

Задание модуля 1.

1. Выполните базовую настройку всех устройств:

а. Присвоить имена в соответствии с топологией

HQ-SRV

```
hostnamectl set-hostname HQ-SRV
```

HQ-R

```
hostnamectl set-hostname HQ-R
```

ISP

```
hostnamectl set-hostname ISP
```

BR-R

```
hostnamectl set-hostname BR-R
```

BR-SRV

```
hostnamectl set-hostname BR-SRV
```

CLI

```
hostnamectl set-hostname HQ-R
```

б. Рассчитайте IP-адресацию IPv4 и IPv6.

Необходимо заполнить таблицу №1, чтобы эксперты могли проверить ваше рабочее место.

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

172.16.100.0/28

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

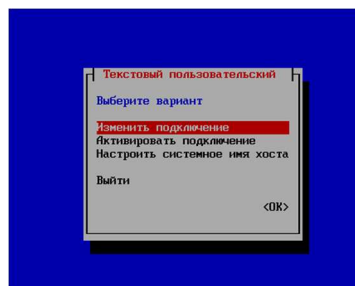
192.168.100.0/26

Имя устройства	IP
CLI	ens192: 3.3.3.2/30 ens192 gateway: 3.3.3.1 ens224: 20.20.20.20/24
ISP	ens224: 1.1.1.1/30 ens192: 2.2.2.1/30 ens256: 3.3.3.1/30
HQ-R	ens224: 192.168.100.1/26 ens192: 1.1.1.2/30 ens192 gateway: 1.1.1.1 ens256: 20.20.20.1/24

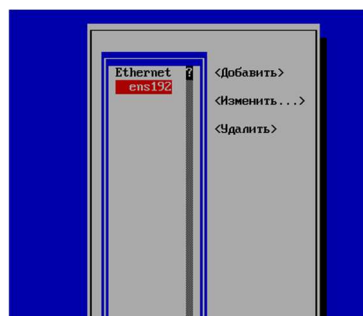
HQ-SRV	ens192: 192.168.100.10/26 ens192 gateway: 192.168.100.1
BR-R	ens224: 172.16.100.1/28 ens192: 2.2.2.2/30 ens192 gateway: 2.2.2.1
BR-SRV	ens192: 172.16.100.10/28 ens192 gateway: 172.16.100.1

Настраиваем IP-адресацию на всех хостах с помощью сетевой утилиты nmtui согласно таблице. (На примере HQ-SRV).

1. Заходим в псевдографический интерфейс nmtui и нажимаем на «Изменить подключение».



2. Выбираем необходимый интерфейс для настройки.



3. Настраиваем сетевой интерфейс согласно схеме адресации.

Раскрываем «Конфигурацию IPv4», выбираем тип подключения «Вручную», назначаем IP-адрес и шлюз и нажимаем на ОК.

Изменить подключение

Имя профиля ens192

Устройство ens192 (00:0C:29:22:11:40)

= ETHERNET <Показать>

КОНФИГУРАЦИЯ IPv4 <Выйти> <Скрыть>

Адреса 192.168.100.10/26 <Удалить>

<Добавить...>

Шлюз 192.168.100.1

Серверы DNS <добавить...>

Домены поиска <Добавить...>

Маршрутизация (нет дополнительных маршрутов) <Изменить...>

☐ Не использовать эту сеть для маршрута по умолчанию

☐ Игнорировать автоматически полученные маршруты

☐ Игнорировать автоматически полученные параметры DNS

☐ Требовать адресацию IPv4 для этого подключения

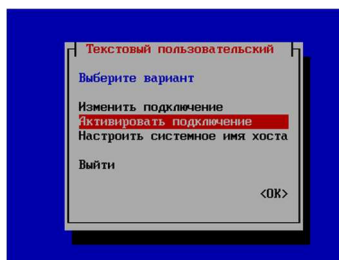
= КОНФИГУРАЦИЯ IPv6 <Автоматически> <Показать>

☒ Подключаться автоматически

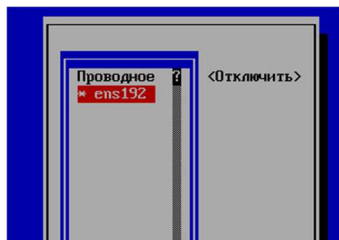
☒ Доступно всем пользователям

<Отменить> <OK>

4. Для подтверждения изменений выходим в главное меню и выбираем пункт «Активировать подключение»



5. Выключаем и включаем интерфейс необходимый интерфейс.



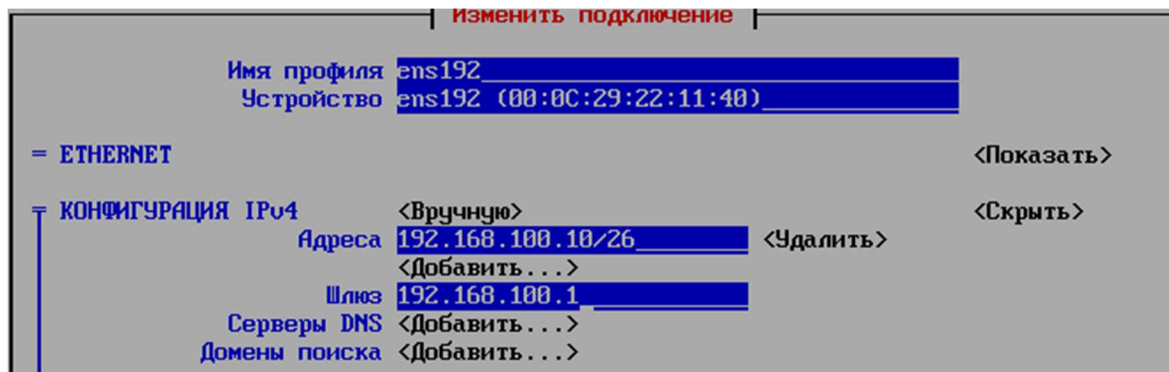
Примечание. Чтобы перезапустить интерфейс, можно также воспользоваться командой строкой «nmcli connection up ens192»

6. Выходим из псевдографического интерфейса и проверяем адресацию с помощью команды «ip a»

```
[root@HQ-SRV ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:22:11:40 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.100.10/26 brd 192.168.100.63 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe22:1140/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Повторяем эти действия на остальных устройствах и приводим к примерному виду ниже.

HQ-SRV:



HQ-R:

Изменить подключение	
Имя профиля	ens192
Устройство	ens192 (00:0C:29:31:95:24)
= ETHERNET	
Показать	
= КОНФИГУРАЦИЯ IPv4	
Вручную	
Скрыть	
Адреса	1.1.1.2/30
Удалить	
Добавить...	
Шлюз	1.1.1.1
Серверы DNS	Добавить...
Домены поиска	Добавить...

Изменить подключение	
Имя профиля	ens224
Устройство	ens224 (00:0C:29:31:95:2E)
= ETHERNET	
Показать	
= КОНФИГУРАЦИЯ IPv4	
Вручную	
Скрыть	
Адреса	192.168.100.1/26
Удалить	
Добавить...	
Шлюз	
Серверы DNS	Добавить...
Домены поиска	Добавить...

Изменить подключение	
Имя профиля	ens256
Устройство	ens256 (00:0C:29:31:95:38)
= ETHERNET	
Показать	
= КОНФИГУРАЦИЯ IPv4	
Вручную	
Скрыть	
Адреса	20.20.20.1/24
Удалить	
Добавить...	
Шлюз	
Серверы DNS	Добавить...
Домены поиска	Добавить...

ISP:

Изменить подключение	
Имя профиля	ens192
Устройство	ens192 (00:0C:29:A6:10:25)
= ETHERNET	
Показать	
= КОНФИГУРАЦИЯ IPv4	
Вручную	
Скрыть	
Адреса	2.2.2.1/30
Удалить	
Добавить...	
Шлюз	
Серверы DNS	Добавить...
Домены поиска	Добавить...

Изменить подключение	
Имя профиля	ens224
Устройство	ens224 (00:0C:29:A6:10:2F)
= ETHERNET	
Показать	
= КОНФИГУРАЦИЯ IPv4	
Вручную	
Скрыть	
Адреса	1.1.1.1/30
Удалить	
Добавить...	
Шлюз	
Серверы DNS	Добавить...
Домены поиска	Добавить...

Изменить подключение	
Имя профиля	ens256
Устройство	ens256 (00:0C:29:A6:10:39)
= ETHERNET	
Показать	
= КОНФИГУРАЦИЯ IPv4	
Вручную	
Скрыть	
Адреса	3.3.3.1/30
Удалить	
Добавить...	
Шлюз	
Серверы DNS	Добавить...
Домены поиска	Добавить...

BR-R:

Изменить подключение

Имя профиля
Устройство

ens192
ens192 (00:0C:29:41:51:D7)

= ETHERNET

Показать

КОНФИГУРАЦИЯ IPv4

Вручную

Скрыть

Адреса

2.2.2.2/30

Удалить

Добавить...

Шлюз

2.2.2.1

Серверы DNS

Добавить...

Домены поиска

Добавить...

Изменить подключение

Имя профиля
Устройство

ens224
ens224 (00:0C:29:41:51:E1)

= ETHERNET

Показать

КОНФИГУРАЦИЯ IPv4

Вручную

Скрыть

Адреса

172.16.100.1/28

Удалить

Добавить...

Шлюз

Серверы DNS

Добавить...

Домены поиска

Добавить...

BR-SRV:

Изменить подключение

Имя профиля
Устройство

ens192
ens192 (00:0C:29:E3:53:7D)

= ETHERNET

Показать

КОНФИГУРАЦИЯ IPv4

Вручную

Скрыть

Адреса

172.16.100.10/28

Удалить

Добавить...

Шлюз

172.16.100.1

Серверы DNS

Добавить...

Домены поиска

Добавить...

CLI:

Изменить подключение

Имя профиля
Устройство

ens192
ens192 (00:0C:29:9F:88:A8)

= ETHERNET

Показать

КОНФИГУРАЦИЯ IPv4

Вручную

Скрыть

Адреса

3.3.3.2/30

Удалить

Добавить...

Шлюз

Серверы DNS

Добавить...

Домены поиска

Добавить...

Изменить подключение

Имя профиля
Устройство

ens224
ens224 (00:0C:29:9F:88:B2)

= ETHERNET

Показать

КОНФИГУРАЦИЯ IPv4

Вручную

Скрыть

Адреса

20.20.20.20/24

Удалить

Добавить...

Шлюз

Серверы DNS

192.168.100.10

Удалить

Добавить...

Домены поиска

Добавить...

Маршрутизация

1 дополнительный маршрут

Изменить...

Также в маршрутизации на CLI добавить маршрут:

Назначение/Префикс	Следующий переход	Метрика	
192.168.100.0/26	20.20.20.1		Удалить

Необходимо включить маршрутизацию пакетов на роутерах HQ-R, ISP, BR-R.

Отправляем параметр пересылки пакетов в файл sysctl.conf

```
echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
```

Перезаписываем файл sysctl.conf

```
sysctl -p
```

Выключаем SELinux на всех хостах.

1. Заходим в конфигурационный файл SELinux.

```
nano /etc/sysconfig/selinux
```

```
GNU nano 4.3 /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

2. Значение параметра SELINUX меняем с «enforcing» на «permissive»

```
GNU nano 4.3 /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Примечание. Посмотреть все возможные параметры можно выше, в комментариях.

```
GNU nano 4.3 /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

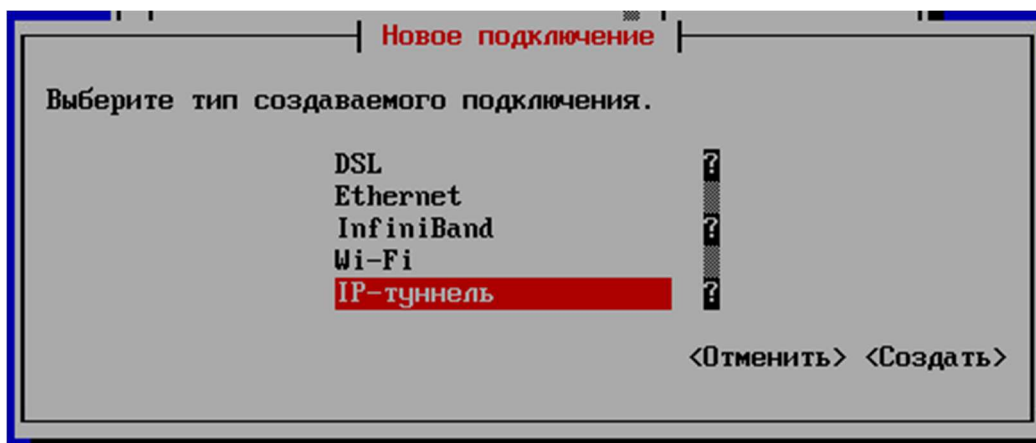
3. Перезапускаем виртуальную машину.

```
reboot
```

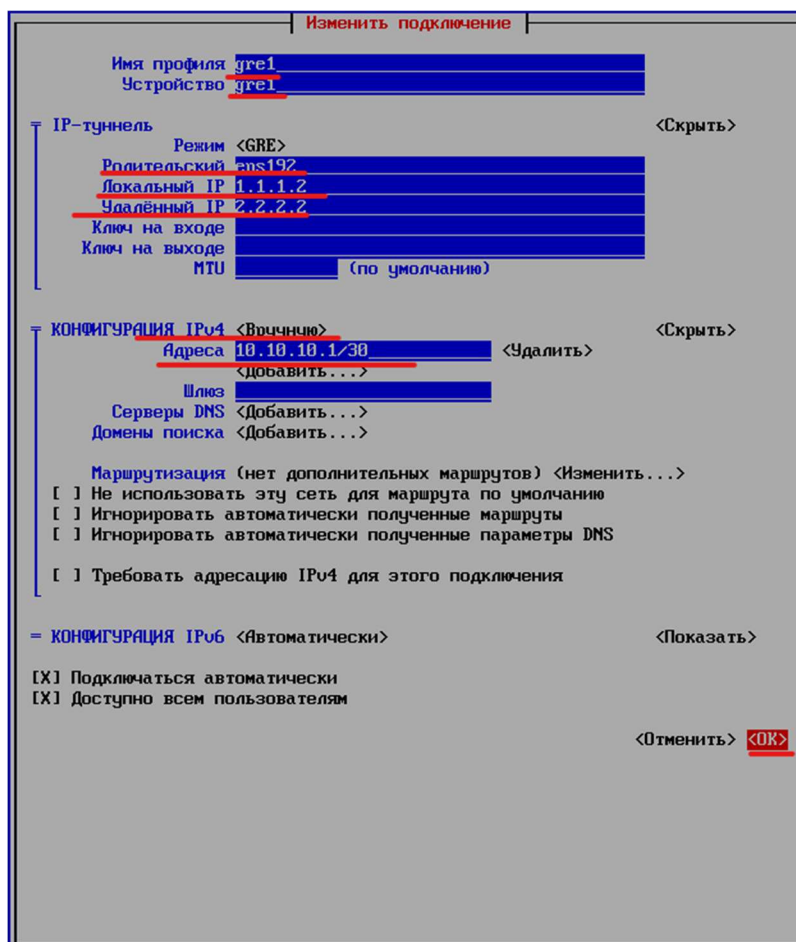
Для дальнейшей настройки необходимо связать филиалы с помощью туннеля.

HQ-R:

1. Заходим в псевдографический интерфейс nmtui в «Изменить подключение» и нажимаем на «Добавить». В окне необходимо выбрать «IP-Туннель» и «Создать».

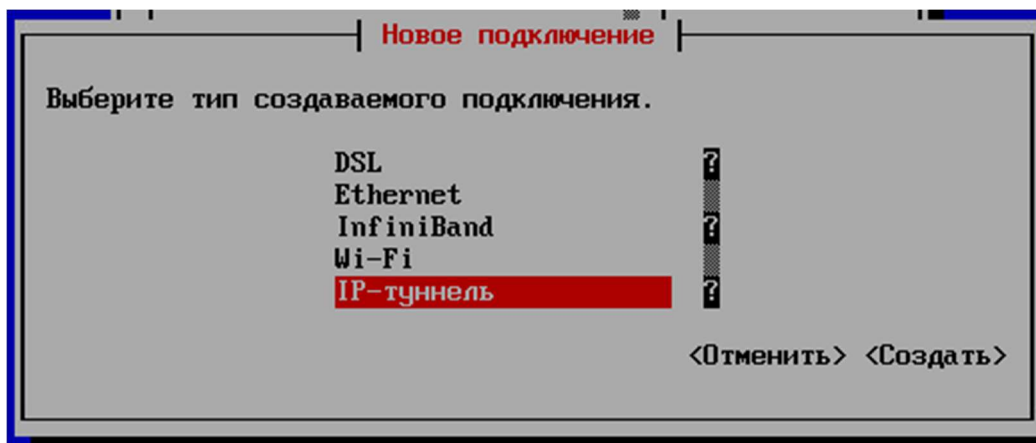


2. Настраиваем имя устройство «gre1», устройство «gre1», режим «GRE», родительский интерфейс «ens192», локальный адрес «1.1.1.2», удаленный адрес «2.2.2.2», конфигурация IPv4 «Вручную», адреса «10.10.10.1/30».

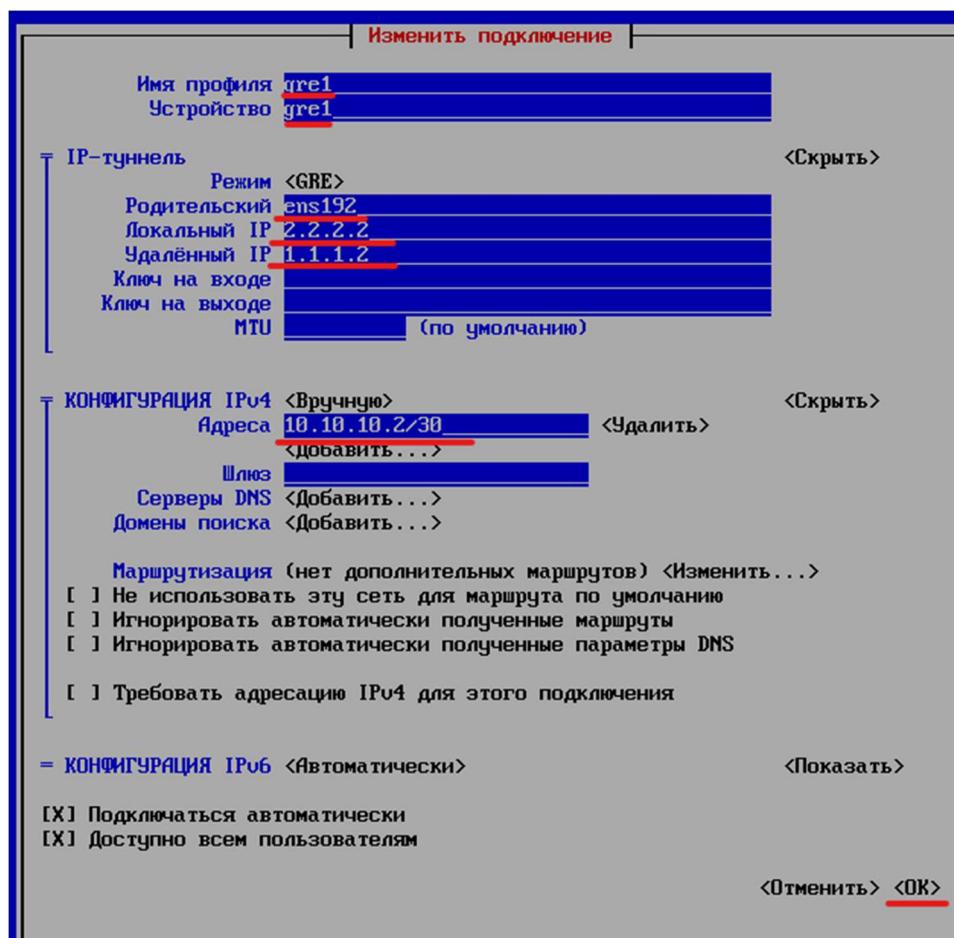


BR-R:

1. Заходим в псевдографический интерфейс nmtui в «Изменить подключение» и нажимаем на «Добавить». В окне необходимо выбрать «IP-Туннель» и «Создать».



2. Настраиваем имя устройство «gre1», устройство «gre1», режим «GRE», родительский интерфейс «ens192», локальный адрес «2.2.2.2», удаленный адрес «1.1.1.2», конфигурация IPv4 «Вручную», адреса «10.10.10.2/30».



Проверка. Отправляем ping на адреса IP-tunnel.

Настройте внутреннюю динамическую маршрутизацию по средствам FRR. Выберите и обоснуйте выбор протокола динамической маршрутизации из расчёта, что в дальнейшем сеть будет масштабироваться.

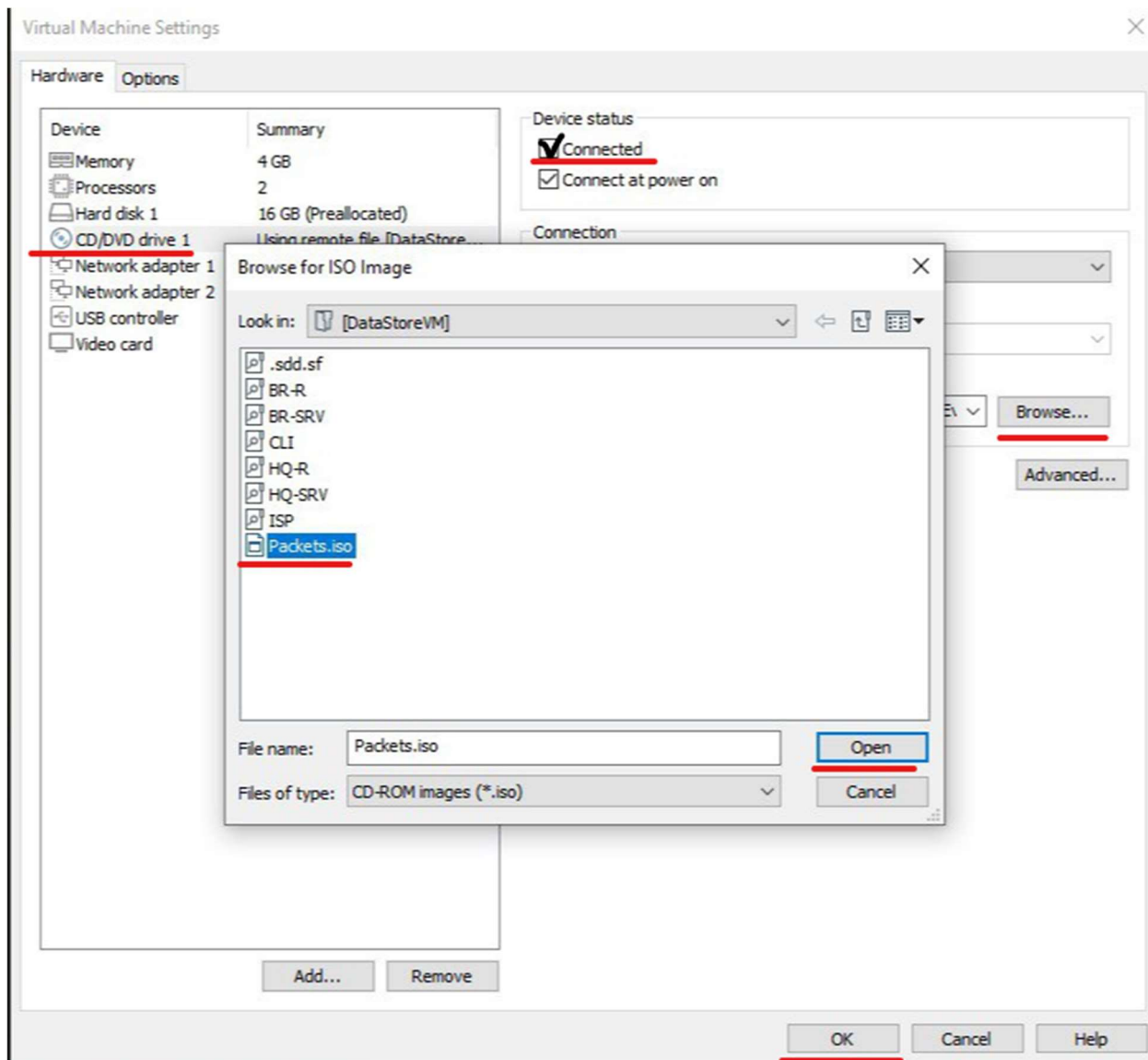
Перед настройкой динамической маршрутизации необходимо поменять ttl туннеля.

HQ-R и BR-R:

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

HQ-R:

Перед установкой выполняем монтирование диска Packets на уровне VM.



Монтируем в Linux.

```
mount /dev/cdrom /mnt
```

1. Устанавливаем FRR

```
cd /mnt/frr
```

```
rpm -i --force *
```

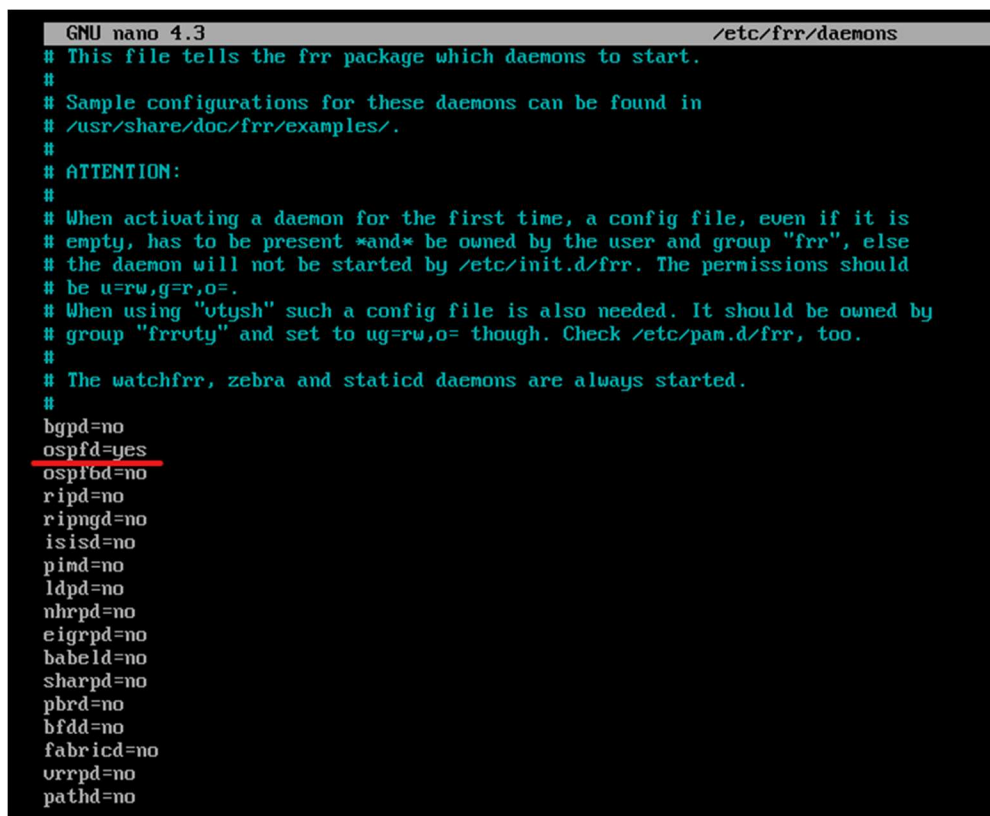
2. Запускаем и отправляем frr в автозагрузку

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

```
systemctl status frr
```

3. Включаем поддержку OSPF

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



```
GNU nano 4.3 /etc/frr/daemons
# This file tells the frr package which daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activating a daemon for the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /etc/init.d/frr. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr, zebra and staticd daemons are always started.
#
bgpd=no
ospfd=yes
ospfbd=no
ripd=no
ripngd=no
isisd=no
pimd=no
ldpd=no
nhrrpd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfd=no
fabricd=no
vrrpd=no
pathd=no
```

4. Перезапускаем frr

```
systemctl restart frr
```

5. Запускаем vtysh и настраиваем OSPF

```
vtysh
```

```
conf t
```

```
router ospf
```

```
network 192.168.100.0/26 area 0
```

```
network 10.10.10.0/30 area 0
```

```
do wr
```

```
exit
```

BR-R:

1. Устанавливаем FRR

```
cd /mnt/frr
```

```
rpm -i --force *
```

2. Запускаем и отправляем frr в автозагрузку

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

```
systemctl status frr
```

3. Включаем поддержку OSPF

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

```
GNU nano 4.3 /etc/frr/daemons
# This file tells the frr package which daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activating a daemon for the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /etc/init.d/frr. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr, zebra and staticd daemons are always started.
#
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
ldpd=no
nhdpd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfd=
fabricd=no
vrrpd=no
pathd=no
```

4. Перезапускаем frr

```
systemctl restart frr
```

5. Запускаем vtysh и настраиваем OSPF

```
vtysh
```

```
conf t
```

```
router ospf
```

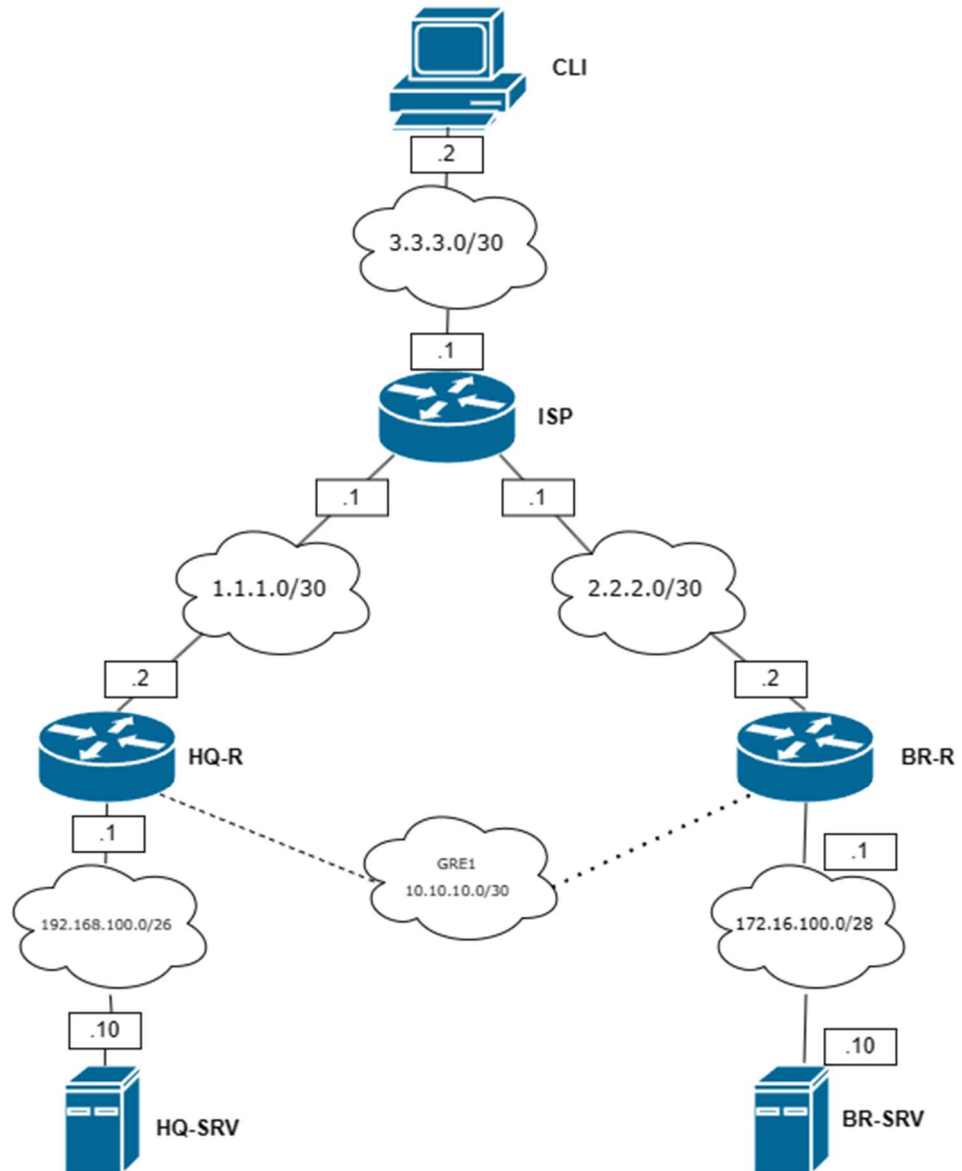
```
network 172.16.100.0/28 area 0
```

```
network 10.10.10.0/30 area 0
```

```
do wr
```

```
exit
```

а. Составьте топологию сети L3.



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

1. Устанавливаем dhcp

```
cd /mnt/dhcp
```

```
rpm -i --force *
```

2. Настраиваем конфигурационный файл

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

```
subnet 192.168.100.0 netmask 255.255.255.192 {  
  range 192.168.100.2 192.168.100.62;  
  option domain-name-servers 192.168.100.10;  
  option routers 192.168.100.1;  
  default-lease-time 600;  
  max-lease-time 7200;  
}
```

3. Запускаем и отправляем dhcpd в автозагрузку

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

```
systemctl status dhcpd
```

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

1. Настраиваем конфигурационный файл

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

```
host hq-srv {  
    hardware ethernet 08:0C:29:22:11:40;  
    fixed-address 192.168.100.10;  
}
```

Настройте локальные учётные записи на всех устройствах в соответствии с таблицей 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

1. На CLI, HQ-SRV, HQ-R

```
useradd Admin
```

```
passwd Admin
```

(Пишем пароль P@ssw0rd два раза)

2. На BR-SRV, BR-R

```
useradd Branch_admin
```

```
passwd Branch_admin
```

(Пишем пароль P@ssw0rd два раза)

3. На HQ-R, BR-R, BR-SRV

```
useradd Network_admin
```

```
passwd Network_admin
```

(Пишем пароль P@ssw0rd два раза)

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

HQ-R и ISP:

1. Устанавливаем iperf

```
cd /mnt/iperf
```

```
rpm -i --force *
```

2. На ISP:

```
iperf3 -s
```

3. На HQ-R:

```
iperf3 -c 1.1.1.1
```

В качестве отчёта предоставляем скрин после тестирования.

```
Accepted connection from 1.1.1.2, port 55450
[ 5] local 1.1.1.1 port 5201 connected to 1.1.1.2 port 55452
[ ID] Interval           Transfer     Bitrate
[ 5]  0.00-1.00      sec    610 MBytes  5.12 Gbits/sec
[ 5]  1.00-2.00      sec    687 MBytes  5.76 Gbits/sec
[ 5]  2.00-3.00      sec    666 MBytes  5.59 Gbits/sec
[ 5]  3.00-4.00      sec    635 MBytes  5.32 Gbits/sec
[ 5]  4.00-5.00      sec    663 MBytes  5.56 Gbits/sec
[ 5]  5.00-6.00      sec    656 MBytes  5.50 Gbits/sec
[ 5]  6.00-7.00      sec    661 MBytes  5.55 Gbits/sec
[ 5]  7.00-8.00      sec    637 MBytes  5.35 Gbits/sec
[ 5]  8.00-9.00      sec    658 MBytes  5.52 Gbits/sec
[ 5]  9.00-10.00     sec    675 MBytes  5.66 Gbits/sec
-----
[ ID] Interval           Transfer     Bitrate
[ 5]  0.00-10.00     sec    6.39 GBytes  5.49 Gbits/sec
receiver
```

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

HQ-R и BR-R:

1. Создаём файл backup.sh и пишем там скрипт.

cd

nano backup.sh

HQ-R

```
GNU nano 4.3
#!/bin/bash
SAVE="user@192.168.100.10:/home/user"
BACKUP="/root/backup-hq-r.tar.gz"
sudo tar cvpzf $BACKUP --exclude=/proc --exclude=$BACKUP /
scp $BACKUP $SAVE
```

BR-R

```
#!/bin/bash
SAVE="user@172.16.100.10:/home/user"
BACKUP="/root/backup-br-r.tar.gz"
sudo tar cvpzf $BACKUP --exclude=/proc --exclude=$BACKUP /
scp $BACKUP $SAVE
```

2. Добавляем возможность запускать скрипт.

chmod +x backup.sh

3. Запускаем скрипт.

./backup.sh

4. По окончании снятия backup будет запрошен логин и пароль от пользователя user.

P@ssw0rd

5. Проверяем наличие backup файлов на HQ-SRV и BR-SRV

cd /home/user/

ls

```
[root@BR-SRV user]# ls
backup-br-r.tar.gz  B
[root@BR-SRV user]#
```


Примечание. IPTables лучше настраивать в самом конце, так как при установке FreeIPA устанавливает свои правила, которые необходимо сбросить.

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.

HQ-SRV:

1. Настраиваем систему контролирования трафика для перенаправления трафика.

```
iptables -t nat -A PREROUTING -p tcp --dport 2222 -j REDIRECT --to-port 22
```

2. Включаем iptables-services для работы правил после перезагрузки:
`systemctl enable --now iptables`

3. Сохраняем текущую конфигурацию

```
iptables-save > /etc/sysconfig/iptables
```

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

HQ-SRV:

1. Настраиваем систему контролирования трафика для перенаправления трафика.

```
iptables -A INPUT -s 20.20.20.20 -p tcp --dport 22 -j DROP
```

2. Сохраняем текущую конфигурацию

```
iptables-save > /etc/sysconfig/iptables
```

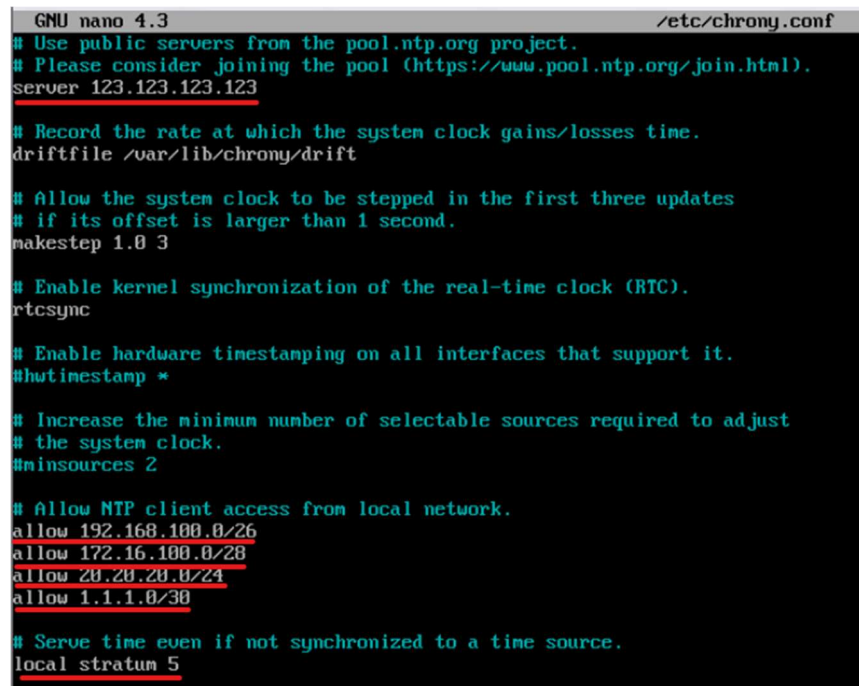
Задание модуля 2

Настройте синхронизацию времени между сетевыми устройствами по протоколу NTP.

а. В качестве сервера должен выступать роутер HQ-R со стратумом 5
По умолчанию chrony установлен. Сразу начинаем с его настройки.

1. Изменяем конфигурационный файл.

`nano /etc/chrony.conf`



```
GNU nano 4.3 /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
server 123.123.123.123

# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift

# Allow the system clock to be stepped in the first three updates
# if its offset is larger than 1 second.
makestep 1.0 3

# Enable kernel synchronization of the real-time clock (RTC).
rtcsync

# Enable hardware timestamping on all interfaces that support it.
#hwtimestamp *

# Increase the minimum number of selectable sources required to adjust
# the system clock.
#minsources 2

# Allow NTP client access from local network.
allow 192.168.100.0/26
allow 172.16.100.0/28
allow 20.20.20.0/24
allow 1.1.1.0/30

# Serve time even if not synchronized to a time source.
local stratum 5
```

б. Используйте Loopback интерфейс на HQ-R, как источник сервера времени

1. Создаём loopback интерфейс

`nmcli conn add type dummy connection.interface-name Lo1`

`nmcli conn edit dummy-Lo1`

`set connection.id Lo1`

`set connection.interface-name Lo1`

`set connection.autoconnect yes`

`set ipv4.method manual`

`set ipv4.addresses 123.123.123.123/32`

`save`

`quit`

2. Проверяем созданный loopback

ip a

```
12: Lo1: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether b2:c5:e7:b3:e4:97 brd ff:ff:ff:ff:ff:ff
    inet 123.123.123.123/32 scope global noprefixroute Lo1
        valid_lft forever preferred_lft forever
    inet6 fe80::6fa2:e600:9d86:ecf2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

3. Перезапускаем сервис.

systemctl restart chronyd

с. Все остальные устройства и сервера должны синхронизировать свое время с роутером HQ-R

1. На всех устройствах кроме ISP и CLI

nano /etc/chrony.conf

```
GNU nano 4.3 /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
server 192.168.100.1 iburst
```

На ISP

```
GNU nano 4.3 /etc/chrony.co
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
server 1.1.1.2 iburst
```

На CLI

```
GNU nano 4.3 /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
server 20.20.20.1 iburst
```

2. Перезапускаем сервис

systemctl restart chronyd

d. Все устройства и сервера настроены на московский часовой пояс (UTC +3)

1. На всех устройствах

timedatectl set-timezone Europe/Moscow

Настройте сервер домена выбор, его типа обоснуйте, на базе HQ-SRV через web интерфейс, выбор технологий обоснуйте.

b. Организуйте отслеживание подключения к домену

1. Устанавливаем пакеты FreeIPA на HQ-SRV

cd /mnt/freeipa-server

rpm -i --force *

Удаляем java 11

```
rpm -e java-11-openjdk-headless --nodeps
```

2. Задаём HQ-SRV hostname:

```
hostnamectl set-hostname hq-srv.demo.work
```

2. Начинаем установку FreeIPA домена на HQ-SRV

```
ipa-server-install --mkhomedir
```

Соглашаемся на интегрированную службу DNS

```
Do you want to configure integrated DNS (BIND)? [no]: yes_
```

Соглашаемся со следующими параметрами (Enter):

Имя сервера:

```
Server host name [hq-srv.demo.work]:
```

Доменное имя:

```
Please confirm the domain name [demo.work]: _
```

Realm name:

```
Please provide a realm name [DEMO.WORK]: _
```

Указываем пароль P@ssw0rd для Directory Manager:

```
Directory Manager password:  
Password (confirm):
```

Указываем пароль P@ssw0rd для IPA Admin:

```
IPA admin password:  
Password (confirm):
```

Не соглашаемся с настройкой DNS forwarders

```
Invalid IP address fe80::20c:29ff:fe22:1140 for hq-srv  
Do you want to configure DNS forwarders? [yes]: no
```

Соглашаемся с настройкой обратной зоны:

```
No DNS forwarders configured  
Do you want to search for missing reverse zones? [yes]: yes_
```

NetBIOS domain name:

```
NetBIOS domain name [DEMO]:
```

Отказываемся от настройки NTP:

```
Do you want to configure chrony with NTP server or pool address? [no]:
```

Проверяем заданные параметры и соглашаемся на установку:

```
The IPA Master Server will be configured with:
Hostname:      hq-srv.demo.work
IP address(es): 192.168.100.10
Domain name:   demo.work
Realm name:    DEMO.WORK

The CA will be configured with:
Subject DN:    CN=Certificate Authority,O=DEMO.WORK
Subject base:  O=DEMO.WORK
Chaining:      self-signed

BIND DNS server will be configured to serve IPA domain with:
Forwarders:    No forwarders
Forward policy: only
Reverse zone(s): No reverse zone

Continue to configure the system with these values? [no]: yes
```

3. После установки убедитесь, что сервер IPA работает:

```
kinit admin
```

```
ipa user-find admin
```

4. Устанавливаем оболочку по умолчанию для пользователей:

```
ipa config-mod --defaultshell=/usr/bin/bash
```

5. Удаляем правила iptables

```
iptables -F
```

6. Включаем iptables-services для работы правил после перезагрузки:

```
systemctl enable --now iptables
```

7. Сохраняем текущую конфигурацию

```
iptables-save > /etc/sysconfig/iptables
```

а. Введите машины BR-SRV и CLI в данный домен

1. Устанавливаем пакеты FreeIPA на BR-SRV

```
cd /mnt/freeipa-client
```

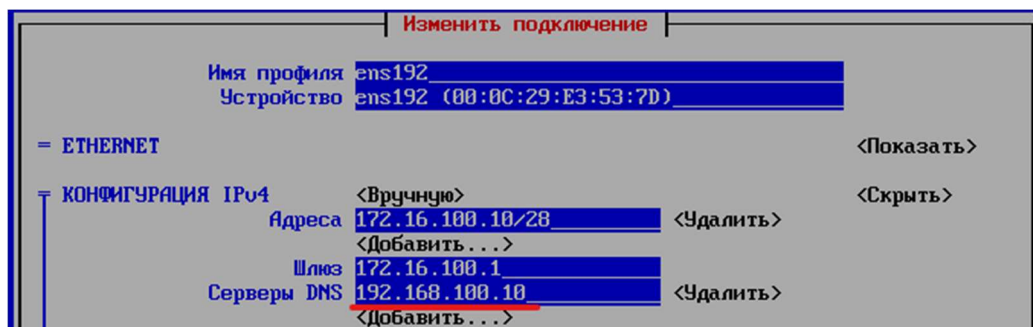
```
rpm -i --force * --nodeps
```

2. Задаём BR-SRV и CLI hostname:

```
hostnamectl set-hostname br-srv.demo.work
```

```
hostnamectl set-hostname cli.demo.work
```

3. Через nmtui задаём DNS-сервер



4. Вводим в домен

```
ipa-client-install --mkhomedir --enable-dns-updates
```

5. Отказываемся от настройки NTP:

```
Discovery was successful!  
Do you want to configure chrony with NTP server or pool address? [no]:
```

Проверяем заданные параметры и соглашаемся на ввод в домен:

```
Realm: DEMO.WORK  
DNS Domain: demo.work  
IPA Server: hq-srv.demo.work  
BaseDN: dc=demo,dc=work  
  
Continue to configure the system with these values? [no]: yes
```

Вводим учетные записи администратора

```
admin:P@ssw0rd
```

```
User authorized to enroll computers: admin  
Password for admin@DEMO.WORK: _
```

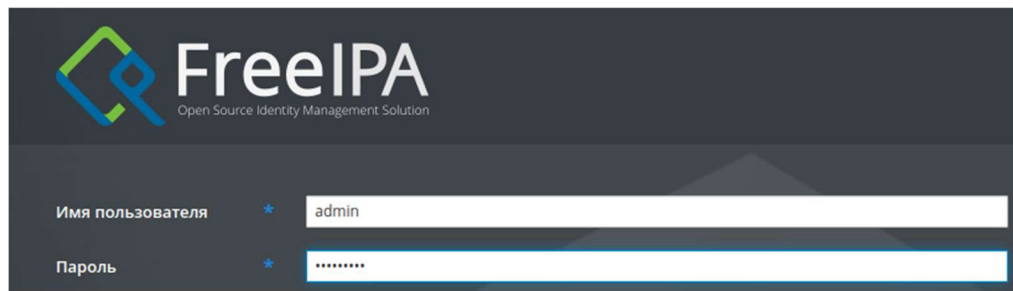
Успешный ввод выглядит так.

```
Configured /etc/krb5.conf for IPA realm DEMO.WORK  
Client configuration complete.  
The ipa-client-install command was successful
```

Проверяем введенные хосты в веб-интерфейсе IPA

Заходим на веб-интерфейс с HQ-SRV по адресу

```
hq-srv.demo.work
```



FreeIPA
Open Source Identity Management Solution

Имя пользователя * admin

Пароль *

Имя пользователя - admin

Пароль - P@ssw0rd

Переходим во вкладку Узлы и проверяем:

Узлы

Поиск	Q
<input type="checkbox"/>	Имя узла
<input type="checkbox"/>	br-srv.demo.work
<input type="checkbox"/>	cli.demo.work
<input type="checkbox"/>	hq-srv.demo.work

Настройте DNS-сервер на сервере HQ-SRV:

а. На DNS сервере необходимо настроить 2 зоны

Зона hq.work, также не забудьте настроить обратную зону.

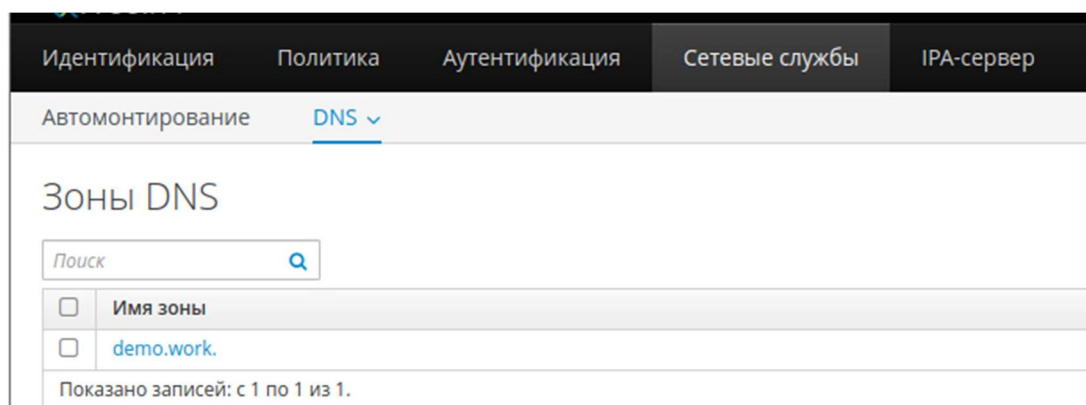
Имя	Тип записи	Адрес
hq-r.hq.work	A, PTR	IP-адрес
hq-srv.hq.work	A, PTR	IP-адрес

Зона branch.work

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

Для создания DNS-сервера воспользуемся интегрированной службой DNS в FreeIPA.

1. Для этого переходим во вкладку Сетевые службы > DNS > Зоны DNS



Идентификация Политика Аутентификация Сетевые службы IPA-сервер

Автомониторинг DNS

Зоны DNS

Поиск Q

<input type="checkbox"/>	Имя зоны
<input type="checkbox"/>	demo.work.

Показано записей: с 1 по 1 из 1.

2. Добавляем прямые и обратные зоны:

☒ Имя зоны *

☒ Имя зоны *

☒ IP-сеть *
обратной зоны

☒ IP-сеть *
обратной зоны

Получаем следующее:

Зоны DNS

Поиск <input type="text"/>	
<input type="checkbox"/>	Имя зоны
<input type="checkbox"/>	100.16.172.in-addr.arpa.
<input type="checkbox"/>	100.168.192.in-addr.arpa.
<input type="checkbox"/>	branch.work.
<input type="checkbox"/>	demo.work.
<input type="checkbox"/>	hq.work.

Заходим в настройки зоны hq.work и добавляем А записи, одновременно создавая PTR

Добавить запись ресурса DNS



Имя записи *

Тип записи



IP Address *

Create reverse ⓘ



* Обязательное поле

Имя записи *

Тип записи



IP Address *

Create reverse ⓘ



* Обязательное поле

Заходим в настройки зоны branch.work и добавляем A записи, одновременно создавая PTR

Имя записи *

Тип записи



IP Address *

Create reverse ⓘ



* Обязательное поле

Имя записи *	<input type="text" value="br-srv"/>
Тип записи	<input type="text" value="A"/>
IP Address *	<input type="text" value="172.16.100.10"/>
Create reverse ⓘ	<input type="checkbox"/>

* Обязательное поле

После поднятия DNS необходимо на всех серверах указать DNS-сервер 192.168.100.10, по аналогии с BR-SRV:

		Изменить подключение	
Имя профиля	ens192		
Устройство	ens192 (00:0C:29:E3:53:7D)		
= ETHERNET			<Показать>
= КОНФИГУРАЦИЯ IPv4	<Вручную>		<Скрыть>
Адреса	172.16.100.10/28	<Удалить>	
	<Добавить...>		
Шлюз	172.16.100.1		
Серверы DNS	192.168.100.10	<Удалить>	
	<Добавить...>		