Методичка для подготовки демонстрационному экзамену.

1.1.Выполните базовую настройку всех устройств

Логин это имя машины (isp, cli, hq-r, hq-s), пароль везде “1”
команда ”ip a” позволяет просмотреть ip адреса на интерфейсах
команда ”ip r” позволяет просмотреть таблицу маршрутизации

Пример IP-адресации представлен в таблице 1:

Таблица 1

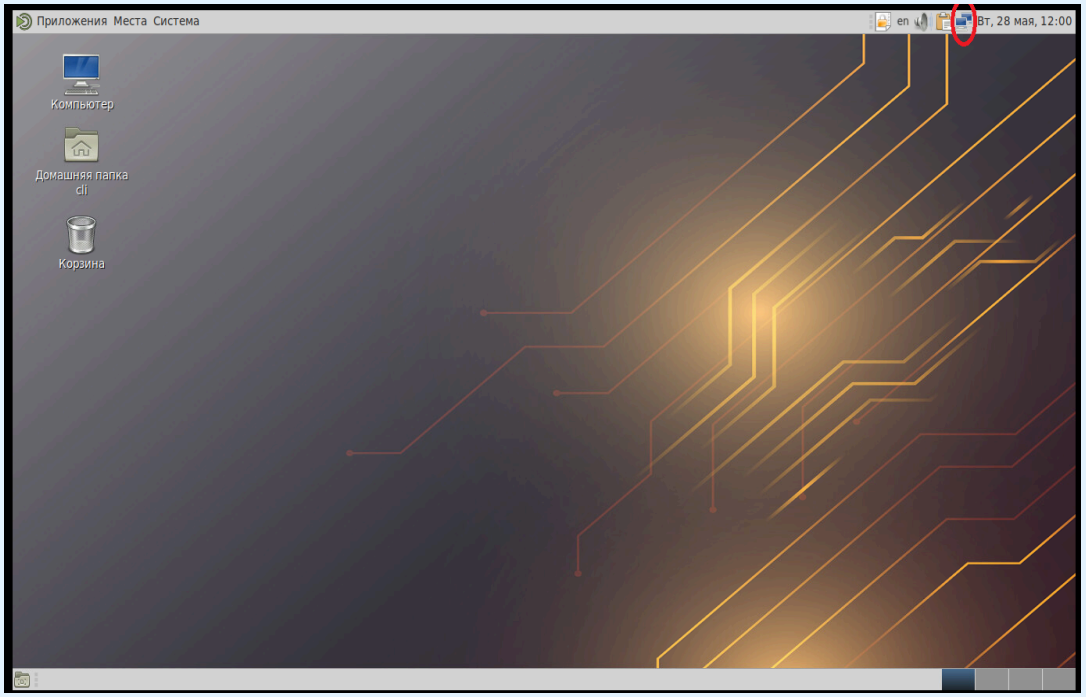
Hostname	Interface	IPv4	GW IPv4	DNS	IPv6	GW IPv6	Network
ISP	ens33	3.3.3.1/30	-	-	2024:3::1/64	-	ISP-CLI
	ens34	1.1.1.1/30	-	-	2024:1::1/64	-	ISP-netL
	ens35	2.2.2.1/30	-	-	2024:2::1/64	-	ISP-netR
	ens38	VM Network	-	-	VM Network	-	VM Network
HQ_R	ens33	1.1.1.2/30	1.1.1.1	10.104.1.100	2024:1::2/64	2024:1::1	ISP-netR
	ens34	172.16.100.1/26	-	-	FD24:172::1/122	-	HQ_R-HQ_S
	tun1	192.168.161.1/30	-	-	FD24:161::1/64	-	HQ_R-BR_R
BR_R	ens33	2.2.2.2/30	2.2.2.1	10.104.1.100	2024:2::2/64	2024:2::1	ISP-netR
	ens34	192.168.100.1/28	-	-	FD24:192::1/124	-	BR_R-BR_S
	tun1	192.168.161.2/30	-	-	FD24:161::2/64	-	HQ_R-BR_R
HQ-SRV	ens33	DHCP	172.16.100.1	10.104.1.100	DHCP	FD24:172::1	HQ_R-HQ_S
BR-SRV	ens33	192.168.100.10/28	192.168.100.1	10.104.1.100	FD24:192::2/124	FD24:192::1	BR_R-BR_S
CLI	ens33	3.3.3.2/30	3.3.3.1		2024:3::2/64	2024:3::1	ISP-CLI

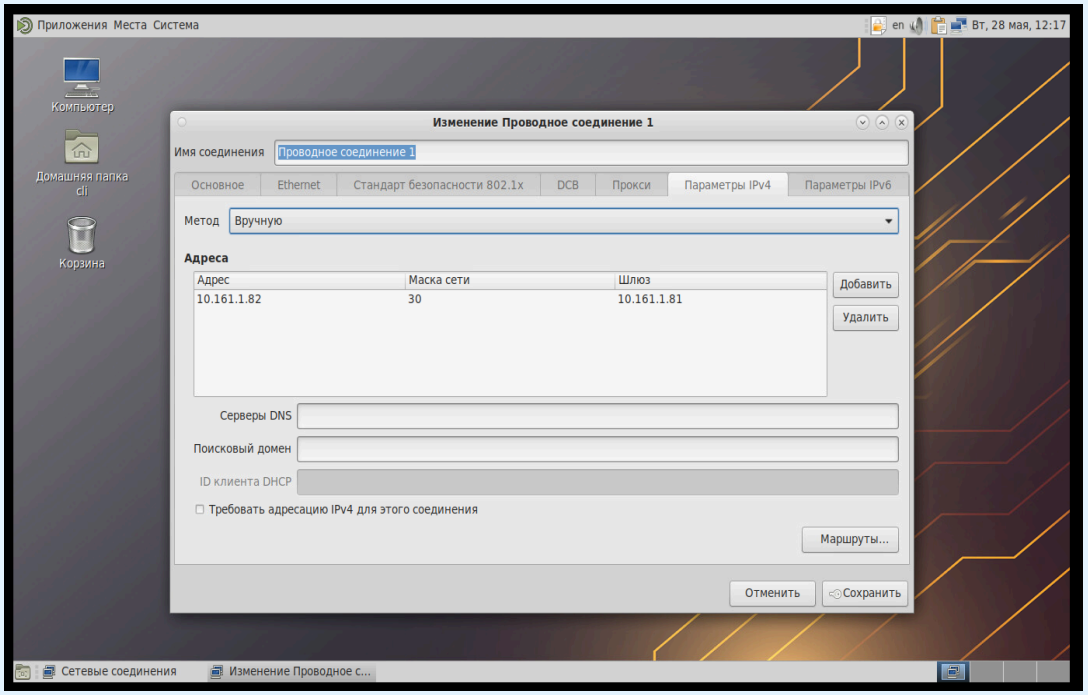
a. Присвоить имена в соответствии с топологией

Имена устройств (hostname) – прописывать строчными символами (маленькими буквами)

```
nmcli general hostname <NAME>
exec bash
```

На машинах с графикой правой кнопкой мыши нажимаем на вкладку “проводное соединение”, параметры соединений и два раза кликаем на “Проводное соединение 1” пишем ip адрес, маску и шлюз.
Не забываем указать метод “Вручную” и нажимаем кнопку сохранить.
Нажимаем на проводное соединение чтобы установилось соединение.



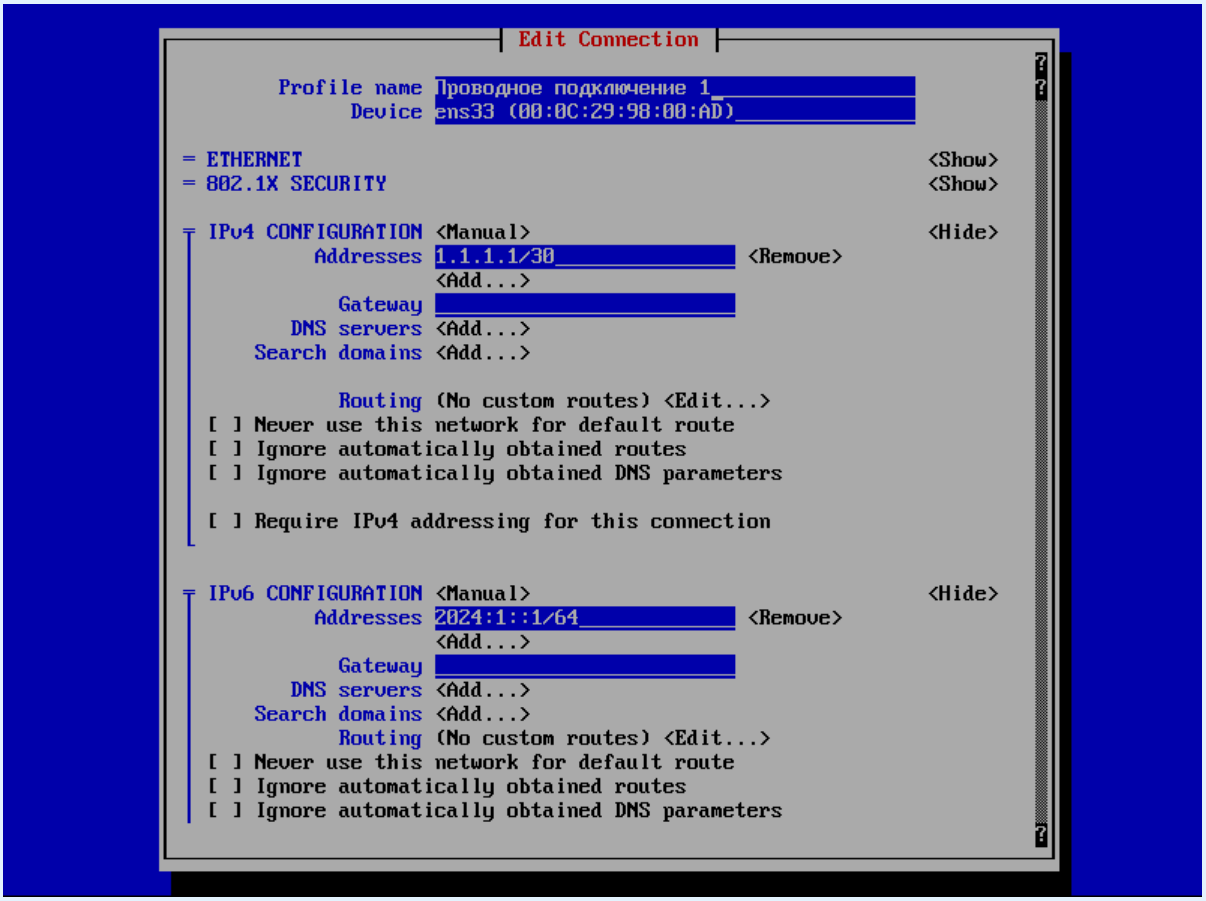


На машинах без графики с помощью предустановленного средства управления сетевыми интерфейсами Network Manager прописываем IP-адреса.

С помощью утилиты nmtui задаем IP адреса сетевым интерфейсам

Шлюзы прописываем только на тех интерфейсах которые являются конечными в сети.

Пример настройки:



После установки ip-адресов необходимо переподключить интерфейсы. Командой “ping IP” (нужный вам ip адрес)

```
[root@isp ~]# ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2) 56(84) bytes of data.
64 bytes from 1.1.1.2: icmp_seq=1 ttl=64 time=3.61 ms
64 bytes from 1.1.1.2: icmp_seq=2 ttl=64 time=0.848 ms
64 bytes from 1.1.1.2: icmp_seq=3 ttl=64 time=1.26 ms
64 bytes from 1.1.1.2: icmp_seq=4 ttl=64 time=0.846 ms
^C
--- 1.1.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.846/1.641/3.613/1.150 ms
[root@isp ~]# _
```

```
[root@isp ~]# ping 2024:1::2
PING 2024:1::2(2024:1::2) 56 data bytes
64 bytes from 2024:1::2: icmp_seq=1 ttl=64 time=1.10 ms
64 bytes from 2024:1::2: icmp_seq=2 ttl=64 time=0.931 ms
64 bytes from 2024:1::2: icmp_seq=3 ttl=64 time=0.773 ms
64 bytes from 2024:1::2: icmp_seq=4 ttl=64 time=1.10 ms
^C
--- 2024:1::2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.773/0.976/1.101/0.136 ms
[root@isp ~]# S_
```

Настройка доступа в интернет

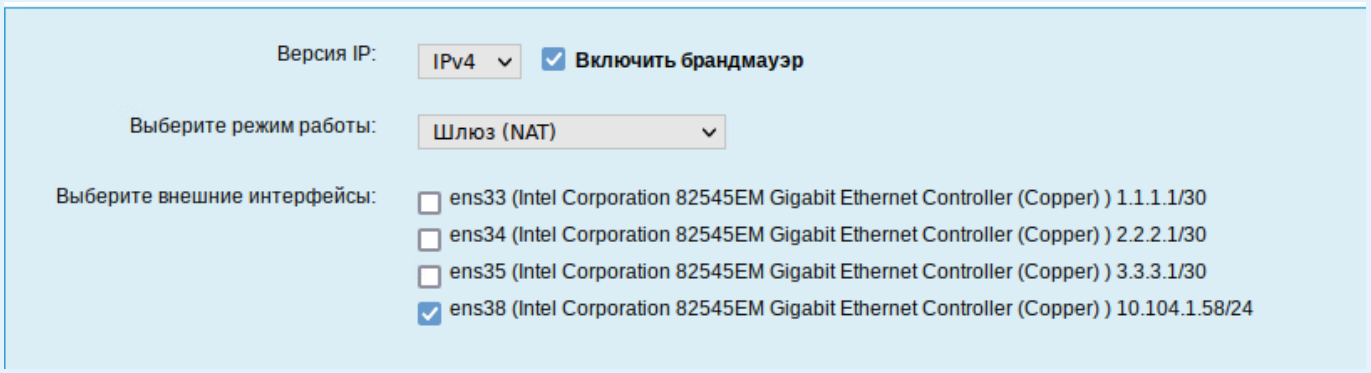
Сначала нужно обновить репозитории и затем установить нужные пакеты Альтератора:

```
apt-get update
apt-get install alterator-ahttpd alterator-net-iptables
```

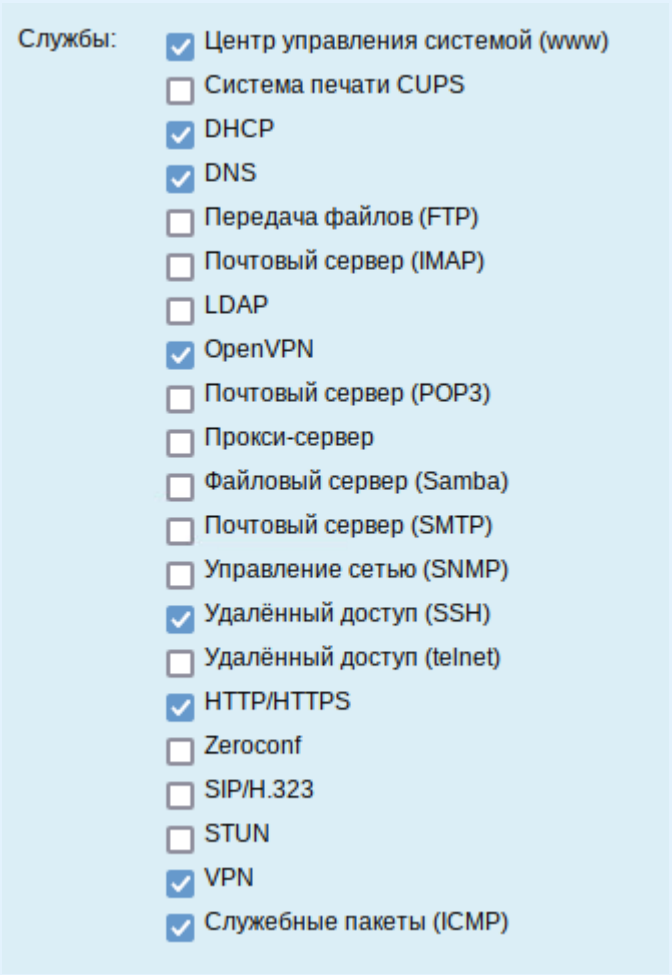
Добавляем альтератор в автозапуск и сразу запускаем его

```
systemctl enable ahttpd --now
```

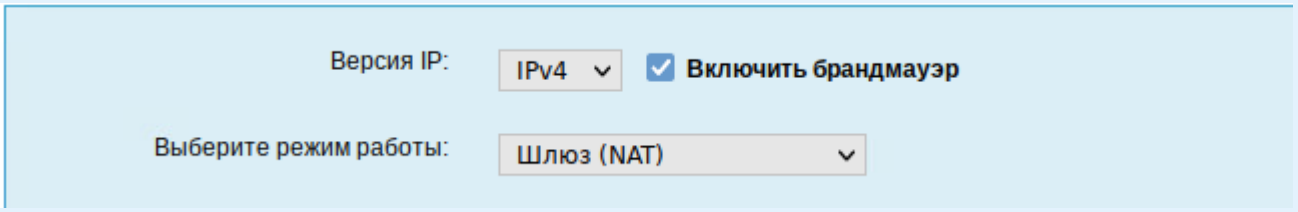
На машине CLI в браузере заходим по адресу 1.1.1.1:8080:
Выбираем внешний интерфейс



В службах выбираем > WWW;DHCP;DNS;OpenVPN;SSH;HTTP/HTTPS;VPN;ICMP



Включаем брандмауэр



1.2.Настройка внутренней динамической маршрутизации по средствам FRR.

Настройка HQ-R

```
# nmcli connection add type ip-tunnel ip-tunnel.mode gre ip-tunnel.parent ens33 con-name gre1 ifname gre1 remote 2.2.2.2 local 1.1.1.2
# nmcli connection modify gre1 ipv4.method manual ipv4.addresses '192.168.161.1/30'
# nmcli connection modify gre1 +ipv4.routes "192.168.100.0/28 192.168.161.2"
```

Для корректной работы протокола динамической маршрутизации требуется увеличить параметр TTL на интерфейсе туннеля:

```
# nmcli connection modify gre1 ip-tunnel.ttl 64
```

Проверяем:

```
ip -c a
```

```
gre1@ens33: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default qlen 1000
link/gre 1.1.1.2 peer 2.2.2.2
inet 192.168.161.1/30 brd 192.168.161.3 scope global noprefixroute gre1
   valid_lft forever preferred_lft forever
inet6 fd24:161::1/64 scope global noprefixroute
   valid_lft forever preferred_lft forever
inet6 fe80::b2e0:be8f:6fda:8313/64 scope link noprefixroute
   valid_lft forever preferred_lft forever
```

Настройка BR-R

Настройка GRE – туннеля на BR-R производится аналогично HQ-R

```
# nmcli connection add type ip-tunnel ip-tunnel.mode gre ip-tunnel.parent ens33 con-name gre1 ifname gre1 remote 1.1.1.2 local 2.2.2.2
# nmcli connection modify gre1 ipv4.method manual ipv4.addresses '192.168.161.2/30'
# nmcli connection modify gre1 +ipv4.routes "172.16.100.0/26 192.168.161.1"
```

Для корректной работы протокола динамической маршрутизации требуется увеличить параметр TTL на интерфейсе туннеля:

```
# nmcli connection modify gre1 ip-tunnel.ttl 64
```

Проверяем:

```
ip -c a
```

```
grel@ens33: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default qlen 1000
link/gre 2.2.2.2 peer 1.1.1.2
inet 192.168.161.2/30 brd 192.168.161.3 scope global noprefixroute grel
   valid_lft forever preferred_lft forever
inet6 fd24:161::2/64 scope global noprefixroute
   valid_lft forever preferred_lft forever
inet6 fe80::2e03:6681:277d:1241/64 scope link noprefixroute
   valid_lft forever preferred_lft forever
```

Был создан новый виртуальный интерфейс (туннель) для прямого взаимодействия устройств HQ-R и BR-R. Они будут напрямую обмениваться маршрутами внутренних сетей HQ и BRANCH через это соединение.

Проверяем

HQ-R

```
[root@hq-r ~]# ip -c --br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             1.1.1.2/30 2024:1::2/64 fe80::8159:a47c:b461:137/64
ens34            UP             172.16.100.1/26 fd24:172::1/122 fe80::c2f2:c4c0:103d:8677/64
gre0@NONE        DOWN
gretap0@NONE     DOWN
erspan0@NONE     DOWN
gre1@ens33       UNKNOWN        192.168.161.1/30 fd24:161::1/64 fe80::b2e0:be8f:6fda:8313/64
[root@hq-r ~]# ping -c4 192.168.161.2
PING 192.168.161.2 (192.168.161.2) 56(84) bytes of data.
64 bytes from 192.168.161.2: icmp_seq=1 ttl=64 time=1.99 ms
64 bytes from 192.168.161.2: icmp_seq=2 ttl=64 time=1.72 ms
64 bytes from 192.168.161.2: icmp_seq=3 ttl=64 time=5.57 ms
64 bytes from 192.168.161.2: icmp_seq=4 ttl=64 time=1.36 ms

--- 192.168.161.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.363/2.659/5.569/1.694 ms
[root@hq-r ~]# ping -c4 fd24:161::2
PING fd24:161::2(fd24:161::2) 56 data bytes
64 bytes from fd24:161::2: icmp_seq=1 ttl=64 time=2.00 ms
64 bytes from fd24:161::2: icmp_seq=2 ttl=64 time=1.75 ms
64 bytes from fd24:161::2: icmp_seq=3 ttl=64 time=1.97 ms
64 bytes from fd24:161::2: icmp_seq=4 ttl=64 time=1.36 ms

--- fd24:161::2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.357/1.768/2.001/0.257 ms
[root@hq-r ~]#
```

BR-R

```
[root@br-r ~]# ip -c --br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             2.2.2.2/30 2024:2::2/64 fe80::14ed:13d2:c44d:eb22/64
ens34            UP             192.168.100.1/28 fd24:192::1/124 fe80::4e0b:f9b2:e3f3:a3e8/64
gre0@NONE        DOWN
gretap0@NONE     DOWN
erspan0@NONE     DOWN
gre1@ens33       UNKNOWN        192.168.161.2/30 fd24:161::2/64 fe80::2e03:6681:277d:1241/64
[root@br-r ~]# ping -c4 192.168.161.1
PING 192.168.161.1 (192.168.161.1) 56(84) bytes of data.
64 bytes from 192.168.161.1: icmp_seq=1 ttl=64 time=1.91 ms
64 bytes from 192.168.161.1: icmp_seq=2 ttl=64 time=1.71 ms
64 bytes from 192.168.161.1: icmp_seq=3 ttl=64 time=1.83 ms
64 bytes from 192.168.161.1: icmp_seq=4 ttl=64 time=1.91 ms

--- 192.168.161.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.714/1.841/1.912/0.080 ms
[root@br-r ~]# ping -c4 fd24:161::1
PING fd24:161::1(fd24:161::1) 56 data bytes
64 bytes from fd24:161::1: icmp_seq=1 ttl=64 time=4.35 ms
64 bytes from fd24:161::1: icmp_seq=2 ttl=64 time=1.29 ms
64 bytes from fd24:161::1: icmp_seq=3 ttl=64 time=1.99 ms
64 bytes from fd24:161::1: icmp_seq=4 ttl=64 time=5.32 ms

--- fd24:161::1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.286/3.236/5.317/1.654 ms
[root@br-r ~]#
```

Настройка динамической (внутренней) маршрутизации средствами FRR

Настройка на HQ-R

Установка пакет frr

```
# apt-get install -y frr
```

Для настройки внутренней динамической маршрутизации для IPv4 и IPv6 будет использован протокол OSPFv2 и OSPFv3

Для настройки ospf необходимо включить соответствующий демон в конфигурации /etc/frr/daemons

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

В конфигурационном файле /etc/frr/daemons необходимо активировать выбранный протокол для дальнейшей реализации его настройки:

ospfd = yes - для OSPFv2 (IPv4)

ospf6d = yes - для OSPFv3 (IPv6)

Включаем и добавляем в автозагрузку службу FRR

```
# systemctl enable --now frr
```

Переходим в интерфейс управление симуляцией FRR при помощи vtysh (аналог cisco)

```
# vtysh
```

Настройки OSPFv2 и OSPFv3 на HQ-R

```
[root@hq-r ~]# vtysh

Hello, this is FRRouting (version 9.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

hq-r# conf t
hq-r(config)# router ospf
hq-r(config-router)# passive-interface default
hq-r(config-router)# network 172.16.100.0/26 area 0
hq-r(config-router)# network 192.168.161.0/30 area 0
hq-r(config-router)# ex
hq-r(config)# interface gre1
hq-r(config-if)# no ip ospf network broadcast
hq-r(config-if)# no ip ospf passive
hq-r(config-if)# ex
hq-r(config)# do write
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
hq-r(config)# router ospf6
hq-r(config-ospf6)# ospf6 router-id 1.1.1.1
hq-r(config-ospf6)# ex
hq-r(config)# interface gre1
hq-r(config-if)# ipv6 ospf6 area 0
gre1 already attached to Area 0
hq-r(config-if)# ex
hq-r(config)# interface ens34
hq-r(config-if)# ipv6 ospf6 area 0
hq-r(config-if)# ex
hq-r(config)# do write
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
hq-r(config)#
```

где:

OSPFv2

conf t или configure terminal - вход в режим глобальной конфигурации

router ospf - переход в режим конфигурации OSPFv2

passive-interface default - перевод всех интерфейсов в пассивный режим

network - объявляем локальную сеть офиса HQ и сеть (GRE-туннеля)

exit - выход и режима конфигурации OSPFv2

туннельный интерфейс gre1 делаем активным, для установления соседства с BR-R и обмена внутренними маршрутами

no ip ospf passive - перевод интерфейса tun1 в активный режим

do write - сохраняем текущую конфигурацию

OSPFv3

router ospf6 - переход в режим конфигурации OSPFv3

ospf6 router-id - назначение номера router-id

сети интерфейсов gre1 и ens34 добавляем в конфигурацию OSPFv3

do write - сохраняем текущую конфигурацию

Перезапускаем frr

```
# systemctl restart frr
```

Посмотреть текущую конфигурацию можно с помощью следующих команд

```
# vtysh # show running-config
```

Настройка на BR-R

Настройки OSPFv2 и OSPFv3 на BR-R аналогичны HQ-R

Необходимо изменить

объявляемые сети в OSPFv2;

router-id в OSPFv3

Настройки OSPFv2 и OSPFv3 на BR-R

```
[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)# router ospf
br-r(config-router)# passive-interface default
br-r(config-router)# network 192.168.100.0/28 area 0
br-r(config-router)# network 192.168.161.0/30 area 0
br-r(config-router)# ex
br-r(config)# interface grel
br-r(config-if)# no ip ospf network broadcast
br-r(config-if)# no ip ospf passive
br-r(config-if)# ex
br-r(config)# do wri
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
br-r(config)# router ospf6
br-r(config-ospf6)# ospf6 router-id 2.2.2.2
br-r(config-ospf6)# ex
br-r(config)# interface ens34
br-r(config-if)# ipv6 ospf6 area 0
br-r(config-if)# ex
br-r(config)# interface grel
br-r(config-if)# ipv6 ospf6 area 0
br-r(config-if)# ex
br-r(config)# do write
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
br-r(config)#
```

Посмотреть текущую конфигурацию можно с помощью следующих команд
vtysh # show running-config

1.3.Настройте автоматическое распределение IP-адресов на роутере HQ-R.

a. Учтите, что у сервера должен быть зарезервирован адрес.

Настройка DHCP на HQ-R для IPv4

Установка DHCP

```
# apt-get update && apt-get install -y dhcp-server
```

Настройки для диапазона адресов IPv4 производятся в файле /etc/dhcp/dhcpd.conf. Пример данного файла можно посмотреть в файле /usr/share/doc/dhcp-server/dhcpd.conf.example.

Открываем файл конфигурации

```
# nano /etc/dhcp/dhcpd.conf
```

Подсети обозначаются блоками, пример такого блока представлен ниже:

```
subnet 172.16.100.0 netmask 255.255.255.192  {
        range 172.16.100.2 172.16.100.62;
        option routers 172.16.100.1;
        default-lease-time 600;
        max-lease-time 7200;
}
```

где:

subnet - обозначает сеть, в области которой будет работать данная группа настроек;
range — диапазон, из которого будут браться IP-адреса;
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.

Резервирование ip-адреса за клиентом

Хосту с именем HQ-SRV , у которого сетевая карта имеет MAC ff:ff:ff:ff:ff:ff зарезервируем адрес 172.16.100.2.

```
host HQ-SRV {
        hardware ethernet ff:ff:ff:ff:ff:ff;
        fixed-address 172.16.100.2;
}
```

ff:ff:ff:ff:ff:ff - mac адрес интерфейса которому будет выдан статический ip-адрес

Выбираем интерфейс, для которого будет работать DHCP сервер

Открываем файл конфигурации

```
# nano /etc/sysconfig/dhcpd
```

Добавляем в него следующее:

```
DHCPDARGS=ens34
```

где:

ens34 - интерфейс смотрящий в сторону HQ-SRV

Запускаем и добавляем в автозагрузку службу dhcpd (для IPv4):

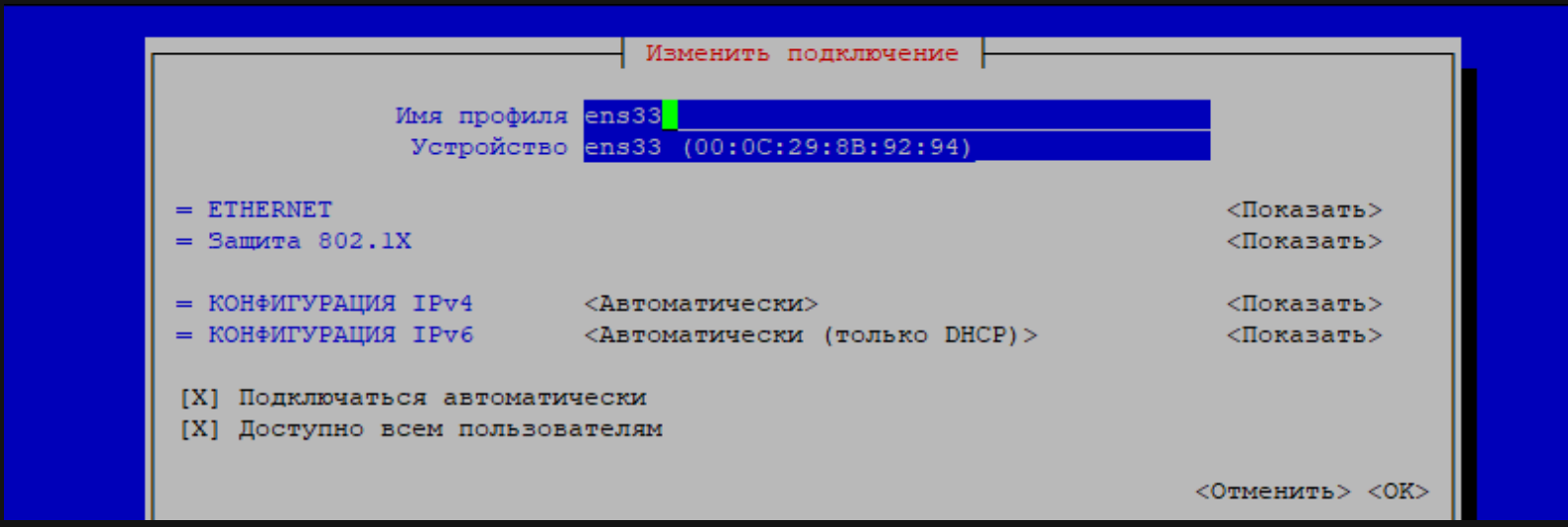
```
# systemctl enable --now dhcpd
```

Проверка на HQ-SRV

Открываем на HQ-SRV настройку сетевых интерфейсов

```
# nmtui
```

Настраиваем интерфейс на автоматическое получение адресов



Перезагружаем интерфейс и убеждаемся в работоспособности DHCP сервера

```
[root@hq-s ~]# ip -c 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:8b:92:94 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.100.10/26 brd 172.16.100.63 scope global dynamic noprefixroute ens33
       valid_lft 2877lsec preferred_lft 2877lsec
    inet6 fe80::70dc:c38e:b71e:ecfb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Настройка DHCP на HQ-R для IPv6

Настройки для диапазона адресов IPv6 производятся в файле /etc/dhcp/dhcpd6.conf. Пример данного файла можно посмотреть в файле /usr/share/doc/dhcp-server/dhcpd6.conf.example.

Для облегчения создания конфигурационного файла для DHCPv6

- Создаем резервную копию файла /etc/dhcp/dhcpd6.conf переименовав его
- Копируем файл /etc/dhcp/dhcpd6.conf.example в директорию /etc/dhcp/ с именем dhcpd6.conf

```
[root@hq-r dhcp]#
[root@hq-r dhcp]# mv /etc/dhcp/dhcpd6.conf /etc/dhcp/dhcpd6.conf.bak
[root@hq-r dhcp]#
[root@hq-r dhcp]# cp /etc/dhcp/dhcpd6.conf.sample /etc/dhcp/dhcpd6.conf
[root@hq-r dhcp]#
```

Открываем на редактирование файл конфигурации DHCPv6

```
# nano /etc/dhcp/dhcpd6.conf
```

Приводим файл к следующему виду удалив строки

Вы можете использовать клавиши Ctrl + K, которые вырезают всю строку

```
default-lease-time 2592000;
preferred-lifetime 604800;
option dhcp-renewal-time 3600;
option dhcp-rebinding-time 7200;

allow leasequery;

option dhcp6.preference 255;
option dhcp6.info-refresh-time 21600;

subnet6 FD24:172::/64 {
        range6 FD24:172::2 FD24:172::12;
}

#host HQ-SRV {
#        host-identifier option
#                dhcp6.client-id 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2;
#        fixed-address6 FD24:172::2;
#        fixed-prefix6 FD24:172::/64;
#        option dhcp6.name-servers FD24:172:2;
#}
```

Блок host комментируем. Для резервирования IPv6 требуется получить dhcp6.client-id.
dhcp6.client-id можно получить после запуска и получения клиентом (HQ-SRV) адреса.
Запускаем и добавляем в автозагрузку службу dhcpd6
systemctl enable --now dhcpd6

Перезагружаем сетевой интерфейс на HQ-SRV
Просматриваем журнал и ищем необходимый "DUID" для того, чтобы зарезервировать IPv6 адрес

```
[root@hq-r dhcp]# journalctl -f -u dhcpd6
июн 07 14:46:28 hq-r dhcpd[65717]: No pool found for IA_NA address fd24:172::3d
июн 07 14:46:28 hq-r dhcpd[65717]: Wrote 0 NA, 0 TA, 0 PD leases to lease file.
июн 07 14:46:28 hq-r dhcpd[65717]: Server starting service.
июн 07 14:46:44 hq-r dhcpd[65717]: Solicit message from fe80::70dc:c38e:b71e:ecfb port 546, transaction ID 0xB6E82D00
июн 07 14:46:44 hq-r dhcpd[65717]: Picking pool address fd24:172::12
июн 07 14:46:44 hq-r dhcpd[65717]: Advertise NA: address fd24:172::12 to client with duid 00:04:54:a8:c3:b5:83:74:7e:08:3c:e3:96:33:e1:d6:8f:48 iaid = 731133121 valid for 2592000 seconds
июн 07 14:46:44 hq-r dhcpd[65717]: Sending Advertise to fe80::70dc:c38e:b71e:ecfb port 546
июн 07 14:46:44 hq-r dhcpd[65717]: Request message from fe80::70dc:c38e:b71e:ecfb port 546, transaction ID 0xD7CC3600
июн 07 14:46:44 hq-r dhcpd[65717]: Reply NA: address fd24:172::12 to client with duid 00:04:54:a8:c3:b5:83:74:7e:08:3c:e3:96:33:e1:d6:8f:48 iaid = 731133121 valid for 2592000 seconds
июн 07 14:46:44 hq-r dhcpd[65717]: Sending Reply to fe80::70dc:c38e:b71e:ecfb port 546
^C
```

Этот DUID добавляем в host-identifier option при настройке HQ-R как DHCP сервера для IPv6. Снимаем коментарии с блока host.

```
default-lease-time 2592000;
preferred-lifetime 604800;
option dhcp-renewal-time 3600;
option dhcp-rebinding-time 7200;

allow leasequery;

option dhcp6.preference 255;
option dhcp6.info-refresh-time 21600;

subnet6 FD24:172::/122 {
        range6 FD24:172::2 FD24:172::12;
}

host HQ-SRV {
        host-identifier option
                dhcp6.client-id 00:04:17:06:02:ee:33:c3:7b:49:af:a0:d9:a5:44:b1:67:f1;
        fixed-address6 FD24:172::2;
        fixed-prefix6 FD24:172::/122;
        option dhcp6.name-servers FD24:172:2;
}
```

Перезагружаем службу dhcpd6

systemctl restart dhcpd6
Copy
Отключаем и включаем сетевой интерфейс на HQ-R и HQ-SRV и проверяем:

```
[hq-s@hq-s ~]$ ip -c 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:8b:92:94 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.100.10/26 brd 172.16.100.63 scope global dynamic noprefixroute ens33
       valid_lft 28722sec preferred_lft 28722sec
    inet6 fd24:172::2/128 scope global dynamic noprefixroute
       valid_lft 2591924sec preferred_lft 604724sec
    inet6 fe80::70dc:c38e:b71e:ecfb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[hq-s@hq-s ~]$
```

Установка и настройка RA (Router Advertisement)

Шлюз на HQ-SRV для IPv4 раздается автоматически , за это отвечает параметр option routers в настройках dhcpd.conf
Для IPv6 такого параметра нет, шлюзы IPv6 выдаются маршрутизаторами средствами RA (Router Advertisement)
Установку и настройку RA производим на HQ-R
Установливаем пакет radvd:
apt-get install -y radvd

Заходим в файл /etc/sysctl.conf
nano /etc/sysctl.conf

Добавляем строку
net.ipv6.conf.enp0s8.accept_ra=2

Открываем файл конфигурации radvd. По умолчанию находится в /etc/radvd.conf:
nano /etc/radvd.conf

Приводим его к следующему виду:

```
#auto generated by alterator-dhcp-reset

interface ens34 {
        AdvSendAdvert on;
        AdvManagedFlag on;
        AdvOtherConfigFlag on;
        prefix fd24:172::/122 {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
        };
};
```

Параметр prefix – прописываем свои параметры
Перезапускаем dhcpd6.service
systemctl restart dhcpd6

Запускаем и добавляем в автозагрузку radvd:
systemctl enable --now radvd

Настройка на HQ-SRV

Через nmtui изменяем режим КОНФИГУРАЦИЯ IPv6 с <Автоматически (только DHCP)> на <Автоматически>
Отключаем и включаем сетевой интерфейс на HQ-R и HQ-SRV и проверяем

Проверка

IPv4

```
[root@hq-s ~]#
[root@hq-s ~]# ip -c a show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:8b:92:94 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.100.10/26 brd 172.16.100.63 scope global dynamic noprefixroute ens33
       valid_lft 28719sec preferred_lft 28719sec
    inet6 fd24:172::2/128 scope global dynamic noprefixroute
       valid_lft 2591920sec preferred_lft 604720sec
    inet6 fe80::70dc:c38e:b71e:ecfb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@hq-s ~]#
[root@hq-s ~]# ip -c route
default via 172.16.100.1 dev ens33 proto dhcp src 172.16.100.10 metric 100
172.16.100.0/26 dev ens33 proto kernel scope link src 172.16.100.10 metric 100
[root@hq-s ~]#
[root@hq-s ~]# ping -c4 172.16.100.1
PING 172.16.100.1 (172.16.100.1) 56(84) bytes of data.
64 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=0.850 ms
64 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=0.783 ms
64 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=0.925 ms
64 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.696 ms

--- 172.16.100.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3064ms
rtt min/avg/max/mdev = 0.696/0.813/0.925/0.084 ms
[root@hq-s ~]#
```

IPv6

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:8b:92:94 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.100.10/26 brd 172.16.100.63 scope global dynamic noprefixroute ens33
       valid_lft 28517sec preferred_lft 28517sec
    inet6 fd24:172::2/128 scope global dynamic noprefixroute
       valid_lft 2591718sec preferred_lft 604518sec
    inet6 fe80::70dc:c38e:b71e:ecfb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@hq-s ~]#
[root@hq-s ~]# ip -c -6 route
fd24:172::2 dev ens33 proto kernel metric 100 pref medium
fd24:172::/122 dev ens33 proto ra metric 100 pref medium
fe80::/64 dev ens33 proto kernel metric 1024 pref medium
default via fe80::c2f2:c4c0:103d:8677 dev ens33 proto ra metric 100 pref medium
[root@hq-s ~]#
[root@hq-s ~]# ping -c4 fd24:172::1
PING fd24:172::1(fd24:172::1) 56 data bytes
64 bytes from fd24:172::1: icmp_seq=1 ttl=64 time=0.657 ms
64 bytes from fd24:172::1: icmp_seq=2 ttl=64 time=0.816 ms
64 bytes from fd24:172::1: icmp_seq=3 ttl=64 time=1.22 ms
64 bytes from fd24:172::1: icmp_seq=4 ttl=64 time=0.981 ms

--- fd24:172::1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.657/0.919/1.223/0.209 ms
[root@hq-s ~]#
```

1.4.Настройка локальных учётных записей на всех устройствах в соответствии с таблицей 2.

Таблица №2

Учётная запись	Пароль	Примечание
Admin	P@ssw0rd	CLI HQ-SRV HQ-R
Branch admin	P@ssw0rd	BR-SRV BR-R
Network admin	P@ssw0rd	HQ-R BR-R BR-SRV

Решение

Для добавления нового пользователя используйте команды useradd и passwd.

Параметр -c позволяет добавлять пользовательские комментарии, такие как полное имя пользователя, номер телефона и т. д. в файл /etc/passwd. Комментарий может быть добавлен одной строкой без пробелов.

Команда добавит пользователя «admin» и вставит его полное имя, Administrator, в поле комментария.

useradd -c "Admin" admin -U # passwd admin

admin - имя пользователя

-c Admin любая текстовая строка. Используется как поле для имени и фамилии пользователя

-U - создание группы с тем же именем, что и у пользователя, и добавление пользователь в эту группу

passwd admin - задать пароль пользователю

Если имя пользователя состоит из двух слов – пишется через тире или подчеркивание

Добавление пользователей

HQ-R

useradd -c "Admin" admin -U

passwd admin < вводим пароль пользователя > < повторяем ввод пароля >

Создание пользователя Network admin

useradd -c "Network admin" network_admin -U

passwd network_admin < вводим пароль пользователя > < повторяем ввод пароля >

HQ-SRV

Создание пользователя Admin

useradd -c "Admin" admin -U

passwd admin < вводим пароль пользователя > < повторяем ввод пароля >

BR-R

Создание пользователя Branch admin

useradd -c "Branch admin" branch_admin -U

passwd branch_admin < вводим пароль пользователя > < повторяем ввод пароля >

Создание пользователя Network admin

useradd -c "Network admin" network_admin -U

passwd network_admin < вводим пароль пользователя > < повторяем ввод пароля >

BR-SRV

Создание пользователя Branch admin

useradd -c "Branch admin" branch_admin -U

passwd branch_admin < вводим пароль пользователя > < повторяем ввод пароля >

Создание пользователя Network admin

useradd -c "Network admin" network_admin -U

passwd network_admin < вводим пароль пользователя > < повторяем ввод пароля >

CLI

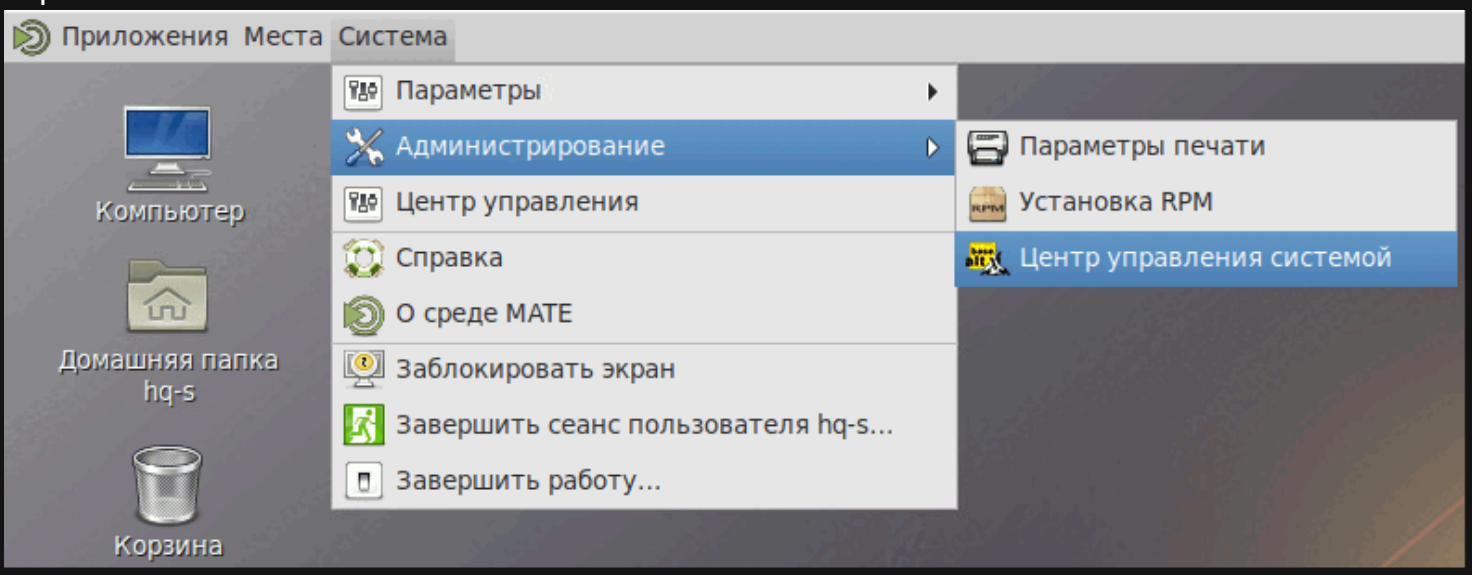
Вариант 1

Создание пользователя Admin

useradd -c "Admin" admin -U

passwd admin < вводим пароль пользователя > < повторяем ввод пароля >

Вариант 2


Приложения
Места
Система
Компьютер
Домашняя папка hq-s
Корзина
Параметры
Администрирование
Центр управления
Справка
О среде MATE
Заблокировать экран
Завершить сеанс пользователя hq-s...
Завершить работу...
Параметры печати
Установка RPM
Центр управления системой

1.5.Измерьте пропускную способность сети между двумя узлами HQ-R-ISP по средствам утилиты iperf 3. Предоставьте описание пропускной способности канала со скриншотами.

Установка утилиты происходит на 2 машинах HQ-R и ISP: одна выступает в роли сервера, другая в роли клиента.

Вывод подсказки о том, как использовать iperf3:
iperf3 -h

Устновка:
apt-get install iperf3 -y

При тестирование пропускной способности одна машина выступает в роли сервера, другая в роли клиента.

Запуск на стороне сервера с ключом -s (машина ISP)
iperf3 -s

Запуск на стороне клиента с ключом -c (машина HQ-R)
iperf3 -c IP_address_ISP

В ходе выполнения команд выполняется 10 секундная передача данных, на основе которых выдается скорость сети.

```
[root@isp ~]# iperf3 -s
-----------------------------------------------------------
Server listening on 5201 (test #1)
-----------------------------------------------------------
Accepted connection from 1.1.1.2, port 37970
[  5] local 1.1.1.1 port 5201 connected to 1.1.1.2 port 37980
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec   410 MBytes  3.44 Gbits/sec
[  5]   1.00-2.00   sec   325 MBytes  2.72 Gbits/sec
[  5]   2.00-3.00   sec   369 MBytes  3.10 Gbits/sec
[  5]   3.00-4.00   sec   218 MBytes  1.83 Gbits/sec
[  5]   4.00-5.00   sec   217 MBytes  1.82 Gbits/sec
[  5]   5.00-6.00   sec   231 MBytes  1.94 Gbits/sec
[  5]   6.00-7.00   sec   289 MBytes  2.43 Gbits/sec
[  5]   7.00-8.00   sec   334 MBytes  2.80 Gbits/sec
[  5]   8.00-9.00   sec   226 MBytes  1.90 Gbits/sec
[  5]   9.00-10.00  sec   212 MBytes  1.79 Gbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec  2.77 GBytes  2.38 Gbits/sec                  receiver
-----------------------------------------------------------
Server listening on 5201 (test #2)
-----------------------------------------------------------
```

```
[root@hq-r dhcp]# iperf3 -c 1.1.1.1
Connecting to host 1.1.1.1, port 5201
[  5] local 1.1.1.2 port 37980 connected to 1.1.1.1 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec   410 MBytes  3.44 Gbits/sec  420    453 KBytes
[  5]   1.00-2.00   sec   326 MBytes  2.74 Gbits/sec  131    406 KBytes
[  5]   2.00-3.00   sec   375 MBytes  3.15 Gbits/sec  251    339 KBytes
[  5]   3.00-4.00   sec   215 MBytes  1.81 Gbits/sec    4    319 KBytes
[  5]   4.00-5.00   sec   217 MBytes  1.82 Gbits/sec    3    282 KBytes
[  5]   5.00-6.00   sec   225 MBytes  1.89 Gbits/sec    3    423 KBytes
[  5]   6.00-7.00   sec   292 MBytes  2.45 Gbits/sec  136    362 KBytes
[  5]   7.00-8.00   sec   334 MBytes  2.80 Gbits/sec  103    338 KBytes
[  5]   8.00-9.01   sec   228 MBytes  1.90 Gbits/sec    7    346 KBytes
[  5]   9.01-10.00  sec   216 MBytes  1.82 Gbits/sec    7    351 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  2.77 GBytes  2.38 Gbits/sec  1065             sender
[  5]   0.00-10.00  sec  2.77 GBytes  2.38 Gbits/sec                  receiver

iperf Done.
[root@hq-r dhcp]#
```

1.6.Составить backup скрипты для сохранения конфигурации сетевых устройств, HQ-R BR-R. Продемонстрируйте их работу.

HQ-R

Создадим простой bash-скрипт резервного копирования всего содержимого директории /etc , конфигурационных файлов FRR, GRE, Nftables, DHCP и настроек сетевых интерфейсов.

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/backup.sh
```

Пример скрипта резервного копирования:

```
#!/bin/bash

echo "Start backup!"

backup_dir="/etc"
dest_dir="/opt/backup"

mkdir -p $dest_dir
tar -czf $dest_dir/$(hostname -s)-$(date +"%d.%m.%y").tgz $backup_dir

echo "Done!"
```

Задаем права скрипту на выполнение:
```
# chmod +x /var/backup-script/backup.sh
```

Запускаем скрипт
```
# /var/backup/backup.sh
```

```
[root@hq-r backup]# chmod +x /var/backup/backup.sh
[root@hq-r backup]# /var/backup/backup.sh
Start backup!
tar: Удаляется начальный `/' из имен объектов
tar: Удаляются начальные `/' из целей жестких ссылок
Done!
[root@hq-r backup]#
```

BR-R

Копируем скрипт с HQ-R на BR-R

Переходим на ВМ BR-R

Создадим директорию для хранения скрипта резервного копирования backup-script и директорию для хранения архивов резервных копий backup
```
# mkdir /var/{backup,backup-script}
```

Забираем с HQ-R backup.sh. Используем IP-адресацию GRE туннеля
```
scp admin@192.168.161.1:/var/backup/backup.sh /var/backup-script/
```

При необходимости задаем права скрипту на выполнение:
```
# chmod +x /var/backup-script/backup.sh
```

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

1.7.Настройте подключение по SSH для удалённого конфигурирования устройства HQ-SRV по порту 2222. Учтите, что вам необходимо перенаправить трафик на этот порт по средствам контролирования трафика.

Настройка подключения

Необходимо изменить порт подключения по SSH с 22 на 2222
В конфигурационном файле /etc/ssh/sshd_config необходимо изменить номер порта
Открываем файл
nano /etc/openssh/sshd_config

Находим строчку Port 22 снимаем комментарий со сроки и изменяем номер порта

```
#       $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 ::
```

Если включен SELinux, то необходимо внести изменения в его политики - разрешить этот порт для работы по нему SSH следующей комавндой: semanage port -a -t ssh_port_t -p tcp 2222
Перезапускаем службу sshd
systemctl restart sshd

Проверить на каком порту работает SSH:
ss -tlpn | grep ssh

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

```
[root@hq-r home]#
[root@hq-r home]#
[root@hq-r home]# ssh admin@172.16.100.10 -p 2222
admin@172.16.100.10's password:
Last login: Mon Jun 10 11:01:12 2024 from 172.16.100.1
[admin@hq-s ~]$
```

Перенаправление

Создаем правило iptables на HQ-R, которое будет перенаправлять внешние подключения к HQ-R на порту 22 -> на порт 2222 сервера HQ-SRV.
Для IPv6 установим пакет iptables-ipv6:
apt-get install -y iptables-ipv6

Добавим цепочку prerouting в таблицу nat
iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 22 -j DNAT --to-destination 172.16.100.10:2222
Примечание
PREROUTING — предназначена для первичной обработки входящих пакетов, адресованных как непосредственно серверу, так и другим узлам сети. Сюда попадает абсолютно весь входящий трафик для дальнейшего анализа.
Проверяем правило
iptables -t nat -L -n -v

```
[root@hq-r ~]# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 1 packets, 68 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  ens33  *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 to:172.16.100.10:2222

Chain INPUT (policy ACCEPT 1 packets, 68 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 3 packets, 260 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 3 packets, 260 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Добавим правило IPv6, через ip6tables

```
# ip6tables -t nat -A PREROUTING -i ens33 -p tcp --dport 22 -j DNAT --to-destination [fd24:172::1]:2222
```

Проверяем правило

```
# ip6tables -t nat -L -n -v
```

```
[root@hq-r ~]# ip6tables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp      ens33  *       ::/0                 ::/0                tcp dpt:22 to:[2024:1::1]:2222

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Сохраняем правила iptables и ip6tables:

iptables:

```
# iptables-save >> /etc/sysconfig/iptables
# systemctl enable --now iptables
```

ip6tables:

```
# ip6tables-save >> /etc/sysconfig/ip6tables
# systemctl enable --now ip6tables
```

Проверка

Подключаемся по SSH с BR-R к HQ-SRV используя внешний IPv4 и IPv6 адрес HQ-R

```
[root@br-r ~]# ssh admin@1.1.1.2
The authenticity of host '1.1.1.2 (1.1.1.2)' can't be established.
ED25519 key fingerprint is SHA256:7VfmL3xiLEEDvszpRs03SNXupq2SUa5A7YqRS6aqDH0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '1.1.1.2' (ED25519) to the list of known hosts.
admin@1.1.1.2's password:
Last login: Mon Jun 10 11:01:32 2024 from 172.16.100.1
[admin@hq-s ~]$ exit
выход
Connection to 1.1.1.2 closed.
[root@br-r ~]#
```

```
[root@hq-r ~]# ssh admin@fd24:172::2 -p 2222
The authenticity of host '[fd24:172::2]:2222 ([fd24:172::2]:2222)' can't be established.
ED25519 key fingerprint is SHA256:CE8gL56+x1XJjVi9HSX3uyYr+FRZ3AUX24KjrsCBXek.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [172.16.100.2]:2222
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[fd24:172::2]:2222' (ED25519) to the list of known hosts.
admin@fd24:172::2's password:
Last login: Sun Apr  7 16:47:13 2024 from 2.2.2.2
[admin@hq-srv ~]$
```

1.8.Настройте контроль доступа до HQ-SRV по SSH со всех устройств, кроме CLI.

Настройка nftables на HQ-SRV ALT server

Установка nftables
```
# apt-get install -y nftables
```

Создаем и открываем файл
```
# mcedit /etc/nftables/nftables.nft
```

Запрещаем подключение CLI к HQ-SRV по IPv4 и IPv6
Добавляем правила, запрещающие доступ по ssh (порт 2222) с CLI, как с временного подключения так и с глобального, как для IPv4 так и для IPv6:
```
# nft add rule inet filter input ip saddr 3.3.3.2 tcp dport 2222 counter drop
# nft add rule inet filter input ip6 saddr 2024:3::/64 tcp dport 2222 counter drop
```

Сохраняем правила nftables:
в конфигурационном файле "/etc/nftables/nftables.nft" - удаляем все не закомментированные записи:

Отправляем результат команды "nft list ruleset" - в файл "/etc/nftables/nftables.nft":
```
# nft list ruleset | tee -a /etc/nftables/nftables.nft
```

Запуск и добавление в автозагрузку сервиса nftables
```
# systemctl enable --now nftables
```

Проверка подключение к HQ-SRV по SSH

Подключение с HQ-R

```
[root@hq-s ~]#
[root@hq-s ~]# ssh admin@172.16.100.10 -p 2222
The authenticity of host '[172.16.100.10]:2222 ([172.16.100.10]:2222)' can't be established.
ED25519 key fingerprint is SHA256:7VfmL3xiLEEDvszpRs03SNXupq2SUa5A7YqRS6aqDH0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[172.16.100.10]:2222' (ED25519) to the list of known hosts.
admin@172.16.100.10's password:
Last login: Mon Jun 10 11:36:37 2024 from 2.2.2.2
[admin@hq-s ~]$ exit
выход
Connection to 172.16.100.10 closed.
[root@hq-s ~]# ssh admin@fd24:172::2 -p 2222
The authenticity of host '[fd24:172::2]:2222 ([fd24:172::2]:2222)' can't be established.
ED25519 key fingerprint is SHA256:7VfmL3xiLEEDvszpRs03SNXupq2SUa5A7YqRS6aqDH0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[fd24:172::2]:2222' (ED25519) to the list of known hosts.
admin@fd24:172::2's password:
Last login: Mon Jun 10 13:11:35 2024 from 172.16.100.10
[admin@hq-s ~]$ exit
выход
Connection to fd24:172::2 closed.
[root@hq-s ~]#
```

Подключение с BR-R

```
[root@br-r .ssh]# ssh admin@1.1.1.2
The authenticity of host '1.1.1.2 (1.1.1.2)' can't be established.
ED25519 key fingerprint is SHA256:AQUtC6WgQc+PJRYwIoGUyxKMRiU2yWZv/pyZBXFAi/E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '1.1.1.2' (ED25519) to the list of known hosts.
admin@1.1.1.2's password:
Last login: Mon Jun 10 11:25:44 2024 from 1.1.1.1
[admin@hq-r ~]$ exit
выход
Connection to 1.1.1.2 closed.
[root@br-r .ssh]#
```

Подключение с BR-SRV

```
[root@br-srv ~]# ssh admin@1.1.1.2
The authenticity of host '1.1.1.2 (1.1.1.2)' can't be established.
ED25519 key fingerprint is SHA256:CE8gL56+x1XJjVi9HSX3uyYr+FRZ3AUXZ4KjrsCBXek.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '1.1.1.2' (ED25519) to the list of known hosts.
admin@1.1.1.2's password:
Last login: Sun Apr  7 16:59:40 2024 from 2.2.2.2
[admin@hq-srv ~]$ exit
выход
Connection to 1.1.1.2 closed.
[root@br-srv ~]# _
```

Подключение с CLI

```
[user@cli ~]$ ssh admin@4.4.4.1 -p 2222
ssh: connect to host 4.4.4.1 port 2222: Connection refused
[user@cli ~]$ ssh admin@2024:4::1 -p 2222
ssh: connect to host 2024:4::1 port 2222: Connection refused
[user@cli ~]$
```

2.1.Настройте DNS-сервер на сервере HQ-SRV

1. Настройте DNS-сервер на сервере HQ-SRV:
   a. На DNS сервере необходимо настроить 2 зоны, также не забудьте настроить обратную зону

Зона hq.work

Имя	Тип записи	Адрес
hq-r.hq.work	A, PTR	IP-адрес
hq-srv.hq.work	A, PTR	IP-адрес

Зона branch.work

Имя	Тип записи	Адрес
br-r.branch.work	A, PTR	IP-адрес
br-srv.branch.work	A	IP-адрес

Перед установкой и настройкой DNS и IPA желательно произвести настройку NTP

Установка и запуск DNS-сервера

Устанавливаем пакеты bind и bind-utils:
apt-get install -y bind bind-utils

В конфигурационном файле /etc/bind/options.conf - правим следующие параметры:
mcedit /etc/bind/options.conf

- listen-on параметр определяет адреса и порты, на которых DNS-сервер будет слушать запросы. Значение any означает, что сервер будет прослушивать запросы на всех доступных интерфейсах и IP-адресах (IPv4 | IPv6);
- в параметре forwarders указать сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне;
- раскомментировать параметр allow-query и указать в нём подсети из которых разрешено подавать запросы;

```
options {
        version "unknown";
        directory "/etc/bind/zone";
        dump-file "/var/run/named_dump.db";
        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; };

        /*
         * If the forward directive is set to "only", the server will only
         * query the forwarders.
         */
        forward first;
        forwarders { 10.104.1.100 };

        /*
         * Specifies which hosts are allowed to ask ordinary questions.
         */
        allow-query { any; };
```

Запускаем и добавляем в автозагрузку службу bind:
systemctl enable --now bind

В конфигурационной файле /etc/bind/local.conf описываем необходимые зоны согласно требованию задания:

- hq.work - зона прямого просмотра;
- branch.work - зона прямого просмотра;
- 100.168.192.in-addr.arpa - зона обратного просмотра;
- 200.168.192.in-addr.arpa - зона обратного просмотра;

```
include "/etc/bind/rfc1912.conf";

// Consider adding the 1918 zones here,
// if they are not used in your organization.
//<---->include "/etc/bind/rfc1918.conf";

// Add other zones here

zone "hq.work" {
<------>type master;
<------>file "hq.db";
};
zone "branch.work" {
<------>type master;
<------>file "branch.db";
};
zone "100.16.172.in-addr.arpa" {
<------>type master;
<------>file "172.db";
};
zone "100.168.192.in-addr.arpa" {
<------>type master;
<------>file "192.db";
};
```

Примеры файлов зон прямого и обратного просмотра расположены по пути /etc/bind/zone:
Копируем примеры файлов для зон прямого просмотра:
cp /etc/bind/zone/{localdomain,hq.db} cp /etc/bind/zone/{localdomain,branch.db}
Copy
Копируем примеры файлов для зон обратного просмотра:
cp /etc/bind/zone/{127.in-addr.arpa,172.db} cp /etc/bind/zone/{127.in-addr.arpa,192.db}
Copy
Задаём необходимые права:
chown root:named /etc/bind/zone/{hq,branch,100,200}.db
Copy
Правим файл зоны прямого просмотра для hq.work:
mcedit /etc/bind/zone/hq.db
Copy
приводим файл к следующему виду - добавляя записи типа A для зоны hq.work:

```
$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       172.16.100.1
hq-srv  IN      A       172.16.100.2
```

Правим файл зоны прямого просмотра для branch.work:
mcedit /etc/bind/zone/branch.db
Copy
приводим файл к следующему виду - добавляя записи типа A для зоны branch.work:

```
$TTL    1D
@       IN      SOA     branch.work. root.branch.work. (
                                2024021400      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
        IN      NS      branch.work.
        IN      A       127.0.0.0
br-r    IN      A       192.168.100.1
br-srv  IN      A       192.168.100.10
```

Правим файл зоны обратного просмотра для hq.work - "172.db":
mcedit /etc/bind/zone/100.db
Copy
приводим файл к следующему виду - добавляя записи типа PTR:

```
$TTL    1D
@       IN      SOA     hq.work. root.hq.work. (
                                2024021400      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
        IN      NS      hq.work.
1       IN      PTR     hq-r.hq.work.
2       IN      PTR     hq-srv.hq.work.
```

Правим файл зоны обратного просмотра для branch.work - "192.db":
mcedit /etc/bind/zone/200.db
Copy
приводим файл к следующему виду - добавляя записи типа PTR:

```
$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.
```

Проверить файлы зон можно утилитой named-checkconf:
named-checkconf -z
Copy

```
[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
hq.db:12: file does not end with newline
zone hq.work/IN: loaded serial 2024021400
zone branch.work/IN: loaded serial 2024021400
zone 100.16.172.in-addr.arpa/IN: loaded serial 2024021400
zone 100.168.192.in-addr.arpa/IN: loaded serial 2024021400
[root@hq-srv ~]#
```

Перезапускаем службу bind:
systemctl restart bind
Copy

```
[root@hq-srv ~]# systemctl restart bind
[root@hq-srv ~]# systemctl status bind.service
● bind.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/lib/systemd/system/bind.service; enabled; vendor preset: disabled)
     Active: active (running) since Wed 2024-05-22 23:00:36 +05; 10s ago
    Process: 4815 ExecStartPre=/etc/init.d/bind rndc_keygen (code=exited, status=0/SUCCESS)
    Process: 4819 ExecStartPre=/usr/sbin/named-checkconf $CHROOT -z /etc/named.conf (code=exited, status=0/SUCCESS)
    Process: 4820 ExecStart=/usr/sbin/named -u named $CHROOT $RETAIN_CAPS $EXTRAOPTIONS (code=exited, status=0/SUCCESS)
      Tasks: 8 (limit: 2340)
     Memory: 18.4M
        CPU: 99ms
     CGroup: /system.slice/bind.service
             └─ 4822 /usr/sbin/named -u named

мая 22 23:00:36 hq-srv.hq.work named[4822]: hq.db:12: file does not end with newline
мая 22 23:00:36 hq-srv.hq.work named[4822]: zone hq.work/IN: loaded serial 2024021400
мая 22 23:00:36 hq-srv.hq.work named[4822]: zone hq.work/IN: sending notifies (serial 2024021400)
мая 22 23:00:36 hq-srv.hq.work named[4822]: zone 255.in-addr.arpa/IN: loaded serial 2024021400
мая 22 23:00:36 hq-srv.hq.work named[4822]: zone branch.work/IN: loaded serial 2024021400
мая 22 23:00:36 hq-srv.hq.work named[4822]: all zones loaded
мая 22 23:00:36 hq-srv.hq.work named[4822]: running
мая 22 23:00:36 hq-srv.hq.work systemd[1]: Started Berkeley Internet Name Domain (DNS).
мая 22 23:00:36 hq-srv.hq.work named[4822]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
мая 22 23:00:46 hq-srv.hq.work named[4822]: resolver priming query complete
```

Проверяем:

зона hq.work:

```
[root@hq-srv ~]# host hq-r.hq.work
hq-r.hq.work has address 172.16.100.1
[root@hq-srv ~]# host hq-srv.hq.work
hq-srv.hq.work has address 172.16.100.2
[root@hq-srv ~]# host 172.16.100.1
1.100.16.172.in-addr.arpa domain name pointer hq-r.hq.work.
[root@hq-srv ~]# host 172.16.100.2
2.100.16.172.in-addr.arpa domain name pointer hq-srv.hq.work.
[root@hq-srv ~]#
```

зона branch.work:

```
[root@hq-srv ~]# host br-r.branch.work
br-r.branch.work has address 192.168.100.1
[root@hq-srv ~]# host br-srv.branch.work
br-srv.branch.work has address 192.168.100.10
[root@hq-srv ~]# host 192.168.100.1
1.100.168.192.in-addr.arpa domain name pointer br-r.branch.work.
[root@hq-srv ~]#
```