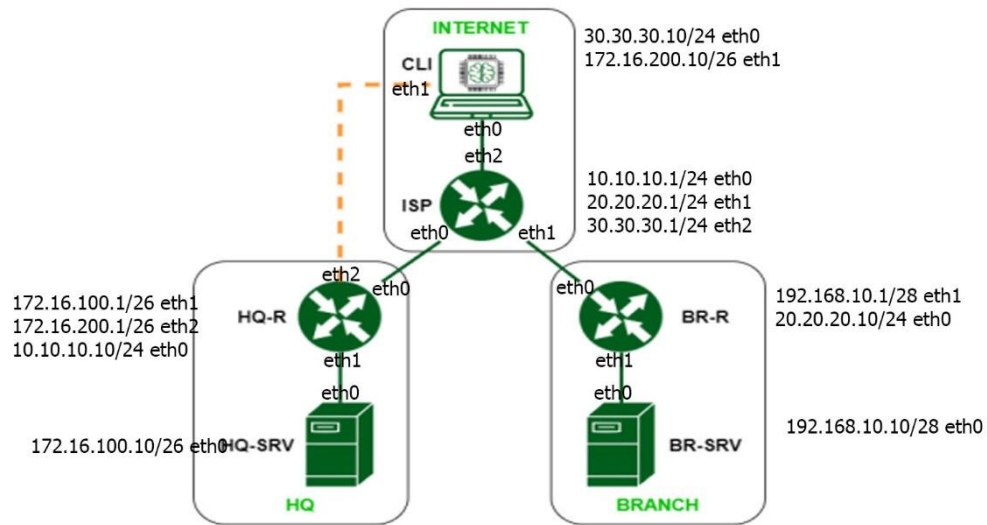


# Топология сети



Hostname	IP	Netmask	Gateway	Interface
CLI	30.30.30.10	255.255.255.0/24	30.30.30.1	Eth0
	172.16.200.10	255.255.255.0/24	-	Eth1
ISP	10.10.10.1	255.255.255.0/24	-	Eth0
	20.20.20.1	255.255.255.0/24	-	Eth1
	30.30.30.1	255.255.255.0/24	-	Eth2
	DHCP			Eth3
HQ-R	10.10.10.10	255.255.255.0/24	10.10.10.1	Eth0
	172.16.100.1	255.255.255.192/26	-	Eth1
	172.16.200.1	255.255.255.0/24	-	Eth2
BR-R	20.20.20.10	255.255.255.0/24	20.20.20.1	Eth0
	192.168.10.1	255.255.255.240/28	-	Eth1
BR-SRV	192.168.10.10	255.255.255.240/28	192.168.10.1	Eth0
HQ-SRV	DHCP			Eth0
HQ-AD				Eth0
HQ-CLI				Eth0

# Предварительная настройка

Каждой машине в настройках вм выдать необходимое количество сетевых интерфейсов. Все интерфейсы настроены как intent кроме 4го интерфейса у ISP через который будет осуществляться доступ в интернет, его настраиваем как сеть NAT.

## Настройка имен

### Зайти в файл

nano /etc/hosts - Файл будет иметь вид

127.0.0.1 localhost

127.0.1.1 astra

astra – необходимо изменить в соответствии с таблицей

### Зайти в файл

nano /etc/hostname – файл будет иметь вид

astra – необходимо изменить в соответствии с таблицей

на машине которая будет использоваться в качестве сервера имен (dns) написать  
hq-srv.hq.work

## Настройка Сети

nano /etc/network/interfaces – в этом файле необходимо добавить записи

auto eth0 – номер интерфейса

iface eth0 inet static/dhcp – в зависимости от типа адреса (в случае если выбран dhcp следующие записи не нужны)

address 10.10.10.10 – ip адрес в соответствии с таблицей

netmask 255.255.255.0 – в соответствии с таблицей

gateway 10.10.10.1 – если есть

dns-nameservers 172.16.100.10 – адрес днс сервера пишется 1 раз не для каждого интерфейса

### выйти и сохранить

Включить пересылку пакетов (выполняется только на роутерах)

### Зайти в файл

Nano /etc/sysctl.conf

Найти строчку «net.ipv4.ip\_forward=1» и раскомментировать

### **Зайти в файл**

Nano /etc/resolv.conf – где необходимо прописать

Nameserver 172.16.100.10

Nameserver 8.8.8.8

### **Выйти из файла и прописать**

Systemctl restart networking

## **Настройка доступа в интернет на ISP и раздача его в соседние сети**

```
iptables -t nat -A POSTROUTING -s 172.16.100.0/26 -o eth3 -j MASQUERADE
```

172.16.100.0 – сеть которой необходимо дать доступ к интернету

Eth3 – интерфейс который подключен к сети NAT

### **Повторить для каждой сети.**

После этого надо сохранить эти правила. Для этого потребуется сделать следующие действия.

```
nano /etc/network/if-post-down.d/iptables
```

```
#!/bin/sh
```

```
touch /etc/iptables_rules
```

```
chmod 640 /etc/iptables_rules
```

```
iptables-save > /etc/iptables.rules
```

```
exit 0
```

### **Выйти из файла**

```
chmod +x /etc/network/if-post-down.d/iptables
```

### **Далее**

```
Sudo nano /etc/network/if-pre-up.d/iptables
```

```
#!/bin/sh
```

```
iptables-restore < /etc/iptables.rules
```

```
exit 0
```

### **Выйти из файла**

```
chmod +x /etc/network/if-pre-up.d/iptables
```

## Установка frr

apt-cdrom add

apt update

apt install curl -y

mkdir /usr/share/keyrings – создать каталог для ключей

### Установить ключи

```
curl -s https://deb.frrouting.org/frr/keys.gpg | sudo tee /usr/share/keyrings/frrouting.gpg > /dev/null
```

### Зайти в файл

nano /etc/apt/sources.list – в нем написать следующее

```
deb https://dl.astralinux.ru/astra/stable/orel/repository orel main contrib non-free
```

### Зайти в файл

nano /etc/apt/sources.list.d/frr.list – в нем написать следующее

```
deb [trusted=true signed-by=/usr/share/keyrings/frrouting.gpg]
```

```
https://deb.frrouting.org/frr stretch frr-stable
```

### Обновляемся и устанавливаем frr

```
apt update && apt install frr frr-pythontools
```

## Настройка frr

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

ospf = no – исправить на yes

```
systemctl restart frr
```

```
Vtysh
```

```
configure
```

```
ip forwarding
```

```
int eth0 (интерфейс, который смотрит к конечному пользователю)
```

```
Ip ospf passive
```

```
Router ospf
```

```
Network 10.10.10.0/24 (подсеть которую знает настраиваемый роутер) area 0
```

### Повторить для всех подсетей которые знает роутер

```
end
```

write

### **Повторить на всех роутерах**

Для того чтобы проверить необходимо написать команду

show ip route

Также после настройки на всех роутерах все узлы должны пинговаться друг с другом.

## **Установка и настройка dhcp**

apt-cdrom add

apt install isc-dhcp-server -y

nano /etc/default/isc-dhcp-server

INTERFACES = "eth0" – указать интерфейс смотрящий во внутреннюю сеть.

### **Выйти и сохранить**

nano /etc/dhcp/dhcp.conf

раскомментировать authoritative

### **создать запись типа**

subnet 172.16.100.0 netmask 255.255.255.0 {

range 172.16.100.10 172.16.100.50;

option routers 172.16.100.1;} – диапазон раздачи адресов

### **создать запись типа**

host hq-srv {

hardware Ethernet 00:00:00:00:00:00;

fixed-address 172.16.100.10;} – выдача фиксированного адреса

### **сохранить и выйти**

systemctl restart isc-dhcp-server

## **Создание пользователей**

adduser username (имя пользователя)

## **Установка iperf3 и замер пропускной способности**

apt-cdrom add

apt install debian-archive-keyring dirmngr

nano /etc/apt/sources.list - добавить ссылку на репозиторий Debian:

deb https://archive.debian.org/debian/ stretch main contrib non-free

apt update

apt install iperf3

**Iperf3 работает в клиент-серверном режиме.**

**На ISP прописать:**

iperf3 -s -запустить серверный режим

**На HQ-R:**

iperf3 -c 10.10.10.1 (ip ISP)

**Так же существует более простой способ установить iperf 1 версии**

apt-cdrom add

apt install iperf

script -c 'iperf3 -c 10.10.10.1(IPv4 ISP, смотрящий в сторону HQ-R) --get-server-output' iperf3\_logfile.txt (файл\_журнала)

## Настройка SSH

apt-cdrom add

apt update && apt install ssh

nano /etc/ssh/sshd\_config

Найти строку #Port 22, раскомментировать и изменить на Port 2222

Найти строку #PermitRootLogin prohibit, раскомментировать изменить на PermitRootLogin no

**добавить строку**

AllowUsers admin netadmin

**Сохранить и выйти**

systemctl restart ssh

данные манипуляции проделываются на сервере ssh

nano /etc/ssh/sshd\_config

раскомментировать “#Port 22” и изменить на “Port 2222”

ssh admin@172.16.100.10 (IP HQ-SRV) – подключение к серверу ssh

## НАСТРОЙКА DNS

Вариант простой настройки "Локальный сервер DNS"

Это вариант настройки собственного полноценного DNS-сервера, обслуживающего собственную локальную сеть (собственный DNS-домен). Создание DNS-сервера в локальной сети необходимо для организации единого пространства имен для всех сетевых служб и пользователей. В отличие от кеширующего сервера из предыдущего примера, этот сервер самостоятельно обрабатывает запросы, относящиеся к его зоне ответственности.

Для примера используем следующую конфигурацию сети:

- домен localnet.example.ru;
- сервер DNS в этом домене с именем dns.localnet.example.ru и адресом 192.168.32.211;
- компьютер host в этом домене с именем host.localnet.example.ru и адресом 192.168.32.96.

Для настройки конфигурации bind:

1. Файл конфигурации /etc/bind/named.conf.options использовать из предыдущего примера;
2. Внести информацию о домене в файл конфигурации /etc/bind/named.conf.local. Исходно в этом файле содержатся только комментарии. Добавить следующие строки:

```
zone "localnet.example.ru" {                               # имя прямой зоны
    type master;                                           # тип master указывает, что запросы относительно этой зоны будут обрабатываться этим сервером, и перенаправляться не будут
    file "/etc/bind/zones/db.localnet.example.ru";        # путь к файлу данных прямой зоны
};

zone "32.168.192.in-addr.arpa" {                          # имя реверсивной зоны. Имя реверсивной зоны формируется из адреса сети, с обратным порядком чисел.
    type master;                                           # тип master указывает, что запросы, относящиеся к этой зоне, будут обрабатываться этим сервером, и перенаправляться не будут
    file "/etc/bind/zones/db.32.168.192";                # подсеть 192.168.32.0/24, путь к файлу данных
};
```

3. Создать подкаталог /etc/bind/zones для хранения файлов данных, и скопировать в созданный каталог образцы файлов данных:

```
sudo mkdir /etc/bind/zones
sudo cp /etc/bind/db.local /etc/bind/zones/db.localnet.example.ru
sudo cp /etc/bind/db.127 /etc/bind/zones/db.32.168.192
sudo chown -R bind:bind /etc/bind/zones
```

4. Внести изменения в файл прямой зоны /etc/bind/zones/db.localnet.example.ru:

```
$TTL      604800
@         IN      SOA      dns.localnet.example.ru. admin.localnet.example.ru. (
                                3          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
; name servers - NS records - определяем имена DNS-серверов
IN        NS       dns.localnet.example.ru.
; name servers - A records - определяем адреса компьютеров, сначала сервер(ы) DNS
dns.localnet.example.ru.      IN      A       192.168.32.211
; 192.168.32.0/24 - A records - а потом все остальные компьютер(ы) сети
host.localnet.example.ru.     IN      A       192.168.32.96
```

5. Внести изменения в файл /etc/bind/zones/db.32.168.192 реверсивной зоны:

```
$TTL      604800
@         IN      SOA      localnet.example.ru. admin.localnet.example.ru. (
                                3          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL ;

; name servers
IN        NS       dns.localnet.example.ru.
; PTR Records
211 IN      PTR     dns.localnet.example.ru.    ; 192.168.32.211
96  IN      PTR     host.localnet.example.ru.   ; 192.168.32.96
```

6. Проверить созданную конфигурацию с помощью соответствующих инструментов :

```
sudo named-checkconf
sudo named-checkzone localnet.example.ru /etc/bind/zones/db.localnet.example.ru
sudo named-checkzone 32.168.192.in-addr.arpa /etc/bind/zones/db.32.168.192
```

7. Перезапустить службу:

```
sudo systemctl restart bind9
```

Проверить работу сервера можно выполнив на сервере команду:

```
dig @localhost host.localnet.example.ru
```