**Задание 1 модуля 1**

1. Выполните базовую настройку всех устройств:

a. Были присвоены имена в соответствии с топологией командой

b. Была рассчитана IP-адресация IPv4 и IPv6.

Для чтобы эксперты могли проверить рабочее место была заполнена таблица №1.

c. Для сети офиса BRANCH пул адресов - не более 16.

d. Для сети офиса HQ пул адресов - не более 64.

Таблица 1.

IP-адресация IPv4 и IPv6

|  |  |  |
| --- | --- | --- |
| Имя устройства | IPv4 | IPv6 |
| CLI | 192.168.0.2/24 | 2001:33::2/64 |
| ISP | 192.168.0.1/24 | 2001:33::1/64 |
|  | 10.10.11.1/30 | 2001:11::1/64 |
|  | 10.10.11.5/30 | 2001:22::1/64 |
| HQ-R | 192.168.1.1/26 | 2000:100::3f/122 |
|  | 10.10.11.2/30 | 2001:11::11/64 |
| HQ-SRV | 192.168.1.2/26 | 2000:100::1/122 |
| BR-R | 10.10.11.6/30 | 2001:22::22/64 |
|  | 192.168.2.1/28 | 2000:200::f/124 |
| BR-SRV | 192.168.2.2/28 | 2000:200::1/124 |

МАСКИ ПОМЕНЯТЬ

**Задание 2**

Настройка динамической маршрутизации производится с помощью протокола OSPF. Данный протокол динамической сети позволяет разделять сеть на логические области, что делает его масштабируемым для больших сетей. Каждая область может иметь свою таблицу маршрутизации, что уменьшает нагрузку на маршрутизаторы и улучшает производительность сети.

Настройка DE\_BR-R

1. Необходимо перейти в каталог /etc/frr/daemons и изменить 2 параметра, ospfd и ospf6d, c no на yes (рисунок 1).

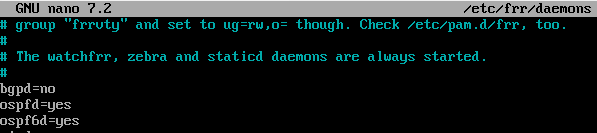


Рисунок 1. Каталог /etc/frr/daemons

1. Далее требуется запуск службы systemctl start frr.service.



Рисунок 2. запуск службы systemctl start frr.service.

С помощью #nano /etc/net/sysctl.conf нужно включить ipv4\_forwarding.

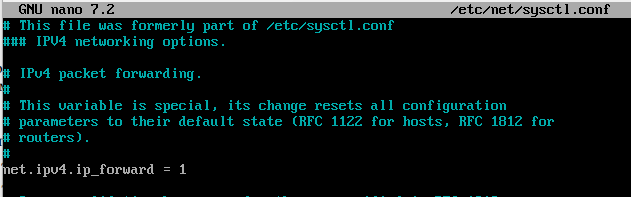


Рисунок 3. Каталог /etc/net/sysctl.conf

1. После входа во vtysh перейти в конфигурацию conf t , и отключить ip forwarding и ipv6 forwarding. Проверить можно командой #do run sho.



Рисунок 4 отключить ip forwarding и ipv6 forwarding

1. Настройка ip адресов

Пример настройки показан на рисунке 5

interface eth0

ip address 10.10.11.6/30

ipv6 address 2000::c:2/126

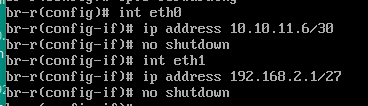


Рисунок 5. Настройка ip адресов

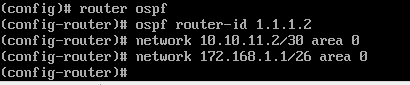


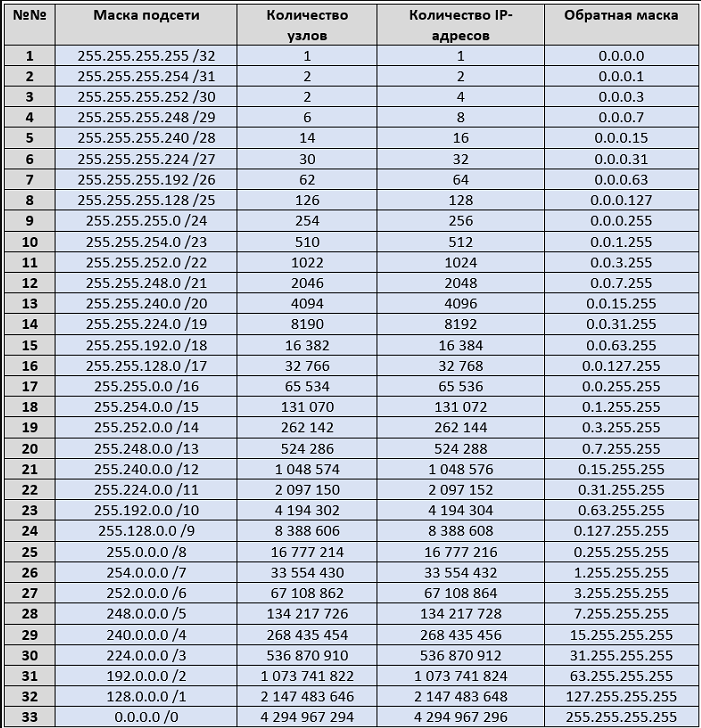
Рисунок 6 Пример настройки ospf

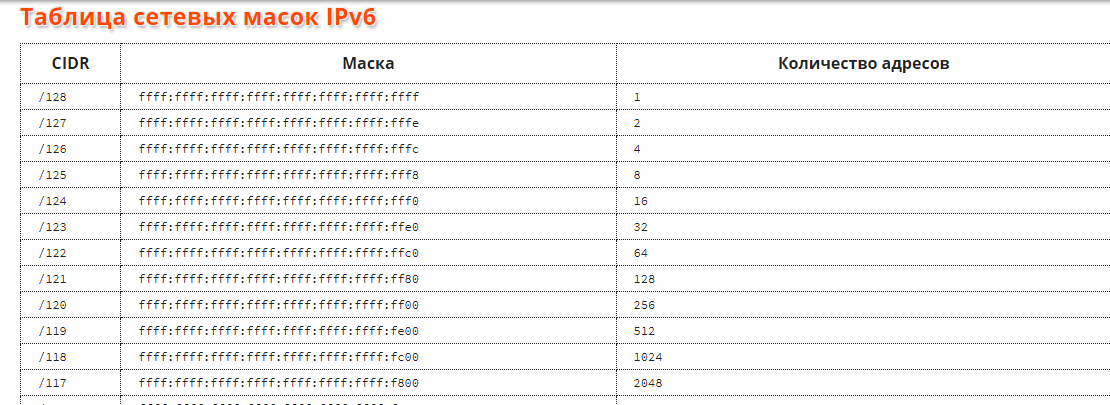
В конце прописать

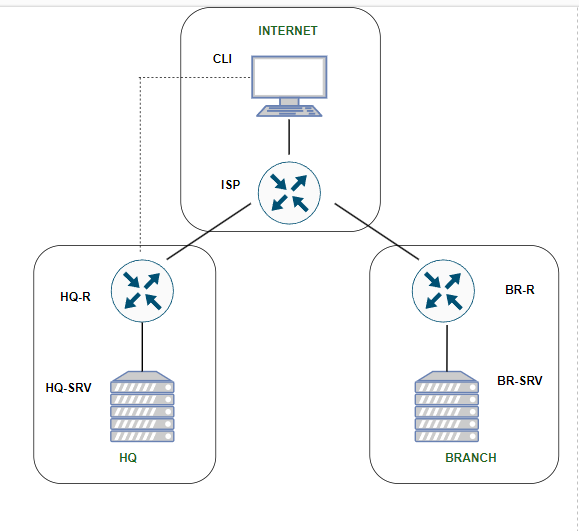
#do wri

#ex

#systemctl restart frr.service







1. НАСТРОЙКА OSPF

BR-R

vtysh

conf t

router ospf

ospf router-id 1.1.1.2

network 10.10.11.2/30 area 0

network 172.168.1.1/26 area 0

end

do wri

ex

systemctl restart frr.service

Аналогично BR-R настраиваем HQ-R и ISP

Пример листинга на HQ-R

nano /etc/frr/daemons

>ospfd=yes

>ospf6d=yes

systemctl start frr.service

vtysh

conf t

ip forwarding

ipv6 forwarding

int eth0

ip address 10.10.11.2/30

no shutdown

int eth1

ip address 192.168.1.1/25

no shutdown

ex

router ospf

network 10.10.11.0/30 a 0

network 192.168.1.0/25 a 0

do wri

end

ex

systemctl restart frr.service

ISP

router ospf

ospf router-id 1.1.1.1

BR-R

router ospf

ospf router-id 1.1.1.2

На ISP нужно отключить frr и поднять порты

vtysh

conf t

ip forwarding

ipv6 forwarding

int eth0

no shutdown

int eth1

no shutdown

int eth1

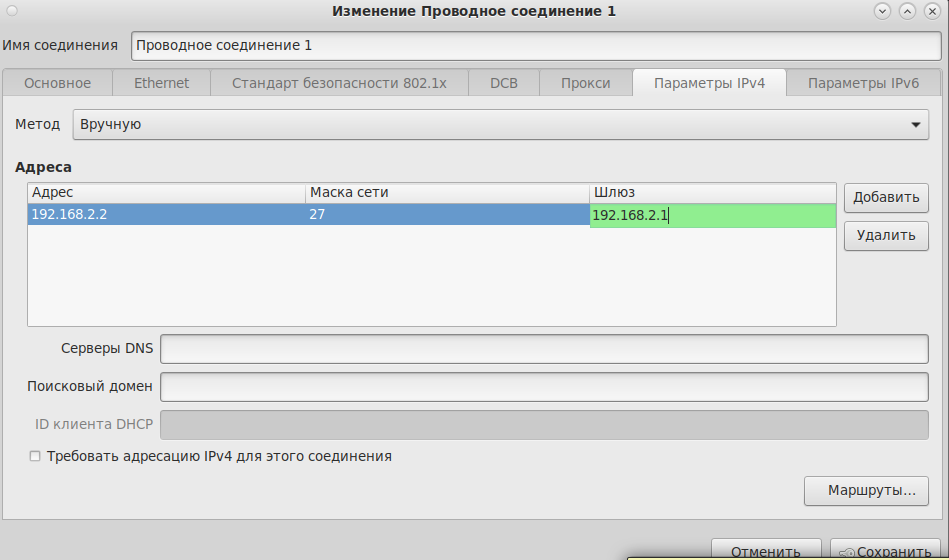
no shutdown

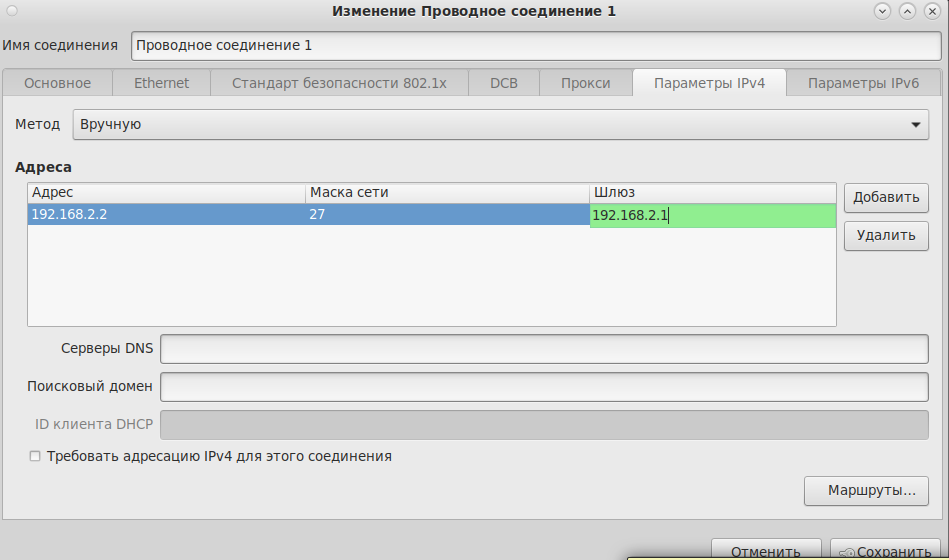
do wri

end

ex

Пример настройки ip-адресов на BR-SRV и CLI. После назначения адреса потребуется включить и выключить поддержку сети для обновления адресов.



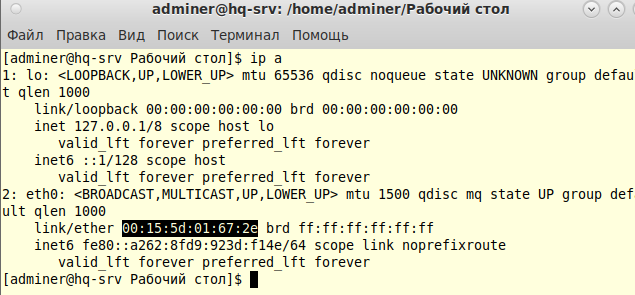


После успешной настройки с BR-SRV должна успешно происходить отправка эхо-запросов до HQ-R.

**1 модуль 3 задание**

Переходим на HQ-R и копируем файл настройки DCHP

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



Пример листинга каталога /etc/dhcp/dhcpd.conf

ddns-update-style none;

subnet 192.168.1.0 netmask 255.255.255.128 {

option routers 192.168.1.1;

option subnet-mask 255.255.255.128;

range dynamic-bootp 192.168.1.2 192.168.1.5;

default-lease-time 21600;

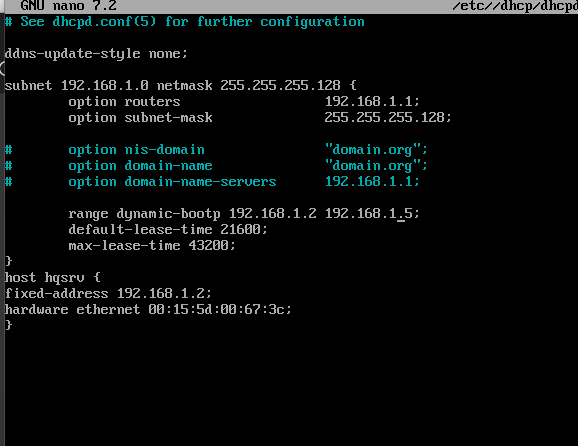
max-lease-time 43200;

host hqsr {

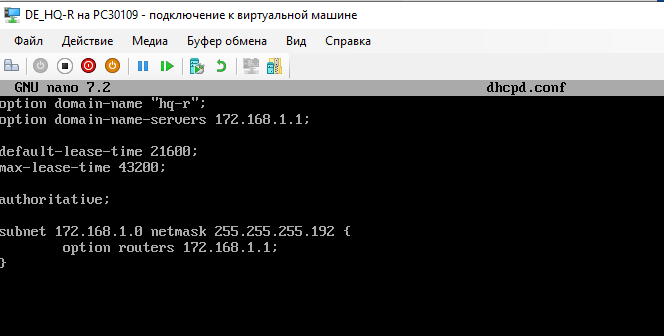
fixed-address 192.168.1.2;

hardware ethernet 00:15:5d:00:67:3c; поменять на свой

}



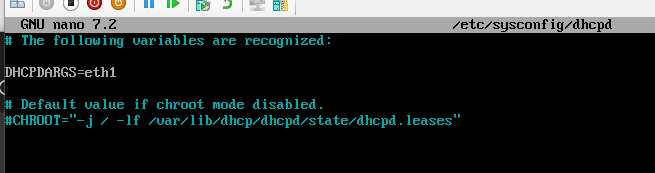
Добавить authoritative;

???

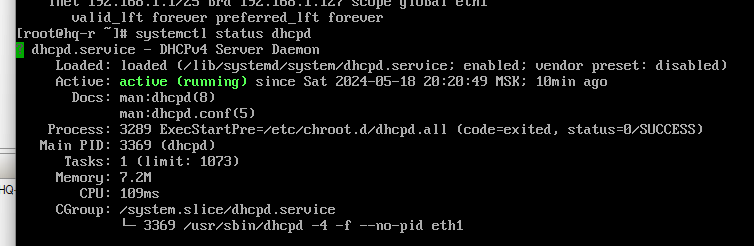
3?

DHCP

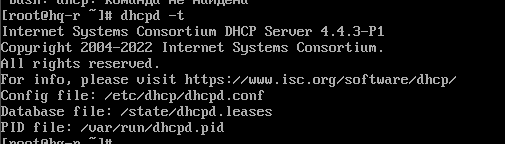
Так же нужно указать порт для раздачи адресов. Переходим в файл командой nano /etc/sysconfig/dhcpd , указываем в параметре DHCPDARGS=eth1.



Вводим #chkconfig dhcpd on для автоматического запуска. Запускаем сервис systemctl start dhcpd. Командой systemctl status dhcpd производится проверка состояния службы.



Проверка конфига dhcp производится командой #dhcpd -t. Если ошибка в конфиге, то он укажет строчку, где была ошибка.



Перезапускаем службы . systemctl restart frrи systemctl restart NetworkManager. И снова перезапускаем dhcpd .

**1 модуль 4 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 |

adduser логин

usermod -aG wheel логин

passwd логин

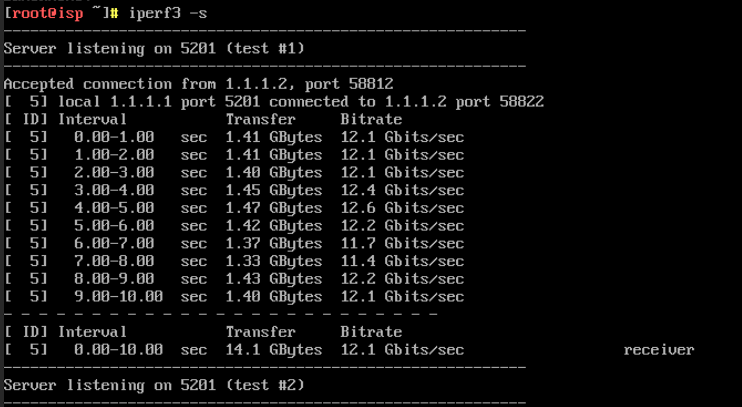
**1 модуль 5 задание**

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

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

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

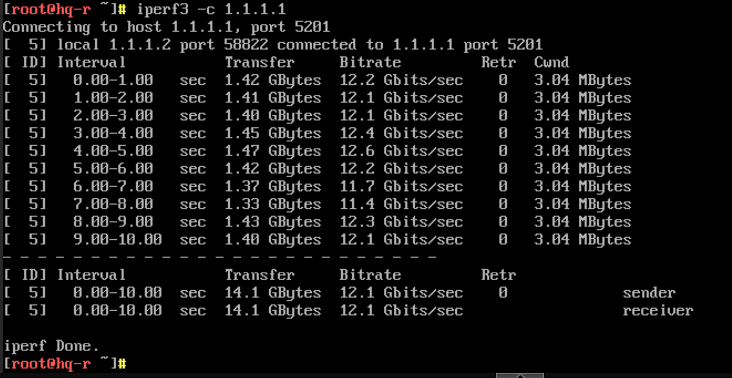
# iperf3 -s



HQ-R

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

# iperf3 -c IP\_address\_ISP



**Модуль 1 задание 6**

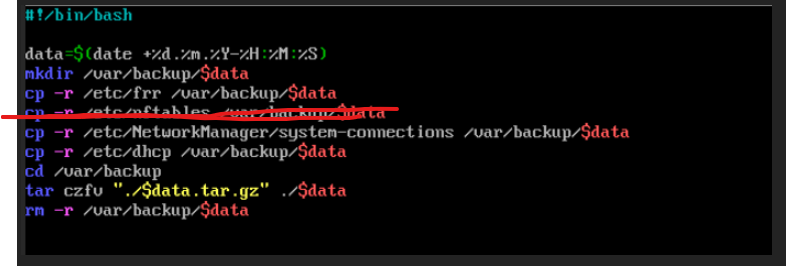
Составьте backup скрипты для сохранения конфигурации сетевых устройств, а именно HQ-R BR-R. Продемонстрируйте их работу.

Была создана директория для хранения скрипта резервного копирования backup-script и директория для хранения архивов резервных копий backup.

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

Создание файла скрипта

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



echo "Start backup"

echo "Done" добавить в начало и конец

Присвоение права скрипту на выполнение:

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

Запуск скрипта

# /var/backup-script/backup.sh

НА BRR ПРОДЕЛАТЬ ТОЖЕ САМОЕ

**Модуль 1 задание 7**

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

HQ-SRV

nano /etc/openssh/sshd\_config

# Раскомментируйте и измените следующую строку

PermitRootLogin yes

порт ssh прописать тот, который указан в задании

ПОРТ ЗАВИСИТ ОТ ЗАДАНИЯ



#systemctl restart sshd

Сохранение правила iptables и ip6tables

Для ipv4

iptables -A FORWARD -i eth1 -s 192.168.0.0/24 -p tcp --dport [порт, указанный в задании] -j DROP

iptables-save > /etc/sysconfig/iptables

systemctl enable --now iptables

Для ipv6

ipv6tables -A FORWARD -i eth1 -s 192.168.0.0/24 -p tcp --dport [порт, указанный в задании] -j DROP

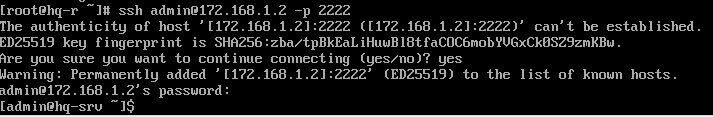
ip6tables-save >> /etc/sysconfig/iptables6

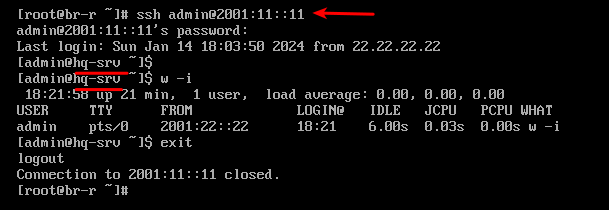
systemctl enable --now ip6tables

Перезапуск службы командой #systemctl restart sshd

После этого тестируем подключение с HQ-R до HQ-SRV

ПОРТ ЗАВИСИТ ОТ ЗАДАНИЯ



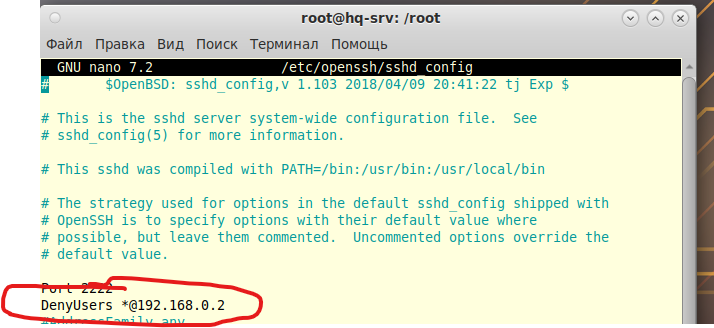


**Модуль 1 задание 8**

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

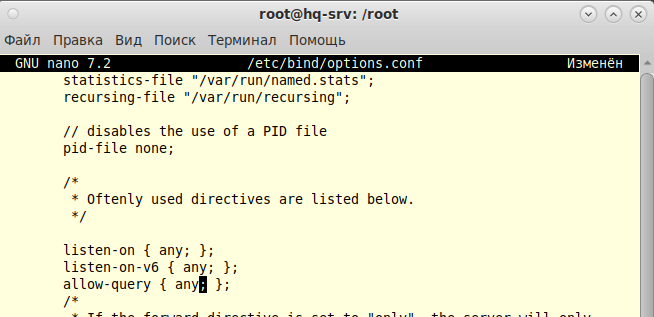
Добавляем правило на сервер, перейдя в каталог /etc/openssh/sshd\_config

В нашем случае ip адресс 192.168.0.2



**МОДУЛЬ 2 ЗАДАНИЕ 1**

Заходим /etc/bind/options.conf и меняем содержимое файла как указано на приведённом далее рисунке.



Запуска и добавление в автозагрузку службу bind:

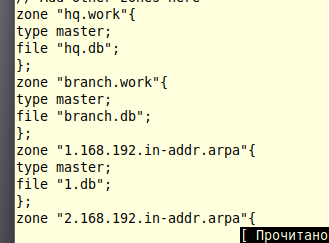
#systemctl enable --now bind

В качестве DNS-сервера для hq-srv должен быть 127.0.0.1:

#echo name\_servers=127.0.0.1 >> /etc/resolvconf.conf

# resolvconf -u

После этого заходим в /etc/bind/local.conf и вписываем туда то, что как указано на приведённом далее рисунке.



Далее необходимо прописать данные команды:

#cp /etc/bind/zone/{localdomain,hq.db}

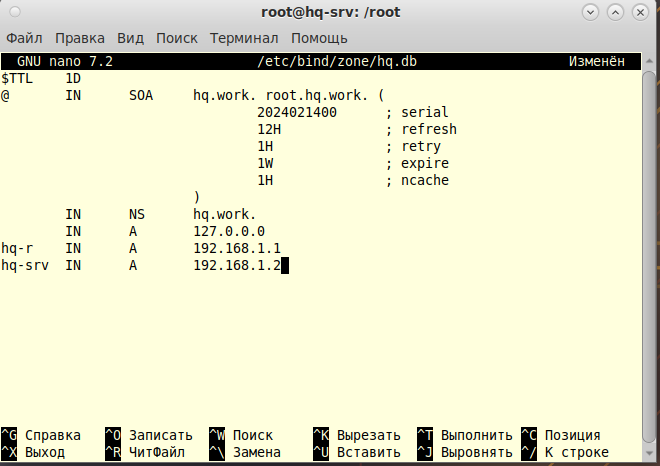
#cp /etc/bind/zone/{localdomain,branch.db}

#cp /etc/bind/zone/{127.in-addr.arpa,1.db}

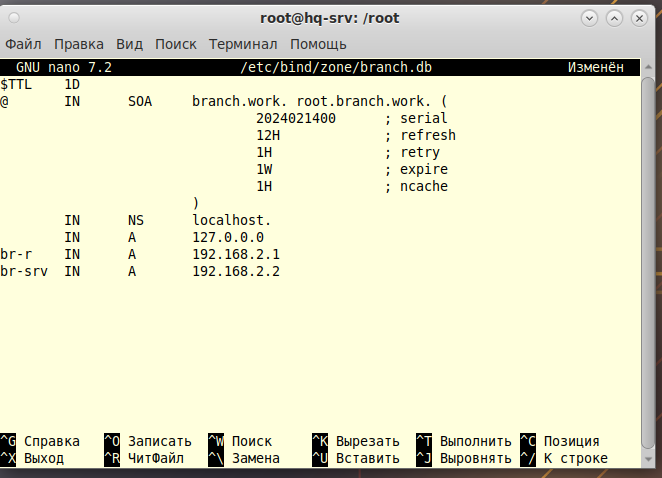
#cp /etc/bind/zone/{127.in-addr.arpa,2.db}

#chown root:named /etc/bind/zone/{hq,branch,1,2}.db

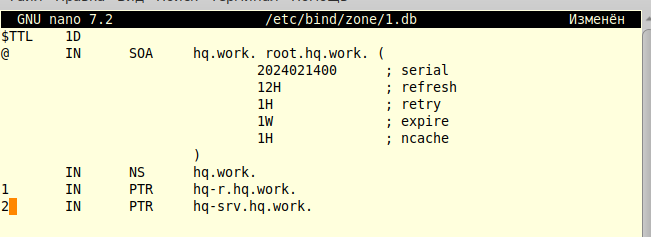
Далее нужно привести каталог /etc/bind/zone/hq.db как указано на приведённом далее рисунке.



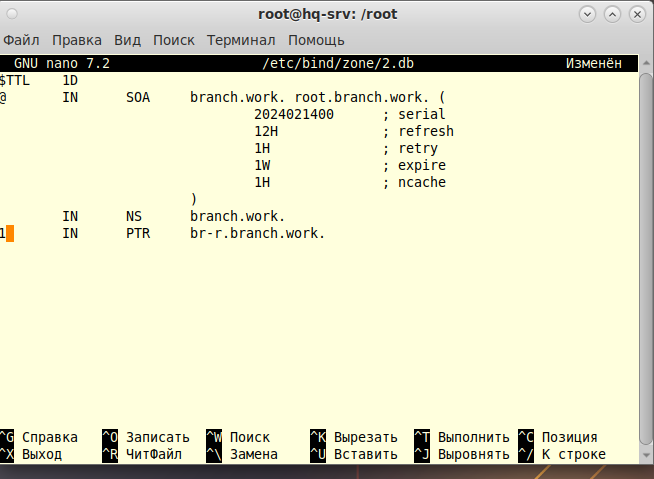
То же самое проделать в каталоге /etc/bind/zone/branch.db



То же самое проделать в каталоге /etc/bind/zone/1.db

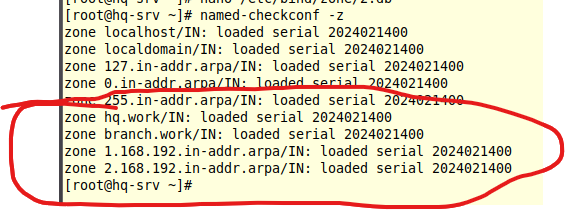


То же самое проделать в каталоге /etc/bind/zone/2.db

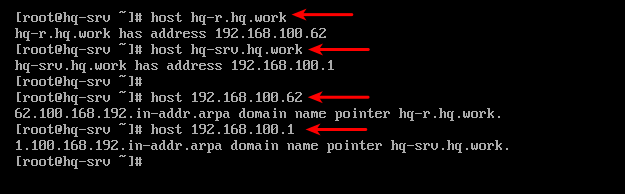


Проверить файлы зон можно утилитой named-checkconf:

# named-checkconf -z



Проверка



1 модуль 2 задание

BR-R

Команды для настройки

nano /etc/frr/daemons

ospfd=yes

ospf6d=yes

systemctl start frr.service

vtysh

conf t

ip forwarding

ipv6 forwarding

int eth0

ip address 10.10.11.6/30

no shutdown

int eth1

ip address 192.168.2.1/27

no shutdown

ex

router ospf

network 10.10.11.4/30 a 0

network 192.168.2.0/27 a 0

end

do wri

ex

systemctl restart frr.service

HQ-R

systemctl restart network NetworkManager frr.service

apt-get update

apt-get install frr

nano /etc/frr/daemons

systemctl start frr

vtysh

conf t

interface eth0

ip address 10.10.11.2/30

ipv6 address 2000::b:2/126

interface eth1

ip address 192.168.1.1/26

ipv6 address 2000::d:1/126

router ospf

ospf router-id 1.1.1.1

network 10.10.11.0/30 area 0

network 192.168.1.0/28 area 0

do sho run

ip forwarding

ipv6 forwarding

do wri

ex

ex

sysctl -a|grep forward

nano /etc/net/sysctl.conf

systemctl restart NetworkManager

systemctl restart frr.service

apt-get install dhcp-server

nano /etc/dhcp/dhcpd.conf

#конфиг option domain-name "HQ-R"; option domain-name-servers 192.168.1.1;

iptables -A FORWARD -i eth1 -s 192.168.0.0/24 -p tcp --dport [порт, указанный в задании] -j DROP iptables-save > /etc/sysconfig/iptables

default-lease-time 6000; max-lease-time 72000; authoritative; subnet 192.168.1.0 netmask 255.255.255.192 { option routers 192.168.1.1; } #конфиг

nano /etc/sysconfig/dhcpd chkconfig dhcpd on service dhcpd start systemctl status dhcpd useradd branch-admin -m -c "Branch admin" -U passwd branch-admin useradd network-admin -m -U useradd network-admin -m -c "Network admin" -U passwd network-admin systemctl enable --now iperf3 iperf3 -c 192.168.0.1 -f m --get-server-output

BR-R

systemctl restart network NetworkManager frr.service

apt-get update

apt-get install frr

nano /etc/frr/daemons

systemctl start frr

vtysh

conf t

interface eth0

ip address 10.10.11.6/30

ipv6 address 2000::c:2/126

interface eth1

ip address 192.168.2.1/28

ipv6 address 2000::e:1/124

router ospf

ospf router-id 1.1.1.2

network 10.10.11.4/30 area 0

network 192.168.2.0/28 area 0

do sho

run ip forwarding

ipv6 forwarding

do wri

ex

ex

sysctl -a|grep forward

nano /etc/net/sysctl.conf

systemctl restart NetworkManager systemctl

restart frr.service

ISP

systemctl restart network NetworkManager frr.service

vtysh

conf t

do sho run

ip forwarding

ipv6 forwarding

do wri

ex

ex

sysctl -a|grep forward

nano /etc/net/sysctl.conf

systemctl restart NetworkManager

systemctl restart frr.service

systemctl enable --now iperf3

HQ-SRV

dnf install openssh-server nano /etc/openssh/sshd\_config