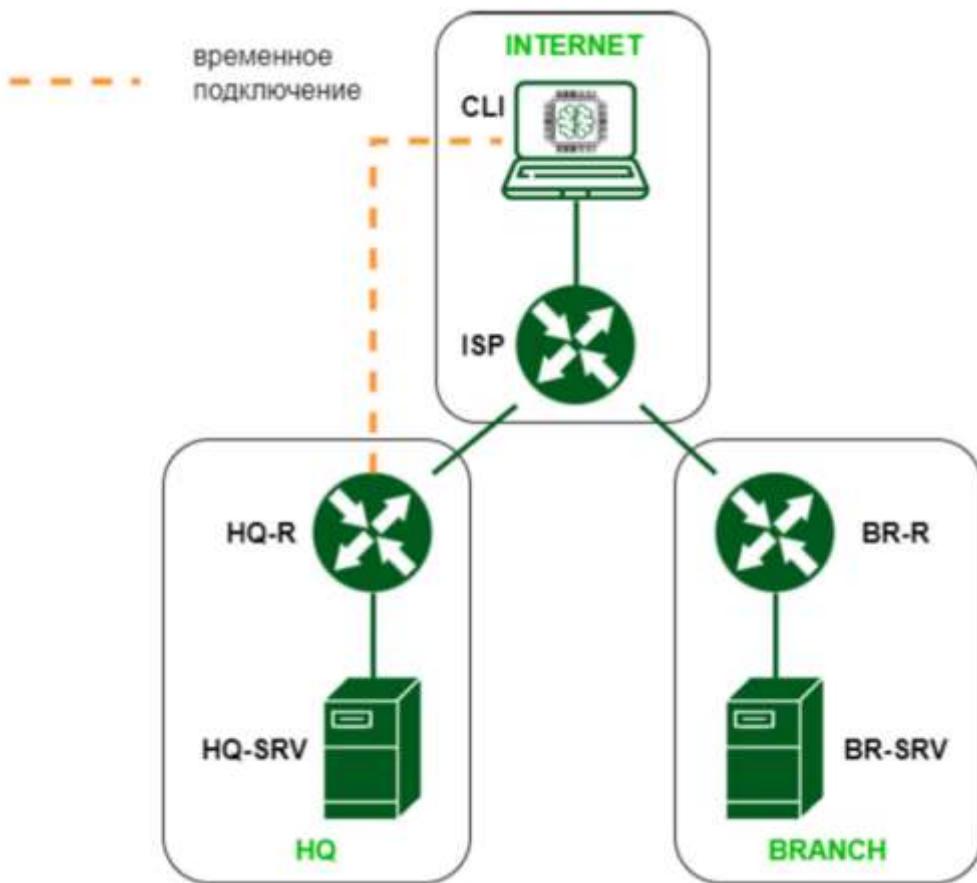


1.1. Выполните базовую настройку всех устройств

Задание

Топология



1. Выполните базовую настройку всех устройств:

- Присвоить имена в соответствии с топологией
- Рассчитать IP-адресацию IPv4 и IPv6. Необходимо заполнить таблицу №1, чтобы эксперты могли проверить ваше рабочее место.
- Пул адресов для сети офиса BRANCH - не более 16
- Пул адресов для сети офиса HQ - не более 64

Таблица №1

Имя устройства	IP
CLI	
ISP	
HQ-R	
HQ-SRV	
BR-R	
BR-SRV	
HQ-CLI	
HQ-AD	

Решение

Таблица IP-адресов

IP – адреса ВМ

Hostname	Interface	IPv4	Gateway IPv4	IPv6	Gateway IPv6	Network
ISP	ens18	DHCP	DHCP	-	-	WAN
	ens19	1.1.1.1/30	-	2024:1::1/64	-	ISP-HQ_R
	ens20	3.3.3.1/30	-	2024:3::1/64	-	ISP-CLI
	ens21	2.2.2.1/30	-	2024:2::1/64	-	ISP-BR_R
HQ_R	ens18	1.1.1.2/30	1.1.1.1	2024:1::2/64	2024:1::1	ISP-HQ_R
	ens19	172.16.100.1/26	-	FD24:172::1/122	-	HQ_R-HQ_SRV
	ens20 [временное подключение]	4.4.4.1/30	-	2024:4::1/64	2024:4::2	CLI-HQ_R
	gre	10.10.10.1/30	-	FD24:10::1/64	-	HQ_R-BR_R
BR_R	ens18	2.2.2.2/30	2.2.2.1	2024:2::2/64	2024:2::1	ISP-BR_R
	ens19	192.168.100.1/28	-	FD24:192::1/124	-	BR_R-BR_SRV
	gre	10.10.10.2/30	-	FD24:10::2/64	-	HQ_R-BR_R
HQ_SRV	ens18	172.16.100.2/26 (DHCP)	172.16.100.1	FD24:172::2/122 (DHCP)	FD24:172::1	HQ_R-HQ_SRV
BR_SRV	ens18	192.168.100.10/28	192.168.100.1	FD24:192::10/124	FD24:192::1	BR_R-BR_SRV
CLI	ens18	3.3.3.2/30	3.3.3.1	2024:3::2/64	2024:3::1	ISP-CLI
	ens20 [временное подключение]	4.4.4.2/30	4.4.4.1	2024:4::2/64	2024:4::1	CLI-HQ_R

а. Присвоить имена в соответствии с топологией



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

```
1 | [root@localhost ~]# hostnamectl set-hostname <NAME>
2 | [root@localhost ~]# exec bash
```

NAME - имя устройства

exec bash – перезапуск оболочки bash для отображения нового хостнейма

Для устройств *BR-SRV* и *CLI* желательно сразу установить полное доменное имя.
Потребуется для ввода этих машин в домен во второй части задания.



Например:

ISP: isp
CLI: cli.hq.work
HQ-R: hq-r.hq.work
HQ-SRV: hq-srv.hq.work
BR-R: br-r.branch.work
BR-SRV: br-srv.branch.work

Пример:

```
[root@localhost ~]#  
[root@localhost ~]# hostnamectl set-hostname isp  
[root@localhost ~]# exec bash  
[root@isp ~]# _
```

b. Рассчитать IP-адресацию IPv4 и IPv6. Необходимо заполнить таблицу №1, чтобы эксперты могли проверить ваше рабочее место.

[см Таблица IP-адресов](#)

c. Пул адресов для сети офиса BRANCH - не более 16



Для пула адресов IPv4 не более 16 - маска подсети /28



Для пула адресов IPv6 не более 16 - длина префикса /124

d. Пул адресов для сети офиса HQ - не более 64



Для пула адресов IPv4 не более 64 - маска подсети /26



Для пула адресов IPv6 не более 64 - длина префикса /122

Настройка сетевых интерфейсов

ISP

Определяемся менем интерфейсов и какой интерфейс в какую сторону смотрит

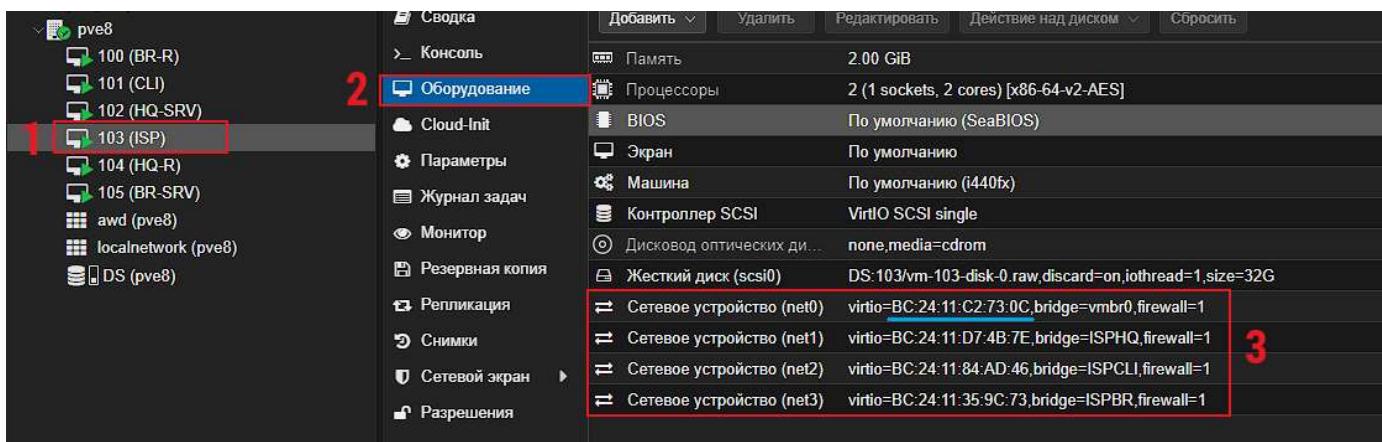
Выводим информацию о сетевых интерфейсах:

```
1 | # ip -c a
```

```
[root@isp ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:c2:73:0c brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.1.39.209/24 brd 10.1.39.255 scope global dynamic noprefixroute ens18
        valid_lft 11912sec preferred_lft 11912sec
    inet6 fe80::bc24:11ff:ec2:730c/64 scope global dynamic noprefixroute
        valid_lft 2591882sec preferred_lft 604682sec
    inet6 fe80::bc24:11ff:fe2:730c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:d7:4b:7e brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet6 fe80::bc24:11ff:fe7d:4b7e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: ens20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:84:ad:46 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
    inet6 fe80::bc24:11ff:fe84:ad46/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
5: ens21: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:35:9c:73 brd ff:ff:ff:ff:ff:ff
    altname enp0s21
    inet6 fe80::bc24:11ff:fe35:9c73/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@isp ~]#
```

Открываем настройки виртуальной машины

1. Выбираем необходимую виртуальную машину
2. Выбираем **Оборудование**
3. Смотрим **MAC-адрес** сетевых интерфейсов, и запоминаем их (лучше записать на черновик)



⚠️ Аналогично смотрим для других сетевых интерфейсов и виртуальных машин

💡 Обычно:

- ens18 – Адаптер 1
- ens19 – Адаптер 2
- ens20 – Адаптер 3
- ens21 – Адаптер 4



С помощью утилиты `nmtui` задаем IP адреса сетевым интерфейсам

Результаты настройки сетевых интерфейсов

ISP

В данном примере получаем:

- **ens18** – WAN интерфейс (в Интернет);
- **ens19** - интерфейс в сторону офиса **HQ**;
- **ens20** - интерфейс в сторону **CLI**;
- **ens21** - интерфейс в сторону офиса **Branch**;

```
[root@isp ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:c2:73:0c brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.1.39.209/24 brd 10.1.39.255 scope global dynamic noprefixroute ens18
        valid_lft 14130sec preferred_lft 14130sec
    inet6 fe80::bc24:11ff:fedc:730c/64 scope global dynamic noprefixroute
        valid_lft 2591895sec preferred_lft 604695sec
    inet6 fe80::bc24:11ff:fedc:730c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:d7:4b:7e brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 1.1.1.1/30 brd 1.1.1.3 scope global noprefixroute ens19
        valid_lft forever preferred_lft forever
    inet6 fe80::bc24:11ff:fed7:4b7e/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::bc24:11ff:fed7:4b7e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: ens20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:84:ad:46 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
    inet 3.3.3.1/30 brd 3.3.3.3 scope global noprefixroute ens20
        valid_lft forever preferred_lft forever
    inet6 fe80::bc24:11ff:fe84:ad46/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::bc24:11ff:fe84:ad46/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
5: ens21: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:35:9c:73 brd ff:ff:ff:ff:ff:ff
    altname enp0s21
    inet 2.2.2.1/30 brd 2.2.2.3 scope global noprefixroute ens21
        valid_lft forever preferred_lft forever
    inet6 fe80::bc24:11ff:fe35:9c73/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::bc24:11ff:fe35:9c73/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@isp ~]#
```

MAC - адреса

Имена интерфейсов

HQ-R

В данном примере для HQ-R:

- **ens18** - интерфейс в сторону **ISP**;
- **ens19** - интерфейс в сторону офиса **HQ**;

- ens20 - интерфейс в сторону **CLI** (временное подключение);

```
[root@hq-r ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:7e:3a:d3 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
        inet 1.1.1.2/30 brd 1.1.1.3 scope global noprefixroute ens18
            valid_lft forever preferred_lft forever
        inet6 fe80::bc24:11ff:fe7e:3ad3/64 scope global noprefixroute
            valid_lft forever preferred_lft forever
        inet6 2001:ad18:1:2/64 scope global noprefixroute
            valid_lft forever preferred_lft forever
        inet6 fe80::bc24:11ff:fe7e:3ad3/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:bf:03:48 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
        inet 172.16.100.1/26 brd 172.16.100.63 scope global noprefixroute ens19
            valid_lft forever preferred_lft forever
        inet6 fe80::bc24:11ff:febf:48/122 scope global noprefixroute
            valid_lft forever preferred_lft forever
        inet6 fe80::bc24:11ff:febf:48/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
4: ens20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:9c:6a:49 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
        inet 4.4.4.1/30 brd 4.4.4.3 scope global noprefixroute ens20
            valid_lft forever preferred_lft forever
        inet6 fe80::bc24:11ff:fe9c:6a49/64 scope global noprefixroute
            valid_lft forever preferred_lft forever
        inet6 fe80::bc24:11ff:fe9c:6a49/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
[root@hq-r ~]#
```

HQ-SRV

Получает IP адрес по DHCP от HQ-R. Настройка описана ниже.

В данном примере для HQ-SRV:

- ens18 - интерфейс в сторону офиса **HQ**;

 Режим КОНФИГУРАЦИЯ IPv4 <Автоматически>

Изменяем режим КОНФИГУРАЦИЯ IPv6 с <Автоматически> на <Автоматически (только DHCP)>

BR-R

В данном примере для HQ-R:

- ens18 - интерфейс в сторону **ISP**;
- ens19 - интерфейс в сторону офиса **Branch**;

```
[root@br-r ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inets6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:23:72:e4 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 2.2.2.2/30 brd 2.2.2.3 scope global noprefixroute ens18
        valid_lft forever preferred_lft forever
    inets6 ::/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inets6 fe80::bc24:11ff:fe23:72e4/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:23:03:6f brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.100.1/28 brd 192.168.100.15 scope global noprefixroute ens19
        valid_lft forever preferred_lft forever
    inets6 ::/124 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inets6 fe80::bc24:11ff:fe03:6f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@br-r ~]# _
```

BR-SRV

BR-SRV - 1 интерфейс в сторону BR-R

```
[root@br-srv ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inets6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:6e:d4:7c brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.100.10/28 brd 192.168.100.15 scope global noprefixroute ens18
        valid_lft forever preferred_lft forever
    inets6 ::/124 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inets6 fe80::bc24:11ff:fe6e:d47c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@br-srv ~]# _
```

CLI

Настройка интерфейса CLI_ISP

Изменение ens18

Адреса		
Адрес	Маска сети	Шлюз
3.3.3.2	30	3.3.3.1

Требовать адресацию IPv4 для этого соединения

Изменение ens18

Адреса		
Адрес	Префикс	Шлюз
2024:3::2	64	2024:3::1

Требовать адресацию IPv6 для этого соединения

Настройка интерфейса HQ-R_CLI (временное соединение)

Настраивается аналогично **CLI_ISP**

root@redos:~

Файл Правка Вид Поиск Терминал Помощь

```
[root@cli ~]# 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:be:ed:9c brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 3.3.3.2/30 brd 3.3.3.3 scope global noprefixroute ens18
        valid_lft forever preferred_lft forever
    inet6 2024:3::2/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::21be:edff:fe24:11ff/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:d5:e2:fc brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 4.4.4.2/30 brd 4.4.4.3 scope global noprefixroute ens19
        valid_lft forever preferred_lft forever
    inet6 2024:4::2/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::21be:e9ff:fe24:d5e2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@cli ~]#
```

Powered by [Wiki.js](#)

Настройка доступа в интернет

Настройка доступа в интернет

Маршрутизация транзитных IP-пакетов



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

Чтобы включить пересылку пакетов между интерфейсами, необходимо отредактировать файл `sysctl.conf`

```
1 | # nano /etc/sysctl.conf
```

В данном файле прописываем следующие строки:

```
1 | net.ipv4.ip_forward=1  
2 |  
3 | net.ipv6.conf.all.forwarding=1
```

После необходимо применить внесенные изменения:

```
1 | # sysctl -p
```



Необходимо предоставить доступ в сеть **Интернет** для всех устройств предложенных в демо-экзамене для установки необходимых пакетов. Для этого необходимо настроить **Nftables** на устройствах ISP, HQ-R и BR-R



Nftables - подсистема ядра Linux, обеспечивающая фильтрацию и классификацию сетевых пакетов/датаграмм/кадров.

Настройка nftables на ISP



Данная настройка позволит получить доступ к сети Интернет с HQ-R и BR-R

Установка nftables

Перед установкой необходимо убедиться что имеется доступ в интернет с BM ISP

```
1 | ping -c4 ya.ru
```

Если ping проходит успешно то устанавливаем nftables

```
1 | # dnf install -y nftables
```

Настройка nftables

По умолчанию создаются несколько примеров файлов для работы с `nftables` в директории `/etc/nftables/`.

Настройка с использованием собственного файла настроек

Можно не использовать ни один из файлов примеров, а написать свой.

Создаем и открываем файл

```
1 | # nano /etc/nftables/isp.nft
```

Прописываем следующие строки

```
1 | table inet my_nat {  
2 |     chain my_masquerade {  
3 |         type nat hook postrouting priority srcnat;  
4 |         oifname "ens18" masquerade  
5 |     }  
6 | }
```

где `ens18` - публичный интерфейс ISP (смотрящий в Интернет)

Затем необходимо включить использование данного файла в `sysconfig`, по умолчанию `nftables` не читает ни один из конфигурационных файлов в `/etc/nftables`

```
1 | # nano /etc/sysconfig/nftables.conf
```

Ниже строки начинающейся на `include` , прописываем строку

```
1 | include "/etc/nftables/isp.nft"
```

Запуск и добавление в автозагрузку сервиса `nftables`

```
1 | # systemctl enable --now nftables
```



При успешной и правильной настройке машины HQ-R и BR-R получат выход в Интернет



На устройствах **HQ-R** и **BR-R** необходимо произвести настройку **Nftables** аналогичным способом для доступа HQ-SRV и BR-SRV к сети Интернет

Настройка nftables на HQ-R

Установка nftables

```
1 | # dnf install -y nftables
```

Создаем и открываем файл

```
1 | # nano /etc/nftables/hq-r.nft
```

Прописываем следующие строки

```
1 | table inet my_nat {  
2 |     chain my_masquerade {  
3 |         type nat hook postrouting priority srcnat;  
4 |         oifname "ens18" masquerade  
5 |     }  
6 | }
```

Включаем использование данного файла в `sysconfig`

```
1 | # nano /etc/sysconfig/nftables.conf
```

Ниже строки начинающейся на `include` , прописываем строку

```
1 | include "/etc/nftables/hq-r.nft"
```

Запуск и добавление в автозагрузку сервиса `nftables`

```
1 | # systemctl enable --now nftables
```

Настройка nftables на BR-R

Установка nftables

```
1 | # dnf install -y nftables
```

Создаем и открываем файл

```
1 | # nano /etc/nftables/br-r.nft
```

Прописываем следующие строки

```
1 | table inet my_nat {  
2 |     chain my_masquerade {  
3 |         type nat hook postrouting priority srcnat;  
4 |         oifname "ens18" masquerade  
5 |     }  
6 | }
```

Включаем использование данного файла в `sysconfig`

```
1 | # nano /etc/sysconfig/nftables.conf
```

Ниже строки начинающейся на `include` , прописываем строку

```
1 | include "/etc/nftables/br-r.nft"
```

Запуск и добавление в автозагрузку сервиса `nftables`

```
1 | # systemctl enable --now nftables
```

1.2. Настройка внутренней динамической маршрутизации по средствам FRR.

Задание

2. Настроить внутреннюю динамическую маршрутизацию по средствам FRR. Выбрать и обосновать выбор протокола динамической маршрутизации из расчёта, что в дальнейшем сеть будет масштабироваться.

- ▶ а. Составьте топологию сети L3.

Решение

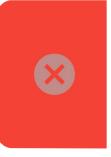
 Маршрутизация внешних сетей по заданию не описана, следовательно, на HQ-R и BR-R достаточно настроить статическую маршрутизацию.

 При настройке IP-адресации в качестве шлюза задать соответствующие адреса маршрутизатора ISP

 Необходимо связать **HQ-R** и **BR-R** туннелем. Обмен между внутренними сетями должен происходить строго между маршрутизаторами **HQ** и **BRANCH**. **ISP** не должен иметь к ним прямого доступа.

Достаточно реализовать простой GRE туннель

GRE-туннель между HQ-R и BR-R

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

Настройка HQ-R

Так как в РЕД ОС используется NetworkManager - следовательно переходим в nmcli:

```
1 | # nmtui
```

Производим настройку

- ▶ Выбираем «Изменить подключение»
- ▶ Выбираем «Добавить»
- ▶ Выбираем «IP-туннель»
- ▶ Задаём понятные имена «Имя профиля» и «Устройство»
- ▶ «Режим работы» выбираем «GRE»
- ▶ «Родительский» указываем **интерфейс в сторону ISP** (ens18)
- ▶ Задаём «Локальный IP» (IP на интерфейсе HQ-R в сторону IPS)
- ▶ Задаём «Удалённый IP» (IP на интерфейсе BR-R в сторону ISP)
- ▶ Переходим к «КОНФИГУРАЦИЯ IPv4»
- ▶ Задаём **адрес IPv4** для туннеля
- ▶ Переходим к «КОНФИГУРАЦИЯ IPv6»
- ▶ Задаём адрес **IPv6** для туннеля
- ▶ Активируем интерфейс **tun1**



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

```
1 | # nmcli connection modify tun1 ip-tunnel.ttl 64
```

Проверяем:

```
1 | 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 brd 0.0.0.0 scope host lo
        valid_lft forever preferred_lft forever
    inetc6 ::1/128 brd 0.0.0.0 scope host
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:7e:3a:d3 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 1.1.1.2/30 brd 1.1.1.3 scope global noprefixroute ens18
        valid_lft forever preferred_lft forever
    inetc6 ::1/64 brd ::/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inetc6 2001:db8::1/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inetc6 fe80::bc24:11ff:fe7e:3ad3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:b1:03:48 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 172.16.100.1/26 brd 172.16.100.63 scope global noprefixroute ens19
        valid_lft forever preferred_lft forever
    inetc6 ::1/122 brd ::/122 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inetc6 fe80::bc24:11ff:fe03:48/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: ens20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:9e:6a:49 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
    inet 4.4.4.1/30 brd 4.4.4.3 scope global noprefixroute ens20
        valid_lft forever preferred_lft forever
    inetc6 ::1/64 brd ::/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inetc6 fe80::bc24:44ff:fe9e:6a49/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
5: gredNONE: <NOARP> mtu 1476 qdisc noop state DOWN group default qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
6: gretapNONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
7: erspanNONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
10: tun@ens18: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default qlen 1000
    link/tun 1.1.1.2 peer 2.2.2.2
    inet 10.10.10.3/30 brd 10.10.10.3 scope global noprefixroute tun1
        valid_lft forever preferred_lft forever
    inetc6 ::1/64 brd ::/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inetc6 fe80::d09c:37ff%tun1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

lroot@hq-r ~#

Настройка BR-R



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

```
1 | # nmcli
```

Производим настройку

- ▶ Выбираем «Изменить подключение»
- ▶ Выбираем «Добавить»
- ▶ Выбираем «IP-туннель»
- ▶ Задаём понятные имена «Имя профиля» и «Устройство»
- ▶ «Режим работы» выбираем «GRE»
- ▶ «Родительский» указываем интерфейс в сторону ISP (ens18)

- Задаём «**Локальный IP**» (IP на интерфейсе BR-R в сторону IPS)
- Задаём «**Удалённый IP**» (IP на интерфейсе HQ-R в сторону ISP)
- Переходим к «**КОНФИГУРАЦИЯ IPv4**»
- Задаём **адрес IPv4** для туннеля
- Переходим к «**КОНФИГУРАЦИЯ IPv6**»
- Задаём адрес **IPv6** для туннеля
- Активируем интерфейс **tun1**



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 brd 0.0.0.0/8
ens18   UP         1.1.1.2/30 brd 1.1.1.3/24 linklayer brd 1.1.1.2/64
ens19   UP         172.16.100.1/26 brd 172.16.100.255/122 linklayer brd 172.16.100.1/64
ens20   UP         4.4.4.1/30 brd 4.4.4.2/24 linklayer brd 4.4.4.1/64
gre0@NONE DOWN
gretap0@NONE DOWN
erspan0@NONE DOWN
tun1@ens18 UNKNOWN    10.10.10.1/30 brd 10.10.10.2/64 linklayer brd 10.10.10.1/64
[root@hq-r ~]#
[root@hq-r ~]# ping -c4 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=2.37 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.935 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=64 time=1.27 ms
--- 10.10.10.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.935/1.422/2.373/0.561 ms
[root@hq-r ~]# ping -c4 fd24:10::2
PING fd24:10::2(Fd24:10::2) 56 data bytes
64 bytes from fd24:10::2: icmp_seq=1 ttl=64 time=1.28 ms
64 bytes from fd24:10::2: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from fd24:10::2: icmp_seq=3 ttl=64 time=0.931 ms
64 bytes from fd24:10::2: icmp_seq=4 ttl=64 time=1.09 ms
--- fd24:10::2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.931/1.182/1.430/0.188 ms
[root@hq-r ~]#
```

BR-R

```
[root@br-r ~]# ip -c --br a
lo      UNKNOWN    127.0.0.1/8 brd 0.0.0.0/8
ens18   UP         2.2.2.2/30 brd 2.2.2.3/24 linklayer brd 2.2.2.2/64
ens19   UP         192.168.100.1/28 brd 192.168.100.255/124 linklayer brd 192.168.100.1/64
gre0@NONE DOWN
gretap0@NONE DOWN
erspan0@NONE DOWN
tun1@ens18 UNKNOWN    10.10.10.2/30 brd 10.10.10.1/24 linklayer brd 10.10.10.2/64
[root@br-r ~]#
[root@br-r ~]# ping -c4 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.967 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=1.20 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=64 time=0.731 ms
--- 10.10.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.731/1.077/1.410/0.254 ms
[root@br-r ~]# ping -c4 fd24:10::1
PING fd24:10::1(Fd24:10::1) 56 data bytes
64 bytes from fd24:10::1: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from fd24:10::1: icmp_seq=2 ttl=64 time=0.749 ms
64 bytes from fd24:10::1: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from fd24:10::1: icmp_seq=4 ttl=64 time=1.17 ms
--- fd24:10::1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.749/1.107/1.414/0.237 ms
[root@br-r ~]#
```

Настройка динамической (внутренней) маршрутизации средствами FRR

Настройка на HQ-R

Установка пакета frr

```
1 | # dnf 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

```
1 | # 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 (IPv3)

Включаем и добавляем в автозагрузку службу FRR

```
1 | # systemctl enable --now frr
```

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

```
1 | # vtysh
```

Настройки OSPFv2 и OSPFv3 на HQ-R

```
[root@hq-r ~]# vtysh
Hello, this is FRRouting (version 9.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

hq-r# conf t
hq-r(config)# router
router    router-id
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 10.10.10.0/30 area 0
hq-r(config-router)# exit
hq-r(config)# interface tun1
hq-r(config-if)# no ip ospf network broadcast
hq-r(config-if)# no ip ospf passive
hq-r(config-if)# exit
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)# exit
hq-r(config)# interface tun1
hq-r(config-if)# ipv6 ospf6 area 0
hq-r(config-if)# exit
hq-r(config)# interface ens18
hq-r(config-if)# ipv6 ospf6 area 0
hq-r(config-if)# exit
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)#

```

OSPFv2

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 HQ и сеть (GRE-туннеля)
exit - выход из режима конфигурации OSPFv2
туннельный интерфейс **tun1** 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 **tun1** и **enp0s3** добавляем в конфигурацию OSPFv3
do write - сохраняем текущую конфигурацию



Перезапускаем frr

```
1 | # systemctl restart frr
```

Посмотреть текущую конфигурацию можно с помощью следующих команд

```
1 # vtysh  
2  
3 # 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 9.1).  
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 10.10.10.0/30 area 0  
br-r(config-router)# exit  
br-r(config)# interface tun1  
br-r(config-if)# no ip ospf network broadcast  
br-r(config-if)# no ip ospf passive  
br-r(config-if)# exit  
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)# router ospf6  
br-r(config-ospf6)# ospf6 router-id 2.2.2.2  
br-r(config-ospf6)# exit  
br-r(config)# interface tun1  
br-r(config-if)# ipv6 ospf6 area 0  
br-r(config-if)# exit  
br-r(config)# interface ens18  
br-r(config-if)# ipv6 ospf6 area 0  
br-r(config-if)# exit  
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)# _
```

OSPFv2

OSPFv3

Посмотреть текущую конфигурацию можно с помощью следующих команд

```
1 # vtysh  
2  
3 # show running-config
```

Проверка

Получить информацию о соседях и установленных отношениях соседства.

```
1 // для IPv4  
2 # show ip ospf neighbor  
3  
4 // для IP6  
5 # show ipv6 ospf6 neighbor
```

Показать маршруты, полученные от процесса OSPF.

```
1 // для IPv4
2 # show ip route ospf
3
4 // для IPv6
5 # show ipv6 route ospf6
```

HQ-R

```
[root@hq-r ~]# utysh
Hello, this is FRRouting (version 9.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

hq-r# show ip ospf neighbor
Neighbor ID      Pri State          Up Time       Dead Time Address      Interface      RXmtL RqstL DBsmL
192.168.100.1    1 Full/-        1m32s        37.764s 10.10.10.2      tun1:10.10.10.1      0     0     0

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

O  10.10.10.0/30 [110/10] is directly connected, tun1, weight 1, 00:03:47
O  172.16.100.0/26 [110/11] is directly connected, ens19, weight 1, 00:03:47
O>* 192.168.100.0/28 [110/11] via 10.10.10.2, tun1, weight 1, 00:01:34
hq-r#
hq-r#
hq-r# show ipv6 ospf6 neighbor
Neighbor ID      Pri DeadTime      State/IfState      Duration I/F[State]
2.2.2.2         1   00:00:30    Full/PointToPoint   00:01:59 tun1[PointToPoint]
hq-r# show ipv6 route ospf6
Codes: K - kernel route, C - connected, S - static, R - RIPng,
      O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
      v - VNC, V - VNC-Direct, F - PBR, f - OpenFabric,
      > - selected route, * - FIB route, q - queued, r - rejected, b - backup
      t - trapped, o - offload failure

O  2024:1::/64 [110/1] is directly connected, ens18, weight 1, 00:04:19
O>* 2024:2::/64 [110/11] via fe80::fa97:b650:59f0:e4e, tun1, weight 1, 00:02:12
O  fd24:10::/64 [110/10] is directly connected, tun1, weight 1, 00:04:19
hq-r#
```

BR-R

```
[root@br-r ~]# utysh
Hello, this is FRRouting (version 9.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

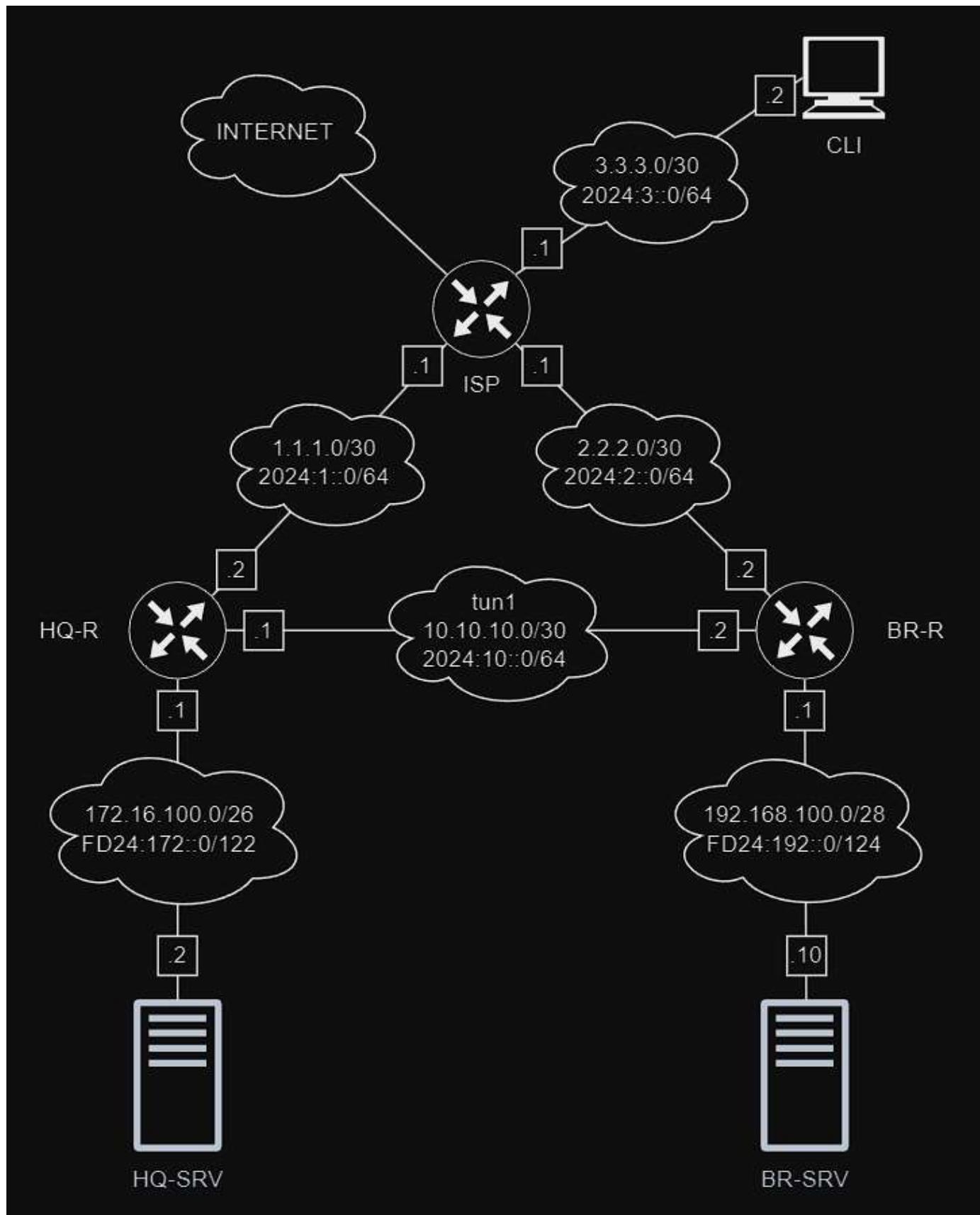
br-r# show ip ospf neighbor
Neighbor ID      Pri State          Up Time       Dead Time Address      Interface      RXmtL RqstL DBsmL
172.16.100.1    1 Full/-        4m50s        36.429s 10.10.10.1      tun1:10.10.10.2      0     0     0

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

O  10.10.10.0/30 [110/10] is directly connected, tun1, weight 1, 00:05:00
O>* 172.16.100.0/26 [110/11] via 10.10.10.1, tun1, weight 1, 00:04:40
O  192.168.100.0/28 [110/11] is directly connected, ens19, weight 1, 00:05:08
br-r#
br-r#
br-r# show ipv6 ospf6 neighbor
Neighbor ID      Pri DeadTime      State/IfState      Duration I/F[State]
1.1.1.1         1   00:00:34    Full/PointToPoint   00:05:13 tun1[PointToPoint]
br-r# show ipv6 route ospf6
Codes: K - kernel route, C - connected, S - static, R - RIPng,
      O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
      v - VNC, V - VNC-Direct, F - PBR, f - OpenFabric,
      > - selected route, * - FIB route, q - queued, r - rejected, b - backup
      t - trapped, o - offload failure

O>* 2024:1::/64 [110/11] via fe80::d69b:377f:9996:1fa6, tun1, weight 1, 00:05:18
O  2024:2::/64 [110/1] is directly connected, ens18, weight 1, 00:05:32
O  fd24:10::/64 [110/10] is directly connected, tun1, weight 1, 00:05:32
br-r# _
```

Топология L3



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

Задание

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

- ▶ а. Учтите, что у сервера должен быть зарезервирован адрес.

Решение

Настройка DHCP на HQ-R для IPv4

Установка DHCP

```
1 | # dnf install 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

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

Подсети обозначаются блоками, пример такого блока представлен ниже:

```
1 subnet 172.16.100.0 netmask 255.255.255.192 {  
2     range 172.16.100.2 172.16.100.62;  
3     option routers 172.16.100.1;  
4     default-lease-time 600;  
5     max-lease-time 7200;  
6 }
```

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`.

```
1 | host HQ-SRV {
2 |     hardware ethernet ff:ff:ff:ff:ff:ff;
3 |     fixed-address 172.16.100.2;
4 | }
```

`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

```
1 | # nano /etc/sysconfig/dhcpd
```

Добавляем в него следующее:

```
1 | DHCPDARGS=ens19
```

где

- `ens19` - интерфейс смотрящий в сторону HQ-SRV

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

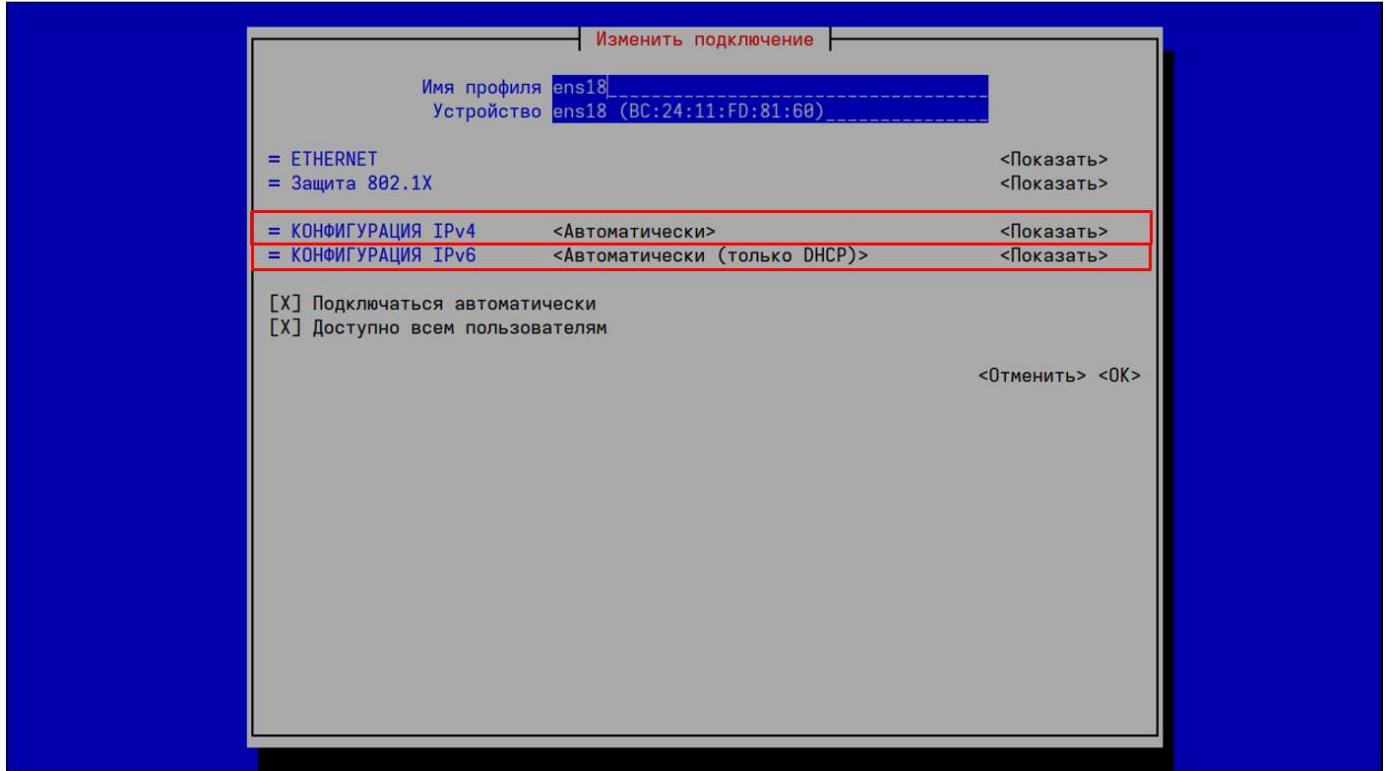
```
1 | # systemctl enable --now dhcpd
```

Проверка на HQ-SRV

Открываем на HQ-SRV настройку сетевых интерфейсов

```
1 | # nmcli
```

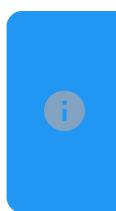
Настраиваем интерфейс на автоматическое получение адресов



Перезагружаем интерфейс и убеждаемся в работоспособности DHCP сервера

```
[root@hq-srv ~]# 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:fd:81:60 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.16.100.2/26 brd 172.16.100.63 scope global dynamic noprefixroute ens18
        valid_lft 443sec preferred_lft 443sec
    inet6 fe80::bc24:11ff:fed:8160/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@hq-srv ~]#
```

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 </usr/share/doc/dhcp-server/dhcpd6.conf.example> в директорию </etc/dhcp/> с именем [dhcpd6.conf](#)

```
[root@hq-r ~]#  
[root@hq-r ~]# mv /etc/dhcp/dhcpd6.conf /etc/dhcp/dhcpd6.conf.bak  
[root@hq-r ~]#  
[root@hq-r ~]# cp /usr/share/doc/dhcp-server/dhcpd6.conf.example /etc/dhcp/dhcpd6.conf  
[root@hq-r ~]#
```

Открываем на редактирование файл конфигурации DHCPv6

```
1 | # 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::/122 {  
    range6 FD24:172::2 FD24:172::12;  
}  
  
#host HQ-SRV {  
#    host-identifier option  
#        dhcp6.client-id 00:04:17:06:02:ee: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;  
#}
```



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`

```
1 | # systemctl enable --now dhcpcd6
```



Перезагружаем сетевой интерфейс на HQ-SRV

Просматриваем журнал и ищем необходимый "DUID" для того, чтобы зарезервировать IPv6 адрес

```
[root@hq ~]# journalctl -f -u dhcpcd6.service
-- Logs begin at Mon 2024-04-01 20:07:04 +05. --
arp 07 15:00:01 hq-r dhcpcd[1164]: Reply NA: address fd24:172::12 to client with duid 00:04:17:06:02:ee:33:c3:7b:49:af:a0:d9:a5:44:b1:67:f1 iaid = -900527782 val id for 2592000 seconds
arp 07 15:00:01 hq-r dhcpcd[1164]: Reusing lease for: fd24:172::12, age 248 secs < 25z, sending shortened lifetimes - preferred: 604552, valid 2591752
arp 07 15:00:01 hq-r dhcpcd[1164]: Sending Reply to fe80::be24:11ff:fedf:8160 port 546
arp 07 15:00:25 hq-r dhcpcd[1164]: Solicit message from fe80::be24:11ff:fedf:8160 port 546, transaction ID 0xA763F900
arp 07 15:00:25 hq-r dhcpcd[1164]: Advertise NA: address fd24:172::12 to client with duid 00:04:17:06:02:ee:33:c3:7b:49:af:a0:d9:a5:44:b1:67:f1 iaid = -900527782 val id for 2592000 seconds
arp 07 15:00:25 hq-r dhcpcd[1164]: Sending Advertise to fe80::be24:11ff:fedf:8160 port 546
arp 07 15:00:25 hq-r dhcpcd[1164]: Request message from fe80::be24:11ff:fedf:8160 port 546, transaction ID 0xB9D8EC00
arp 07 15:00:25 hq-r dhcpcd[1164]: Reply NA: address fd24:172::12 to client with duid 00:04:17:06:02:ee:33:c3:7b:49:af:a0:d9:a5:44:b1:67:f1 iaid = -900527782 val id for 2592000 seconds
arp 07 15:00:25 hq-r dhcpcd[1164]: Reusing lease for: fd24:172::12, age 272 secs < 25z, sending shortened lifetimes - preferred: 604528, valid 2591728
arp 07 15:00:25 hq-r dhcpcd[1164]: Sending Reply to fe80::be24:11ff:fedf:8160 port 546
```

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 dhcpcd6

```
1 | # systemctl restart dhcpcd6
```

Отключаем и включаем сетевой интерфейс на HQ-R и HQ-SRV и проверяем:

```
[root@hq-srv ~]# 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:fd:81:60 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.16.100.2/26 brd 172.16.100.63 scope global dynamic noprefixroute ens18
        valid_lft 581sec preferred_lft 581sec
    inet6 fd24:172::2/128 scope global dynamic noprefixroute
        valid_lft 2591983sec preferred_lft 604783sec
    inet6 fe80::be24:11ff:fedf:8160/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@hq-srv ~]#
```

Установка и настройка RA (Router Advertisement)



Шлюз на HQ-SRV для IPv4 раздается автоматически , за это отвечает параметр option routers в настройках dhcpcd.conf

Для IPv6 такого параметра нет, шлюзы IPv6 выдаются маршрутизаторами средствами RA (Router Advertisement)



Установку и настройку RA производим на HQ-R

Устанавливаем пакет radvd :

```
1 | # dnf install -y radvd
```

Заходим в файл /etc/sysctl.conf

```
1 | # nano /etc/sysctl.conf
```

Добавляем строку

```
1 | net.ipv6.conf.enp0s8.accept_ra=2
```

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

```
1 | nano /etc/radvd.conf
```

Приводим его к следующему виду:

```
# NOTE: there is no such thing as a working "by-default" configuration file.  
#       At least the prefix needs to be specified. Please consult the radvd.conf(5)  
#       man page and/or /usr/share/doc/radvd-*/radvd.conf.example for help.  
#  
#  
interface ens19  
{  
    AdvSendAdvert on;  
    AdvManagedFlag on;  
    AdvOtherConfigFlag on;  
    prefix FD24:172::/122  
    {  
        AdvOnLink on;  
        AdvAutonomous on;  
        AdvRouterAddr on;  
    };  
};
```

Параметр `prefix` – прописываем свои параметры

Перезапускаем `dhcpd6.service`

```
1 | systemctl restart dhcpcd6
```

Запускаем и добавляем в автозагрузку `radvd`:

```
1 | 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-srv ~]# ip -c a show ens18
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:fd:81:60 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.16.100.2/26 brd 172.16.100.63 scope global dynamic noprefixroute ens18
        valid_lft 586sec preferred_lft 586sec
    inet6 fd24:172::7/128 scope global dynamic noprefixroute
        valid_lft 2591987sec preferred_lft 604787sec
    inet6 fe80::be24:11ff:fed:8160/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@hq-srv ~]#
[root@hq-srv ~]# ip -c route
default via 172.16.100.1 dev ens18 proto dhcp src 172.16.100.2 metric 100
172.16.100.0/26 dev ens18 proto kernel scope link src 172.16.100.2 metric 100
[root@hq-srv ~]#
[root@hq-srv ~]# 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=1.21 ms
64 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=0.699 ms
64 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=0.461 ms
64 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.740 ms

--- 172.16.100.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3064ms
rtt min/avg/max/mdev = 0.461/0.778/1.213/0.272 ms
[root@hq-srv ~]#
```

IPv6

```
[root@hq-srv ~]# ip -c a show ens18
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:fd:81:60 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.16.100.1/26 brd 172.16.100.63 scope global dynamic noprefixroute ens18
        valid_lft 502sec preferred_lft 502sec
    inet6 fd24:172::7/128 scope global dynamic noprefixroute
        valid_lft 2590783sec preferred_lft 603503sec
    inet6 fe80::be24:11ff:fed:8160/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@hq-srv ~]#
[root@hq-srv ~]# ip -c -6 route
:1: dev lo proto kernel metric 256 pref medium
:2: dev fd24:172::7 proto kernel metric 100 pref medium
:3: dev fd24:172::7 proto ens18 proto ra metric 100 pref medium
:4: dev fd24:172::7/64 dev ens18 proto kernel metric 1824 pref medium
default via fd24:172::7 dev ens18 proto ra metric 100 pref medium
[root@hq-srv ~]#
[root@hq-srv ~]# 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=0.602 ms
64 bytes from fd24:172::1: icmp_seq=2 ttl=64 time=0.489 ms
64 bytes from fd24:172::1: icmp_seq=3 ttl=64 time=0.546 ms
64 bytes from fd24:172::1: icmp_seq=4 ttl=64 time=0.691 ms

--- fd24:172::1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3111ms
rtt min/avg/max/mdev = 0.489/0.582/0.691/0.074 ms
[root@hq-srv ~]#
```

1.4. Настроить локальные учётные записи на всех устройствах в соответствии с таблицей 2

Задание

Настройте локальные учётные записи 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.

```
1 | # useradd -c "Administrator" admin -U
2 | # passwd admin
```



`admin` - имя пользователя

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

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

`passwd admin` - задать пароль пользователю



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

Добавление пользователей

HQ-R

```
1 # useradd -c "Admin" admin -U
2 # passwd admin
3 < вводим пароль пользователя >
4 < повторяем ввод паря >
```

Создание пользователя Network admin

```
1 # useradd -c "Network admin" network_admin -U
2 # passwd network_admin
3 < вводим пароль пользователя >
4 < повторяем ввод паря >
```

HQ-SRV

Создание пользователя Admin

```
1 # useradd -c "Admin" admin -U
2 # passwd admin
3 < вводим пароль пользователя >
4 < повторяем ввод паря >
```

BR-R

Создание пользователя Branch admin

```
1 # useradd -c "Branch admin" branch_admin -U
2 # passwd branch_admin
3 < вводим пароль пользователя >
4 < повторяем ввод паря >
```

Создание пользователя Network admin

```
1 # useradd -c "Network admin" network_admin -U
2 # passwd network_admin
```

```
3 | < вводим пароль пользователя >
4 | < повторяем ввод паря >
```

BR-SRV

Создание пользователя Branch admin

```
1 | # useradd -c "Branch admin" branch_admin -U
2 | # passwd branch_admin
3 | < вводим пароль пользователя >
4 | < повторяем ввод паря >
```

Создание пользователя Network admin

```
1 | # useradd -c "Network admin" network_admin -U
2 | # passwd network_admin
3 | < вводим пароль пользователя >
4 | < повторяем ввод паря >
```

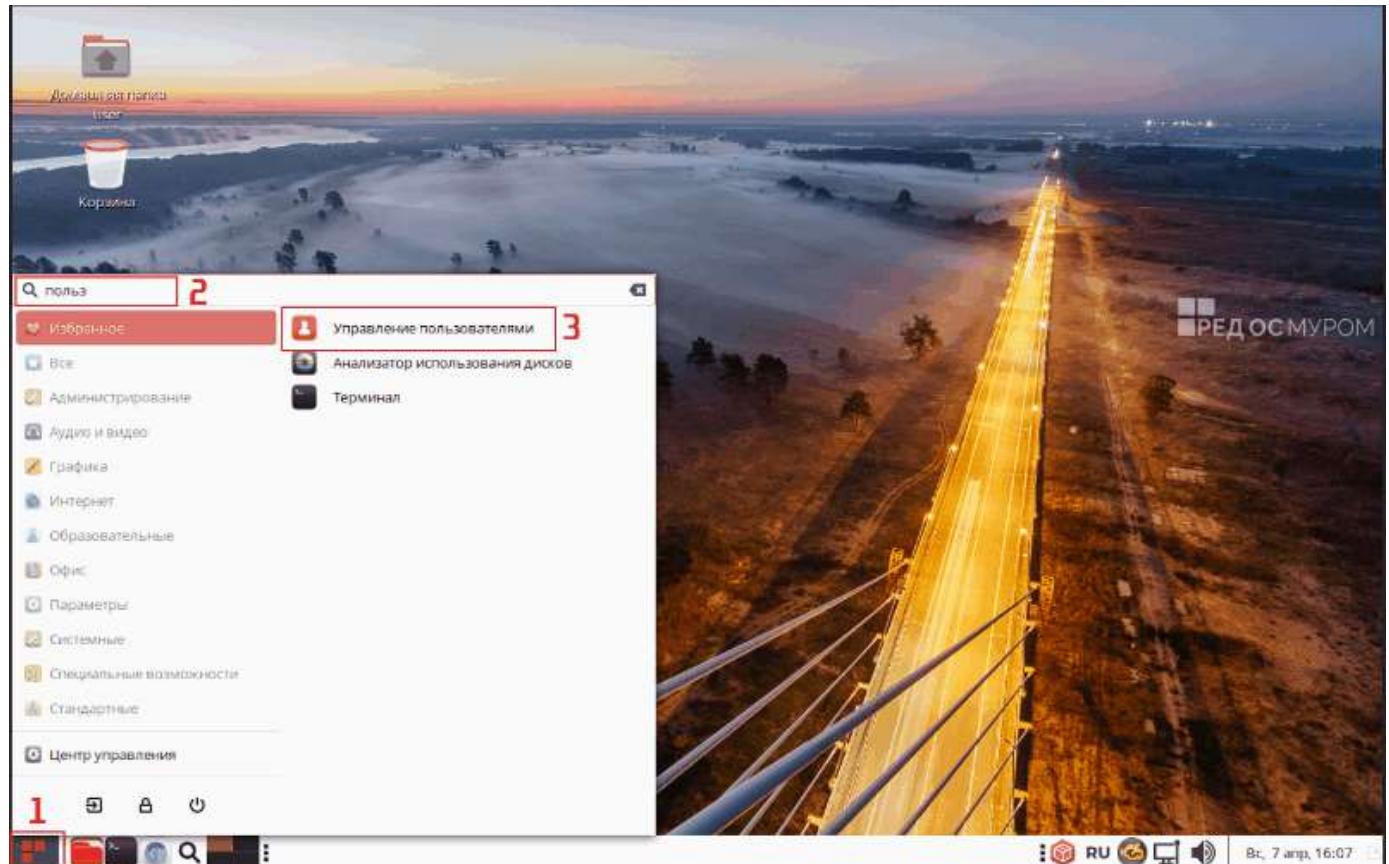
CLI

Вариант -1

Создание пользователя Admin

```
1 | # useradd -c "Admin" admin -U
2 | # passwd admin
3 | < вводим пароль пользователя >
4 | < повторяем ввод паря >
```

Вариант -2



Powered by [Wiki.js](#)

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

Задание

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

Решение



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
```

Установка:

```
1 | # dnf install iperf3 -y
```



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

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

```
1 | # iperf3 -s
```

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

```
1 | # 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 58812
[ 5] local 1.1.1.1 port 5201 connected to 1.1.1.2 port 58822
[ ID] Interval          Transfer     Bitrate
[ 5]  0.00-1.00   sec  1.41 GBytes  12.1 Gbits/sec
[ 5]  1.00-2.00   sec  1.41 GBytes  12.1 Gbits/sec
[ 5]  2.00-3.00   sec  1.40 GBytes  12.1 Gbits/sec
[ 5]  3.00-4.00   sec  1.45 GBytes  12.4 Gbits/sec
[ 5]  4.00-5.00   sec  1.47 GBytes  12.6 Gbits/sec
[ 5]  5.00-6.00   sec  1.42 GBytes  12.2 Gbits/sec
[ 5]  6.00-7.00   sec  1.37 GBytes  11.7 Gbits/sec
[ 5]  7.00-8.00   sec  1.33 GBytes  11.4 Gbits/sec
[ 5]  8.00-9.00   sec  1.43 GBytes  12.2 Gbits/sec
[ 5]  9.00-10.00  sec  1.40 GBytes  12.1 Gbits/sec
-----
[ ID] Interval          Transfer     Bitrate
[ 5]  0.00-10.00  sec  14.1 GBytes  12.1 Gbits/sec
                                         receiver

-----
```

Server listening on 5201 (test #2)

```
[root@hq-r ~]# iperf3 -c 1.1.1.1
Connecting to host 1.1.1.1, port 5201
[ 5] local 1.1.1.2 port 58822 connected to 1.1.1.1 port 5201
[ ID] Interval          Transfer     Bitrate      Retr  Cwnd
[ 5]  0.00-1.00   sec  1.42 GBytes  12.2 Gbits/sec    0  3.04 MBytes
[ 5]  1.00-2.00   sec  1.41 GBytes  12.1 Gbits/sec    0  3.04 MBytes
[ 5]  2.00-3.00   sec  1.40 GBytes  12.1 Gbits/sec    0  3.04 MBytes
[ 5]  3.00-4.00   sec  1.45 GBytes  12.4 Gbits/sec    0  3.04 MBytes
[ 5]  4.00-5.00   sec  1.47 GBytes  12.6 Gbits/sec    0  3.04 MBytes
[ 5]  5.00-6.00   sec  1.42 GBytes  12.2 Gbits/sec    0  3.04 MBytes
[ 5]  6.00-7.00   sec  1.37 GBytes  11.7 Gbits/sec    0  3.04 MBytes
[ 5]  7.00-8.00   sec  1.33 GBytes  11.4 Gbits/sec    0  3.04 MBytes
[ 5]  8.00-9.00   sec  1.43 GBytes  12.3 Gbits/sec    0  3.04 MBytes
[ 5]  9.00-10.00  sec  1.40 GBytes  12.1 Gbits/sec    0  3.04 MBytes
-----
[ ID] Interval          Transfer     Bitrate      Retr
[ 5]  0.00-10.00  sec  14.1 GBytes  12.1 Gbits/sec    0
                                         sender
                                         receiver

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

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

Задание

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

Решение

HQ-R

“

Создадим простой bash-скрипт резервного копирования 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

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

Создадим файл скрипта

```
1 | # 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/$data
cp -r /etc/nftables /var/backup/$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:

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

Запускаем скрипт

```
1 | # /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/utysh.conf
[root@hq-r ~]# _
```



Копируем скрипт с HQ-R на BR-R



Переходим на VM **BR-R**

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

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

Забираем с HQ-R `backup.sh`. Используем IP-адресацию GRE туннеля

```
1 | scp admin@10.10.10.1:/var/backup-script/backup.sh /var/backup-script/
```

При необходимости задаем права скрипту на выполнение:

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

Запускаем скрипт

```
1 | # /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.

Задание

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.

Решение

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

```
1 | # nano /etc/ssh/sshd_config
```

Находим строчку `Port 22` снимаем комментарий со строки и изменяем номер порта

```
# $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
#
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
#
# 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.
#
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
# 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 командой: `semanage port -a -t ssh_port_t -p tcp 2222`

Перезапускаем службу sshd

```
1 | # systemctl restart sshd
```

Проверить на каком порту работает SSH:

```
1 | # ss -tlpn | grep ssh
```

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

```
[root@hq-r ~]#  
[root@hq-r ~]#  
[root@hq-r ~]# ssh admin@172.16.100.2 -p 2222  
admin@172.16.100.2's password:  
Last failed login: Thu Feb 1 23:53:31 MSK 2024 from 172.16.100.1 on ssh:notty  
There was 1 failed login attempt since the last successful login.  
Last login: Thu Feb 1 23:50:40 2024 from 172.16.100.1  
[admin@hq-srv ~]$ _
```

Перенаправление



Создаем правило `nftables` на HQ-R, которое будет перенаправлять внешние подключения к HQ-R на порту 22 -> на порт 2222 сервера HQ-SRV .

Добавим цепочку `prerouting` в таблицу `my_nat` в ранее созданный файл с правилами `nftables` `/etc/nftable/hq-r.nft`

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.

Открываем файл

```
1 | # nano /etc/nftable/hq-r.nft
```

И дописываем правила (выделено красным)

```
table inet mu nat {  
    chain prerouting {  
        type nat hook prerouting priority filter; policy accept;  
        ip daddr 4.4.4.1 tcp dport 22 dnat ip to 172.16.100.2:2222  
        ip daddr 1.1.1.2 tcp dport 22 dnat ip to 172.16.100.2:2222  
        ip6 daddr 2024:4::1 tcp dport 22 dnat ip6 to [fd24:172::2]:2222  
        ip6 daddr 2024:1::2 tcp dport 22 dnat ip6 to [fd24:172::2]:2222  
    }  
  
    chain my_masquerade {  
        type nat hook postrouting priority srcnat;  
        oifname "ens18" masquerade  
    }  
}
```

Перезапускаем nftables

```
1 | # systemctl restart nftables
```

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: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 16:38:44 2024 from 172.16.100.1  
[admin@hq-srv ~]$ _
```

```
[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+FRZ3AUXZ4KjrsCBXek.  
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.

Задание

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

Решение

Настройка nftables на HQ-SRV

Установка nftables

```
1 | # dnf install -y nftables
```

Создаем и открываем файл

```
1 | # nano /etc/nftables/hq-srv.nft
```

[Copy](#)



Запрещаем подключение CLI к HQ-SRV по IPv4 и IPv6

Прописываем следующие строки

```
1 | table inet filter {
2 |     chain input {
3 |         type filter hook input priority filter; policy accept;
4 |         ip saddr 3.3.3.2 tcp dport 2222 counter reject
5 |         ip saddr 4.4.4.0/30 tcp dport 2222 counter reject
6 |         ip6 saddr 2024:ab:cd:3::/64 tcp dport 2222 counter reject
7 |         ip6 saddr 2024:ab:cd:4::/64 tcp dport 2222 counter reject
8 |     }
9 | }
```

Включаем использование данного файла в sysconfig

```
1 | # nano /etc/sysconfig/nftables.conf
```

Ниже строки начинающейся на `include`, прописываем строку

```
1 | include "/etc/nftables/hq-srv.nft"
```

Запуск и добавление в автозагрузку сервиса `nftables`

```
1 | # systemctl enable --now nftables
```

Проверка подключение к HQ-SRV по SSH

Подключение с HQ-R

```
[root@hq-r ~]# ssh admin@172.16.100.2 -p 2222
admin@172.16.100.2's password:
Last login: Sun Apr  7 16:49:26 2024 from fd24:172::1
[admin@hq-srv ~]$ exit
выход
Connection to 172.16.100.2 closed.
[root@hq-r ~]# ssh admin@fd24:172::2 -p 2222
admin@fd24:172::2's password:
Last login: Sun Apr  7 16:58:11 2024 from 172.16.100.1
[admin@hq-srv ~]$ exit
выход
Connection to fd24:172::2 closed.
[root@hq-r ~]#
```

Подключение с BR-R

```
[root@br-r ~]# ssh admin@1.1.1.2
admin@1.1.1.2's password:
Last login: Sun Apr  7 16:59:15 2024 from fd24:10::2
[admin@hq-srv ~]$ exit
выход
Connection to 1.1.1.2 closed.
[root@br-r ~]#
```

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 ~]$ |
```