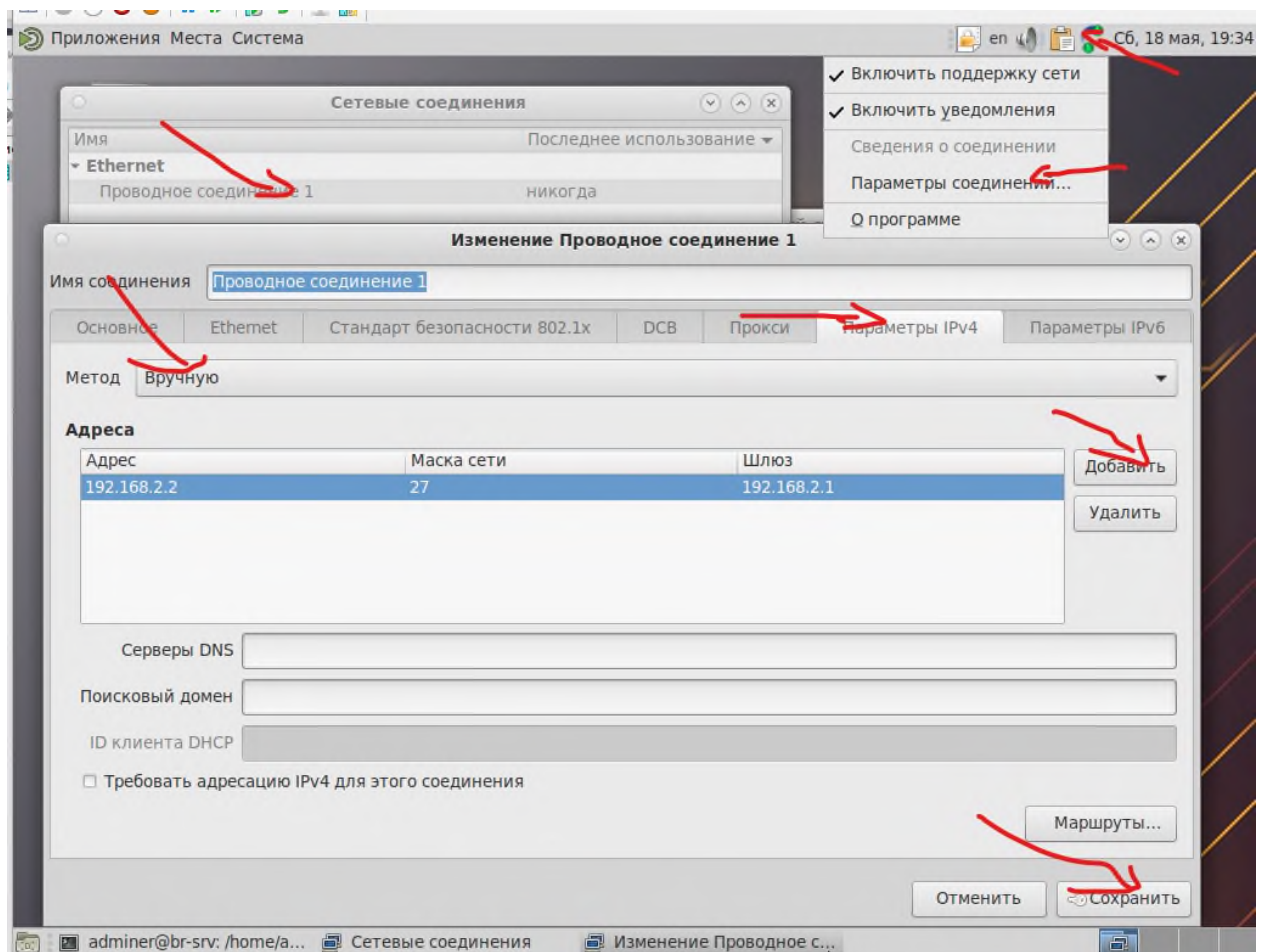
## ISP

Включаем форвардинг и поднимаем порты

```
vtysh
conf t
ip forwarding
ipv6 forwarding
```

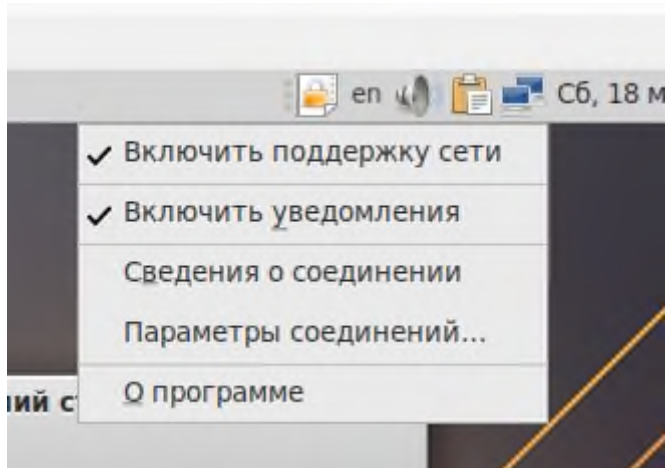
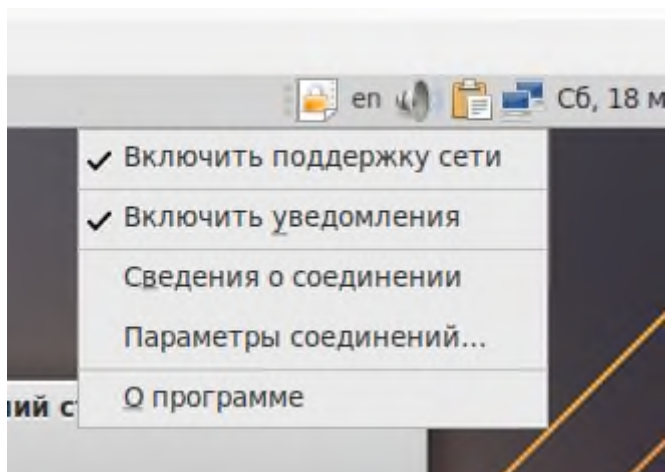
```
int eth0
no shutdown
int eth1
no shutdown
int eth1
no shutdown
do wri
end
ex
```

**BR-SRV (192.168.2.2) и CLI (192.168.0.2)**



После настройки нужно выключить и включить поддержку сети





CLI

## HQ-SRV не трогаем

После успешной настройки с br-srv должен пинговаться до hq-r 192.168.1.1

```

rtt min/avg/max/mdev = 1.143/1.739/1.988/0.346 ms
[adminer@br-srv Рабочий стол]$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=62 time=1.28 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=62 time=1.60 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=62 time=1.91 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=62 time=1.91 ms
^C
--- 192.168.1.1 ping statistics ---
rtt min/avg/max/mdev = 1.143/1.739/1.988/0.346 ms
[adminer@br-srv Рабочий стол]$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=62 time=1.28 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=62 time=1.60 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=62 time=1.91 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=62 time=1.91 ms
^C
--- 192.168.1.1 ping statistics ---

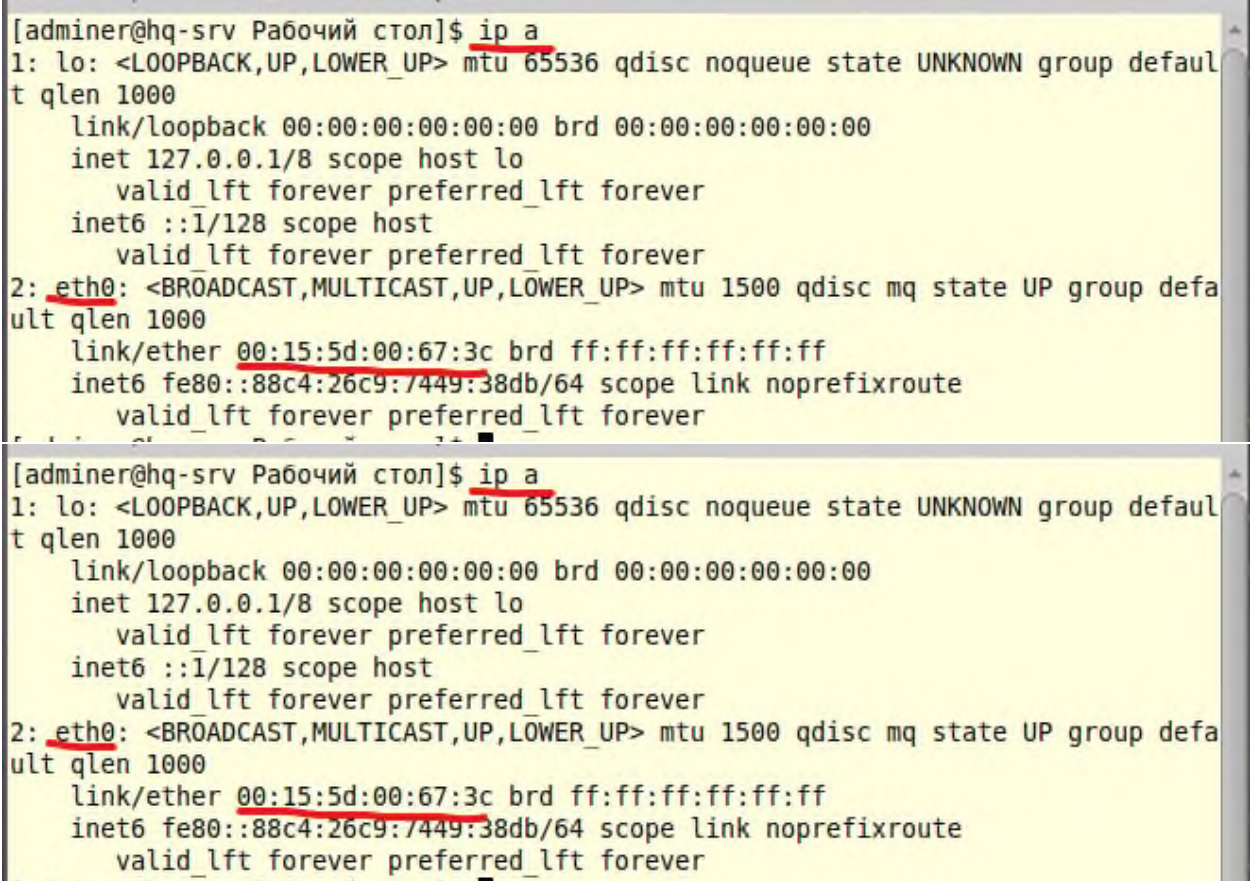
```

Не забудьте составить топологию сети L3. и заполнить таблицу адресов

# 1 модуль 3 задание

Переходим на HQ-R и копируем файл настройки DHCP

`cp /etc/dhcp/dhcpd.conf.sample /etc/dhcp/dhcpd.conf` . И редактируем его командой `nano /etc/dhcp/dhcpd.conf`. Так же перед редакцией посмотрим мак адрес интерфейса на hq-srv , для этого открываем терминал и вписываем `ip a` .



```
[adminer@hq-srv Рабочий стол]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:67:3c brd ff:ff:ff:ff:ff:ff
    inet6 fe80::88c4:26c9:7449:38db/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

[adminer@hq-srv Рабочий стол]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:67:3c brd ff:ff:ff:ff:ff:ff
    inet6 fe80::88c4:26c9:7449:38db/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

hardware ethernet 00:15:5d:00:67:3c; тут вы пишете свой адрес. И внимательно пишете конфиг

```
ddns-update-style none;
subnet 192.168.1.0 netmask 255.255.255.128 {
    option routers 192.168.1.1;
    option subnet-mask 255.255.255.128;
    range dynamic-bootp 192.168.1.2 192.168.1.5;
    default-lease-time 21600;
    max-lease-time 43200;
host hqsr {
    fixed-address 192.168.1.2;
    hardware ethernet 00:15:5d:00:67:3c;
}
```

```
GNU nano 7.2 /etc//dhcp/dhcpd
# See dhcpd.conf(5) for further configuration

ddns-update-style none;

subnet 192.168.1.0 netmask 255.255.255.128 {
    option routers                192.168.1.1;
    option subnet-mask            255.255.255.128;

#    option nis-domain            "domain.org";
#    option domain-name          "domain.org";
#    option domain-name-servers  192.168.1.1;

    range dynamic-bootp 192.168.1.2 192.168.1.5;
    default-lease-time 21600;
    max-lease-time 43200;
}
host hqsrv {
fixed-address 192.168.1.2;
hardware ethernet 00:15:5d:00:67:3c;
}

GNU nano 7.2 /etc//dhcp/dhcpd
# See dhcpd.conf(5) for further configuration

ddns-update-style none;

subnet 192.168.1.0 netmask 255.255.255.128 {
    option routers                192.168.1.1;
    option subnet-mask            255.255.255.128;

#    option nis-domain            "domain.org";
#    option domain-name          "domain.org";
#    option domain-name-servers  192.168.1.1;

    range dynamic-bootp 192.168.1.2 192.168.1.5;
    default-lease-time 21600;
    max-lease-time 43200;
}
host hqsrv {
fixed-address 192.168.1.2;
hardware ethernet 00:15:5d:00:67:3c;
}
```

Так же нужно указать порт для раздачи адресов. Переходим в файл командой `nano /etc/sysconfig/dhcpd` , указываем в параметре `DHCPDARGS=eth1`. После изменения нажимаем `Ctrl + o > Enter > Ctrl + x`

```
GNU nano 7.2 /etc/sysconfig/dhcpd
# The following variables are recognized:

DHCPDARGS=eth1

# Default value if chroot mode disabled.
#CHROOT="-j / -lf /var/lib/dhcp/dhcpd/state/dhcpd.leases"

GNU nano 7.2 /etc/sysconfig/dhcpd
# The following variables are recognized:

DHCPDARGS=eth1

# Default value if chroot mode disabled.
#CHROOT="-j / -lf /var/lib/dhcp/dhcpd/state/dhcpd.leases"
```

Вводим `chkconfig dhcpd on` для автоматического запуска. Запускаем сервис `systemctl start dhcpd`. Командой `systemctl status dhcpd` если сервис был настроен удачно то выглядит так, если красное то это смерть.

```
inet 192.168.1.125 brd 192.168.1.127 scope global eth1
    valid_lft forever preferred_lft forever
[root@hq-r ~]# systemctl status dhcpd
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2024-05-18 20:20:49 MSK; 10min ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
   Process: 3289 ExecStartPre=/etc/chroot.d/dhcpd.all (code=exited, status=0/SUCCESS)
  Main PID: 3369 (dhcpd)
    Tasks: 1 (limit: 1073)
   Memory: 7.2M
      CPU: 109ms
   CGroup: /system.slice/dhcpd.service
           └─ 3369 /usr/sbin/dhcpd -4 -f --no-pid eth1

inet 192.168.1.125 brd 192.168.1.127 scope global eth1
    valid_lft forever preferred_lft forever
[root@hq-r ~]# systemctl status dhcpd
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2024-05-18 20:20:49 MSK; 10min ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
   Process: 3289 ExecStartPre=/etc/chroot.d/dhcpd.all (code=exited, status=0/SUCCESS)
  Main PID: 3369 (dhcpd)
    Tasks: 1 (limit: 1073)
   Memory: 7.2M
      CPU: 109ms
   CGroup: /system.slice/dhcpd.service
           └─ 3369 /usr/sbin/dhcpd -4 -f --no-pid eth1
```

ЕСЛИ ГОРИТ КРАСНЫМ ТО ДЕЛАЙТЕ ЭТИ ПУНКТЫ

- Проверяем конфиг `dhcpr` командой `dhcpr -t`. Если ошибка в конфиге то он укажет строчку где была ошибка. если дела не в конфиге будет так

```

bash: dhcp: команда не найдена
[root@hq-r ~]# dhcpd -t
Internet Systems Consortium DHCP Server 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd.conf
Database file: /state/dhcpd.leases
PID file: /var/run/dhcpd.pid
[root@hq-r ~]#

```

## УДАЧНАЯ ПРОВЕРКА

- Перезапускаем службы. `systemctl restart firewalld systemctl restart NetworkManager`. И снова перезапускаем `dhcpd`.
- Если не помогла попробуйте погуглить до `ip` если не получилось то смотрим интерфейс `ip -a` если нету апи то пробуйте откатиться до снимка и настроить снова устройства

```

[root@hq-r ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:67:3a brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.2/30 brd 10.10.11.3 scope global eth0
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:67:3b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/25 brd 192.168.1.127 scope global eth1
        valid_lft forever preferred_lft forever

```

Так должен выглядеть `hq-r`

## 1 модуль 4 задание

Добавляем пользователей

```

adduser логин
usermod -aG wheel логин
passwd логин
CLI логин - пароль
    admin -P@ssw0rd

```

```
HQ-SRV
admin - P@ssw0rd

HQ-R
admin - P@ssw0rd
network_admin - P@ssw0rd

BR-SRV
branch_admin - P@ssw0rd
network_admin - P@ssw0rd

BR-R
network_admin - P@ssw0rd
branch_admin - P@ssw0rd
```

## 1 модуль 5 задание

ISP как сервер:

если надо открыть портиables -A INPUT -p tcp --dport 5201 -j ACCEPT

```
iperf3 -s
```

HQ-R:

```
iperf3 -c 10.10.11.1 -f M
```

```
[root@isp ~]# iperf3 -s
Server listening on 5201 (test #1)
Accepted connection from 10.10.11.2, port 44808
[ 51] local 10.10.11.1 port 5201 connected to 10.10.11.2 port 44808
[ ID] Interval      Transfer      Bitrate
[ 51] 0.00-1.00 sec  1.11 GBytes  9.49 Gbits/sec
[ 51] 1.00-2.00 sec  1.13 GBytes  9.69 Gbits/sec
[ 51] 2.00-3.00 sec  1.13 GBytes  9.73 Gbits/sec
[ 51] 3.00-4.00 sec  1.15 GBytes  9.88 Gbits/sec
[ 51] 4.00-5.00 sec  1.07 GBytes  9.22 Gbits/sec
[ 51] 5.00-6.00 sec  1.14 GBytes  9.80 Gbits/sec
[ 51] 6.00-7.00 sec  1.13 GBytes  9.69 Gbits/sec
[ 51] 7.00-8.00 sec  1.21 GBytes  10.4 Gbits/sec
[ 51] 8.00-9.00 sec  1.13 GBytes  9.71 Gbits/sec
[ 51] 9.00-10.00 sec 1.14 GBytes  9.76 Gbits/sec
[ 51] 10.00-10.00 sec 1.38 MBytes  8.80 Gbits/sec
[ ID] Interval      Transfer      Bitrate
[ 51] 0.00-10.00 sec 11.3 GBytes  9.73 Gbits/sec
Server listening on 5201 (test #2)
```

```
[root@hq-r ~]# iperf3 -c 10.10.11.1 -f M
Connecting to host 10.10.11.1, port 5201
[ 51] local 10.10.11.2 port 44820 connected to 10.10.11.1 port 5201
[ ID] Interval      Transfer      Bitrate      Retr      Cwnd
[ 51] 0.00-1.00 sec  1.11 GBytes  1135 MBytes/sec  0      3.12 MBytes
[ 51] 1.00-2.00 sec  1.13 GBytes  1154 MBytes/sec  0      3.12 MBytes
[ 51] 2.00-3.00 sec  1.13 GBytes  1162 MBytes/sec  0      3.12 MBytes
[ 51] 3.00-4.00 sec  1.15 GBytes  1177 MBytes/sec  0      3.12 MBytes
[ 51] 4.00-5.00 sec  1.07 GBytes  1099 MBytes/sec  0      3.12 MBytes
[ 51] 5.00-6.00 sec  1.14 GBytes  1169 MBytes/sec  0      3.12 MBytes
[ 51] 6.00-7.00 sec  1.13 GBytes  1155 MBytes/sec  0      3.12 MBytes
[ 51] 7.00-8.00 sec  1.21 GBytes  1235 MBytes/sec  0      3.12 MBytes
[ 51] 8.00-9.00 sec  1.13 GBytes  1157 MBytes/sec  0      3.12 MBytes
[ 51] 9.00-10.00 sec  1.14 GBytes  1163 MBytes/sec  0      3.12 MBytes
[ ID] Interval      Transfer      Bitrate      Retr      Cwnd
[ 51] 0.00-10.00 sec 11.3 GBytes  1161 MBytes/sec  0      sender
[ 51] 0.00-10.00 sec 11.3 GBytes  1160 MBytes/sec  0      receiver
iperf Done.
[root@hq-r ~]#
```

ШО это значит я не знаю

## Модуль 1 задание 6



Создадим директорию для хранения скрипта резервного копирования backup-script и директорию для хранения архивов резервных копий backup

```
# mkdir /var/{backup,backup-script}
```

Создадим файл скрипта

```
# nano /var/backup-script/backup.sh
```

Пример скрипта резервного копирования:

```
#!/bin/bash

data=$(date +%d.%m.%Y-%H:%M:%S)
mkdir /var/backup/$data
cp -r /etc/frr /var/backup/$data
cp -r /etc/netables /var/backup/$data
cp -r /etc/NetworkManager/system-connections /var/backup/$data
cp -r /etc/dhcp /var/backup/$data
cd /var/backup
tar czfu "$data.tar.gz" $data
rm -r /var/backup/$data
```

```
#!/bin/bash

data=$(date +%d.%m.%Y-%H:%M:%S)
mkdir /var/backup/$data
cp -r /etc/frr /var/backup/$data
cp -r /etc/netables /var/backup/$data
cp -r /etc/NetworkManager/system-connections /var/backup/$data
cp -r /etc/dhcp /var/backup/$data
cd /var/backup
tar czfu "$data.tar.gz" $data
rm -r /var/backup/$data
```

Задаем права скрипту на выполнение:

```
# chmod +x /var/backup-script/backup.sh
```

Запускаем скрипт

```
# /var/backup-script/backup.sh
```

```

[root@hq-r ~]# chmod +x /var/backup-script/backup.sh
[root@hq-r ~]# /var/backup-script/backup.sh
./07.04.2024-16:28:34/
./07.04.2024-16:28:34/system-connections/
./07.04.2024-16:28:34/system-connections/Проводное подключение 2.nmconnection
./07.04.2024-16:28:34/system-connections/ens18.nmconnection
./07.04.2024-16:28:34/system-connections/Проводное подключение 1.nmconnection
./07.04.2024-16:28:34/system-connections/tun1.nmconnection
./07.04.2024-16:28:34/nftables/
./07.04.2024-16:28:34/nftables/nat.nft
./07.04.2024-16:28:34/nftables/router.nft
./07.04.2024-16:28:34/nftables/main.nft
./07.04.2024-16:28:34/nftables/hq-r.nft
./07.04.2024-16:28:34/nftables/osf/
./07.04.2024-16:28:34/nftables/osf/pf.os
./07.04.2024-16:28:34/dhcp/
./07.04.2024-16:28:34/dhcp/dhcpd6.conf.save
./07.04.2024-16:28:34/dhcp/dhclient.d/
./07.04.2024-16:28:34/dhcp/dhclient.d/ntp.sh
./07.04.2024-16:28:34/dhcp/dhclient.d/chrony.sh
./07.04.2024-16:28:34/dhcp/dhcpd6.conf.save.1
./07.04.2024-16:28:34/dhcp/dhcpd.conf
./07.04.2024-16:28:34/dhcp/dhcpd6.conf
./07.04.2024-16:28:34/dhcp/dhcpd6.conf.bak
./07.04.2024-16:28:34/frr/
./07.04.2024-16:28:34/frr/frr.conf
./07.04.2024-16:28:34/frr/frr.conf.sav
./07.04.2024-16:28:34/frr/daemons
./07.04.2024-16:28:34/frr/uttysh.conf
[root@hq-r ~]# _

```

```

[root@hq-r ~]# chmod +x /var/backup-script/backup.sh
[root@hq-r ~]# /var/backup-script/backup.sh
./07.04.2024-16:28:34/
./07.04.2024-16:28:34/system-connections/
./07.04.2024-16:28:34/system-connections/Проводное подключение 2.nmconnection
./07.04.2024-16:28:34/system-connections/ens18.nmconnection
./07.04.2024-16:28:34/system-connections/Проводное подключение 1.nmconnection
./07.04.2024-16:28:34/system-connections/tun1.nmconnection
./07.04.2024-16:28:34/nftables/
./07.04.2024-16:28:34/nftables/nat.nft
./07.04.2024-16:28:34/nftables/router.nft
./07.04.2024-16:28:34/nftables/main.nft
./07.04.2024-16:28:34/nftables/hq-r.nft
./07.04.2024-16:28:34/nftables/osf/
./07.04.2024-16:28:34/nftables/osf/pf.os
./07.04.2024-16:28:34/dhcp/
./07.04.2024-16:28:34/dhcp/dhcpd6.conf.save
./07.04.2024-16:28:34/dhcp/dhclient.d/
./07.04.2024-16:28:34/dhcp/dhclient.d/ntp.sh
./07.04.2024-16:28:34/dhcp/dhclient.d/chrony.sh
./07.04.2024-16:28:34/dhcp/dhcpd6.conf.save.1
./07.04.2024-16:28:34/dhcp/dhcpd.conf
./07.04.2024-16:28:34/dhcp/dhcpd6.conf
./07.04.2024-16:28:34/dhcp/dhcpd6.conf.bak
./07.04.2024-16:28:34/frr/
./07.04.2024-16:28:34/frr/frr.conf
./07.04.2024-16:28:34/frr/frr.conf.sav
./07.04.2024-16:28:34/frr/daemons
./07.04.2024-16:28:34/frr/uttysh.conf
[root@hq-r ~]# _

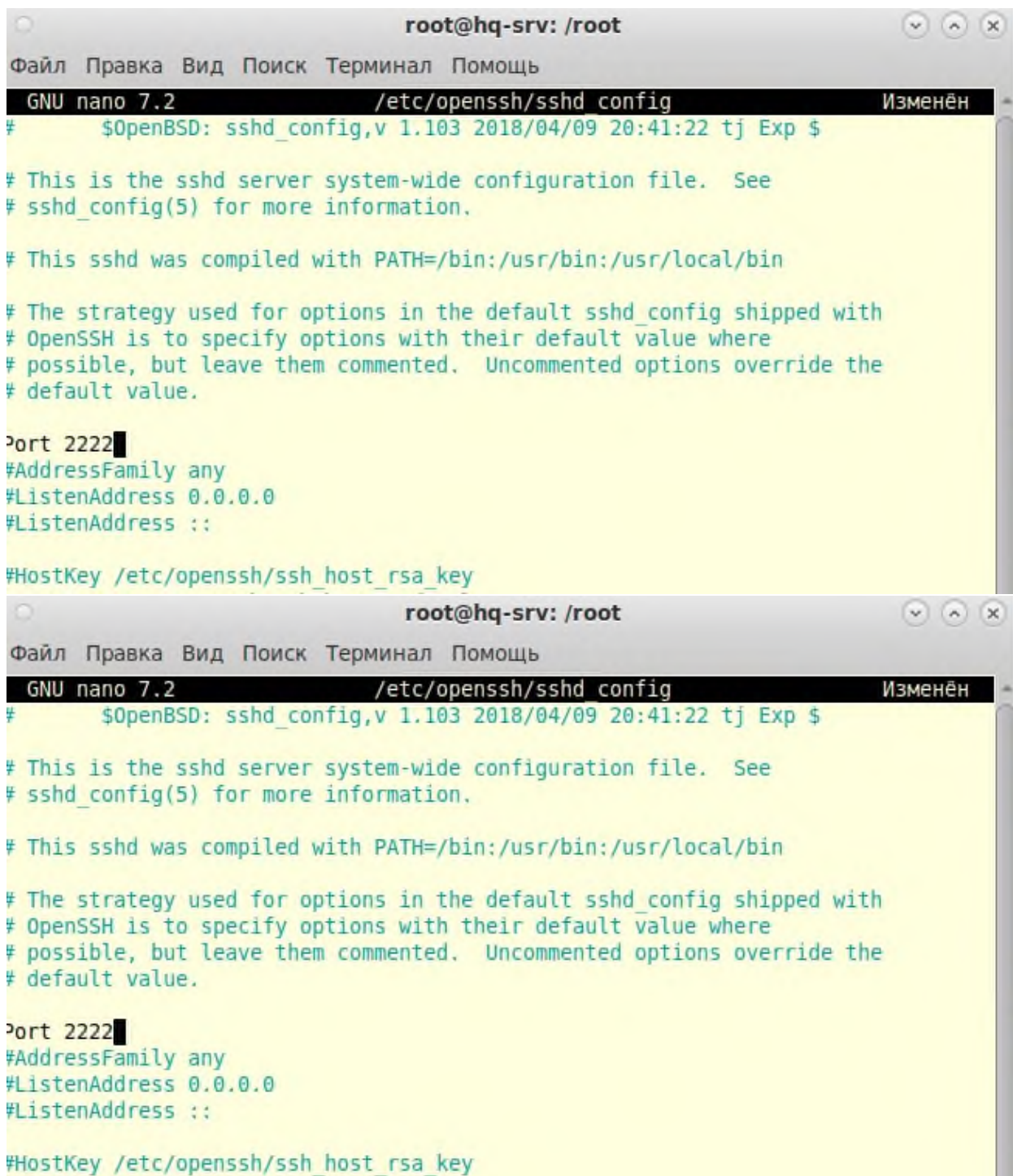
```

## Модуль 1 задание 7

HQ-SRV

nano /etc/openssh/sshd\_config





```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/openssh/sshd config Изменён
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

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

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

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

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/openssh/ssh_host_rsa_key
```

systemctl restart sshd

Тестируем подключение. С HQ-R подключаемся к HQ-SRV на порту 2222

```
[root@hq-r ~]# ssh admin@192.168.1.2 -p 2222
The authenticity of host '[192.168.1.2]:2222 ([192.168.1.2]:2222)' can't be established.
ED25519 key fingerprint is SHA256:zba/tpBkEaLiHuwB18tfaCOC6mobYVGxCK0S29zmKBw.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '[192.168.1.2]:2222' (ED25519) to the list of known hosts.
admin@192.168.1.2's password:
ssh: Permission denied, please try again.
admin@192.168.1.2's password:
[admin@hq-srv ~]#

[root@hq-r ~]# ssh admin@192.168.1.2 -p 2222
The authenticity of host '[192.168.1.2]:2222 ([192.168.1.2]:2222)' can't be established.
ED25519 key fingerprint is SHA256:zba/tpBkEaLiHuwB18tfaCOC6mobYVGxCK0S29zmKBw.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '[192.168.1.2]:2222' (ED25519) to the list of known hosts.
admin@192.168.1.2's password:
ssh: Permission denied, please try again.
admin@192.168.1.2's password:
[admin@hq-srv ~]#
```

перенаправление трафика . написать на hq-r

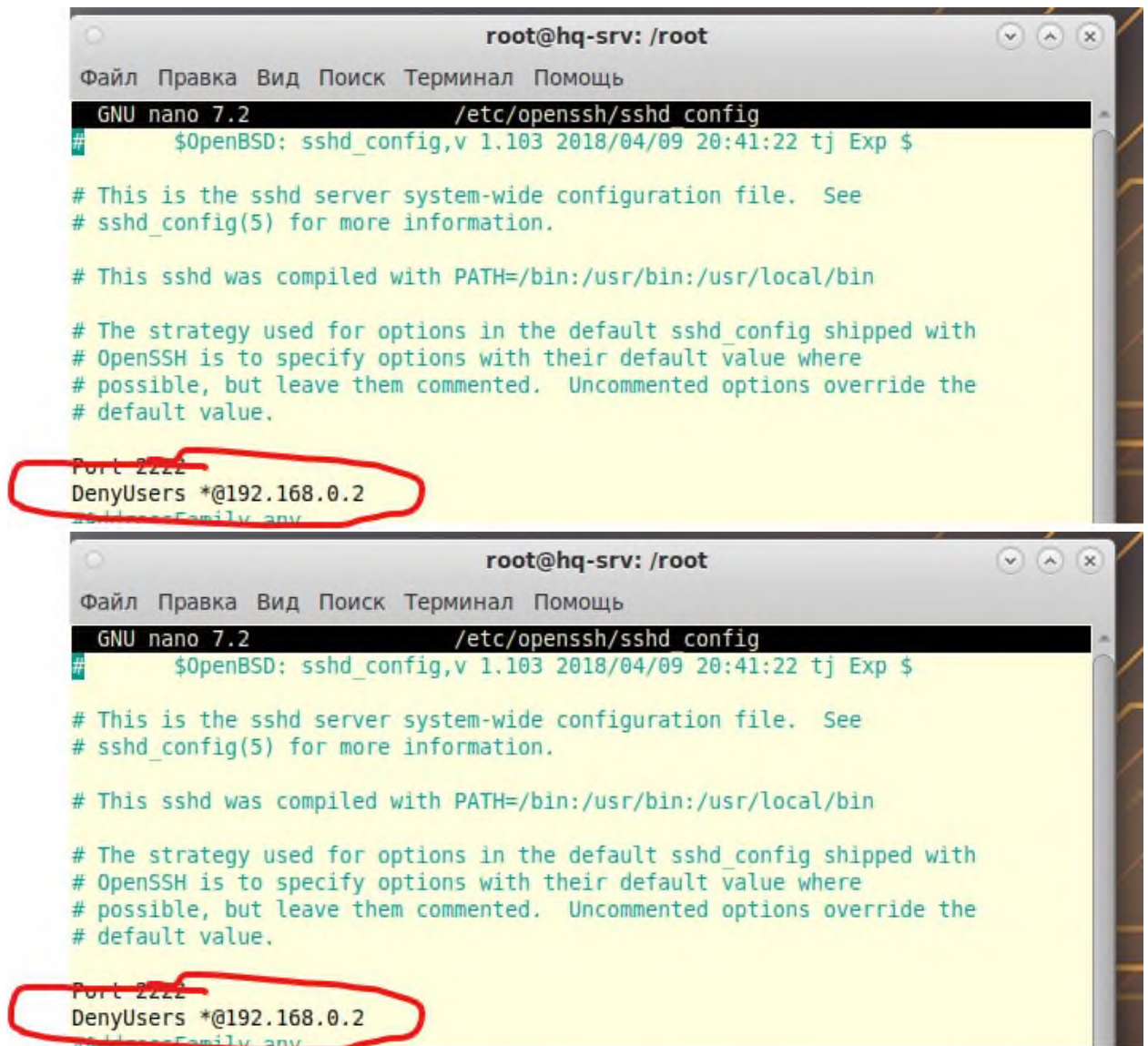
```
iptables -t nat -A PREROUTING -i eth0 -s 10.10.11.0/30 -p tcp --dport 2222 -j DNAT --to-destination 192.168.1.2:2222
```

## Модуль 1 задание 8

HQ-SRV

```
nano /etc/openssh/sshd_config
```

Вместо 192.168.0.2 указывайте свой если он изменяется, можете вообще заблокировать сеть 192.168.0.\* но это не точно



## Модуль 2 задание 1

nano /etc/bind/options.conf

```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/bind/options.conf Изменён
statistics-file "/var/run/named.stats";
recursing-file "/var/run/recursing";

// disables the use of a PID file
pid-file none;

/*
 * Oftenly used directives are listed below.
 */

listen-on { any; };
listen-on-v6 { any; };
allow-query { any; };
/*
 * If the forward directive is set to "only" the server will only
```

```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/bind/options.conf Изменён
statistics-file "/var/run/named.stats";
recursing-file "/var/run/recursing";

// disables the use of a PID file
pid-file none;

/*
 * Oftenly used directives are listed below.
 */

listen-on { any; };
listen-on-v6 { any; };
allow-query { any; };
/*
 * If the forward directive is set to "only" the server will only
```

```
systemctl enable --now bind
echo name servers=127.0.0.1 >> /etc/resolvconf.conf
Executing: /lib/systemd/systemd-sysv-install enable bind
[root@hq-srv ~]# echo name_server=127.0.0.1 >> /etc/resolvconf.conf
[root@hq-srv ~]#
```

```
Executing: /lib/systemd/systemd-sysv-install enable bind
[root@hq-srv ~]# echo name_server=127.0.0.1 >> /etc/resolvconf.conf
[root@hq-srv ~]#
```

```
resolvconf -u
nano /etc/bind/local.conf
```



```
// The other zones here
zone "hq.work"{
type master;
file "hq.db";
};
zone "branch.work"{
type master;
file "branch.db";
};
zone "1.168.192.in-addr.arpa"{
type master;
file "1.db";
};
zone "2.168.192.in-addr.arpa"{
[ Прочитано
```

```
// The other zones here
zone "hq.work"{
type master;
file "hq.db";
};
zone "branch.work"{
type master;
file "branch.db";
};
zone "1.168.192.in-addr.arpa"{
type master;
file "1.db";
};
zone "2.168.192.in-addr.arpa"{
[ Прочитано
```

```
cp /etc/bind/zone/{localdomain,hq.db}
cp /etc/bind/zone/{localdomain,branch.db}
cp /etc/bind/zone/{127.in-addr.arpa,1.db}
cp /etc/bind/zone/{127.in-addr.arpa,2.db}
chown root:named /etc/bind/zone/{hq,branch,1,2}.db
nano /etc/bind/zone/hq.db
```

```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/bind/zone/hq.db Изменён
$TTL      1D
@         IN      SOA      hq.work. root.hq.work. (
                                2024021400      ; serial
                                12H              ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                                )
                                IN      NS       hq.work.
                                IN      A       127.0.0.0
hq-r      IN      A       192.168.1.1
hq-srv    IN      A       192.168.1.2

^G Справка  ^O Записать  ^W Поиск    ^K Вырезать  ^T Выполнить ^C Позиция
^X Выход    ^R ЧитФайл  ^\ Замена  ^U Вставить  ^J Выводить  ^/ К строке
```

```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/bind/zone/hq.db Изменён
$TTL      1D
@         IN      SOA      hq.work. root.hq.work. (
                                2024021400      ; serial
                                12H              ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                                )
                                IN      NS       hq.work.
                                IN      A       127.0.0.0
hq-r      IN      A       192.168.1.1
hq-srv    IN      A       192.168.1.2

^G Справка  ^O Записать  ^W Поиск    ^K Вырезать  ^T Выполнить ^C Позиция
^X Выход    ^R ЧитФайл  ^\ Замена  ^U Вставить  ^J Выводить  ^/ К строке
```

nano /etc/bind/zone/branch.db

```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/bind/zone/branch.db Изменён
$TTL      1D
@          IN      SOA      branch.work. root.branch.work. (
                                2024021400      ; serial
                                12H              ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                                )
                                IN      NS       localhost.
                                IN      A       127.0.0.0
br-r       IN      A       192.168.2.1
br-srv     IN      A       192.168.2.2

^G Справка  ^O Записать ^W Поиск    ^K Вырезать ^T Выполнить ^C Позиция
^X Выход    ^R ЧитФайл ^\ Замена   ^U Вставить ^J Выровнять ^/_ К строке
```

```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/bind/zone/branch.db Изменён
$TTL      1D
@          IN      SOA      branch.work. root.branch.work. (
                                2024021400      ; serial
                                12H              ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                                )
                                IN      NS       localhost.
                                IN      A       127.0.0.0
br-r       IN      A       192.168.2.1
br-srv     IN      A       192.168.2.2

^G Справка  ^O Записать ^W Поиск    ^K Вырезать ^T Выполнить ^C Позиция
^X Выход    ^R ЧитФайл ^\ Замена   ^U Вставить ^J Выровнять ^/_ К строке
```

nano /etc/bind/zone/1.db

```
GNU nano 7.2 /etc/bind/zone/1.db Изменён
$TTL 1D
@ IN SOA hq.work. root.hq.work. (
    2024021400 ; serial
    12H        ; refresh
    1H         ; retry
    1W         ; expire
    1H         ; ncache
)
1 IN NS hq.work.
2 IN PTR hq-r.hq.work.
2 IN PTR hq-srv.hq.work.
```

nano /etc/bind/zone/2.db



```
root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/bind/zone/2.db Изменён
$TTL      1D
@         IN      SOA      branch.work. root.branch.work. (
                                2024021400      ; serial
                                12H              ; refresh
                                1H               ; retry
                                1W               ; expire
                                1H               ; ncache
                                )
          IN      NS       branch.work.
1         IN      PTR      br-r.branch.work.

^G Справка  ^O Записать ^W Поиск   ^K Вырезать ^T Выполнить ^C Позиция
^X Выход    ^R ЧитФайл ^\ Замена  ^U Вставить ^J Выводить  ^/ К строке

root@hq-srv: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/bind/zone/2.db Изменён
$TTL      1D
@         IN      SOA      branch.work. root.branch.work. (
                                2024021400      ; serial
                                12H              ; refresh
                                1H               ; retry
                                1W               ; expire
                                1H               ; ncache
                                )
          IN      NS       branch.work.
1         IN      PTR      br-r.branch.work.
```

```
named-checkconf -z
systemctl restart bind
```

```
[root@hq-srv ~]# named-checkconf -z
zone localhost/IN: loaded serial 2024021400
zone localdomain/IN: loaded serial 2024021400
zone 127.in-addr.arpa/IN: loaded serial 2024021400
zone 0.in-addr.arpa/IN: loaded serial 2024021400
zone 255.in-addr.arpa/IN: loaded serial 2024021400
zone hq.work/IN: loaded serial 2024021400
zone branch.work/IN: loaded serial 2024021400
zone 1.168.192.in-addr.arpa/IN: loaded serial 2024021400
zone 2.168.192.in-addr.arpa/IN: loaded serial 2024021400
[root@hq-srv ~]#
```

```
[root@hq-srv ~]# named-checkconf -z
zone localhost/IN: loaded serial 2024021400
zone localdomain/IN: loaded serial 2024021400
zone 127.in-addr.arpa/IN: loaded serial 2024021400
zone 0.in-addr.arpa/IN: loaded serial 2024021400
zone 255.in-addr.arpa/IN: loaded serial 2024021400
zone hq.work/IN: loaded serial 2024021400
zone branch.work/IN: loaded serial 2024021400
zone 1.168.192.in-addr.arpa/IN: loaded serial 2024021400
zone 2.168.192.in-addr.arpa/IN: loaded serial 2024021400
[root@hq-srv ~]#
```

## Проверяем

```
[root@hq-srv ~]# host hq-r.hq.work
hq-r.hq.work has address 192.168.100.62
[root@hq-srv ~]# host hq-srv.hq.work
hq-srv.hq.work has address 192.168.100.1
[root@hq-srv ~]#
[root@hq-srv ~]# host 192.168.100.62
62.100.168.192.in-addr.arpa domain name pointer hq-r.hq.work.
[root@hq-srv ~]# host 192.168.100.1
1.100.168.192.in-addr.arpa domain name pointer hq-srv.hq.work.
[root@hq-srv ~]#
```

```
[root@hq-srv ~]# host hq-r.hq.work
hq-r.hq.work has address 192.168.100.62
[root@hq-srv ~]# host hq-srv.hq.work
hq-srv.hq.work has address 192.168.100.1
[root@hq-srv ~]#
[root@hq-srv ~]# host 192.168.100.62
62.100.168.192.in-addr.arpa domain name pointer hq-r.hq.work.
[root@hq-srv ~]# host 192.168.100.1
1.100.168.192.in-addr.arpa domain name pointer hq-srv.hq.work.
[root@hq-srv ~]#
```