**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 13.

d. Для сети офиса HQ пул адресов - не более 16.

Таблица 1.

IP-адресация IPv4 и IPv6

|  |  |  |
| --- | --- | --- |
| Имя устройства | IPv4 | IPv6 |
| CLI | 192.168.0.2/24 | 2000::a:2/120 |
| ISP | 192.168.0.1/24 | 2000::a:1/120 |
|  | 10.10.11.1/30 | 2000::b:1/126 |
|  | 10.10.11.5/30 | 2000::c:1/126 |
| HQ-R | 192.168.1.1/28 | 2000::b:3/124 |
|  | 10.10.11.2/30 | 2000::b:2/126 |
| HQ-SRV | 192.168.1.2/28 | 2000::b:4/124 |
| BR-R | 10.10.11.6/30 | 2000::c:2/120 |
|  | 192.168.2.1/29 | 2000::c:3/125 |
| BR-SRV | 192.168.2.2/29 | 2000::c:4/125 |

**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).

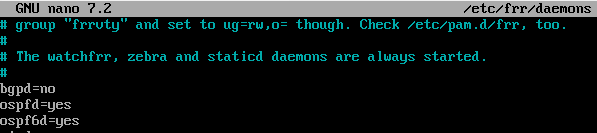


Рисунок 1. Каталог /etc/frr/daemons

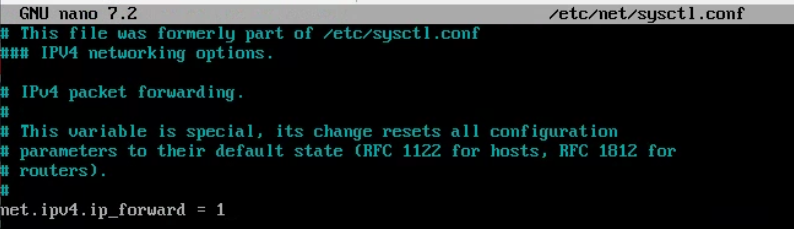


Рисунок 2

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



Рисунок 3. запуск службы systemctl start frr.service.

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



Рисунок 4 включение ip forwarding и ipv6 forwarding

1. Настройка ip адресов

Пример настройки показан на рисунке 5.



Рисунок 5. Настройка ip адресов



Рисунок 6 Пример настройки ospfv2

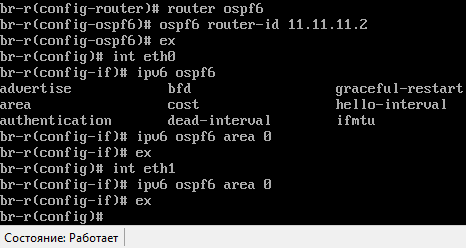


Рисунок 7 Пример настройки ospfv3

Было проверено командой #show running-config



systemctl restart frr.service

Рисунок 8 Проверка

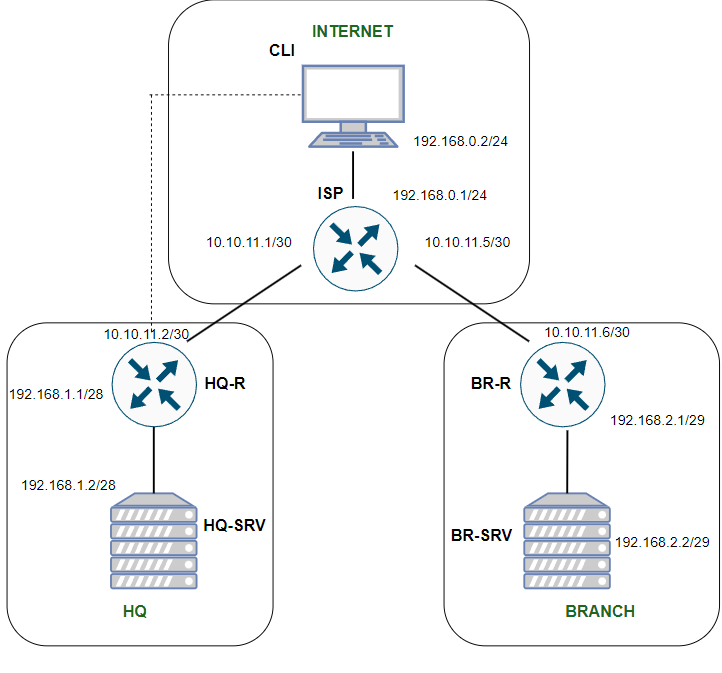


Рисунок 9 Топология

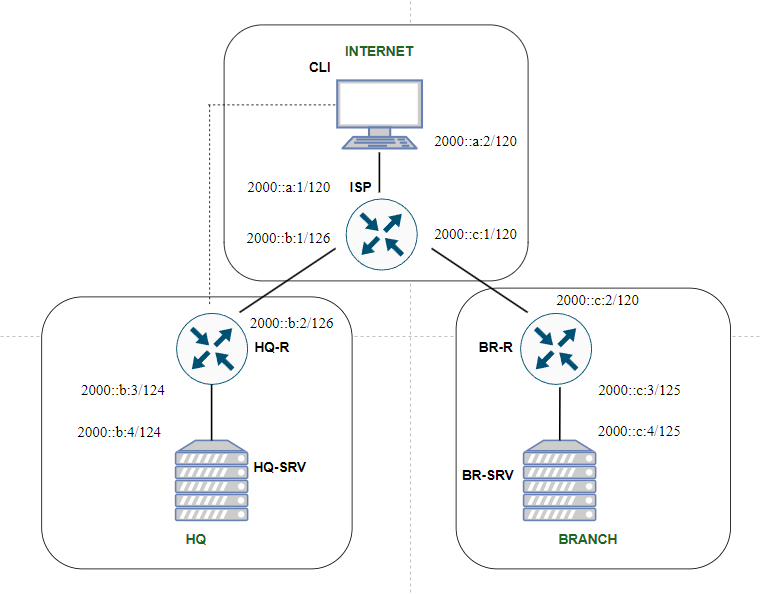


Рисунок 10 Топология

Включить форвардинг? nano /etc/net/sysctl.conf

1. НАСТРОЙКА OSPF

BR-R

vtysh

conf t

router ospf

ospf router-id 1.1.1.2

network 10.10.11.4/30 area 0

network 192.168.1.1/26 area 0

router ospf6

ospf router-id 11.11.11.2

ex

int eth0

ipv6 ospf6 area 0

ex

int eth1

ipv6 ospf6 area 0

do wri

end

ex

systemctl restart frr.service

vtysh

show running-config

Аналогично BR-R был настроен HQ-R

Пример настройки на HQ-R

nano /etc/frr/daemons

>ospfd=yes

>ospf6d=yes

nano /etc/net/sysctl.conf

0->1

systemctl start frr.service

vtysh

conf t

ip forwarding

ipv6 forwarding

int eth0

ip address 10.10.11.2/30

no shutdown

ipv6 address 2001:11::11/64

no shutdown

int eth1

ip address 192.168.1.1/28

no shutdown

ipv6 address 2000:100::3f/124

no shutdown

ex

router ospf

ospf router-id 1.1.1.1

network 10.10.11.0/30 a 0

network 192.168.1.0/28 a 0

router ospf6

ospf router-id 11.11.11.1

ex

int eth0

ipv6 ospf6 area 0

ex

int eth1

ipv6 ospf6 area 0

do wri

end

ex

systemctl restart frr.service

vtysh

show running-config

На ISP нужно включить frr и поднять порты

vtysh

conf t

ip forwarding

ipv6 forwarding

int eth0

no shutdown

int eth1

no shutdown

router ospf6

ospf router-id 11.11.11.1

ospf router-id 11.11.11.2

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.

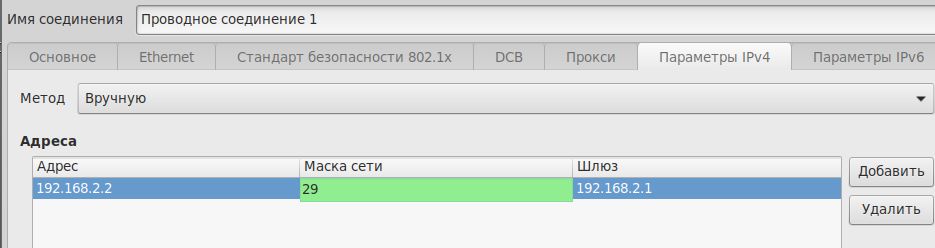


Рисунок 11 Настройка BR-R

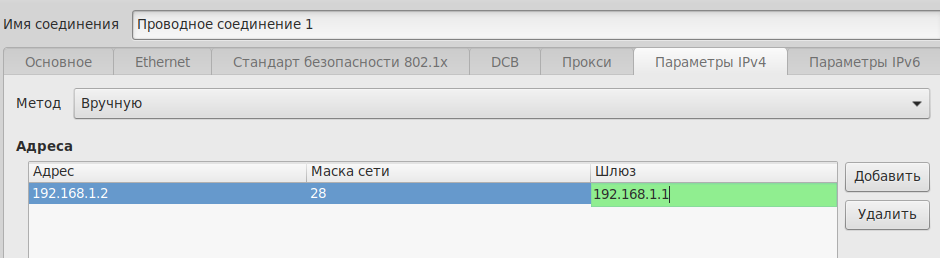


Рисунок 12 Настройка HQ-R

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

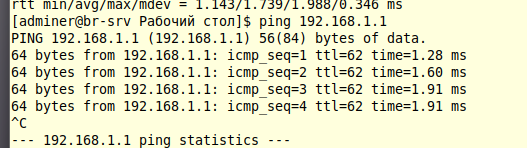


Рисунок 13 Отрпавка эхо-запроса

**1 модуль 3 задание**

Настройте автоматическое распределение IP-адресов на роутере HQ-R. a. Учтите, что у сервера должен быть зарезервирован адрес.

Нужно перейти на HQ-R и скопировать файл настройки DCHP

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

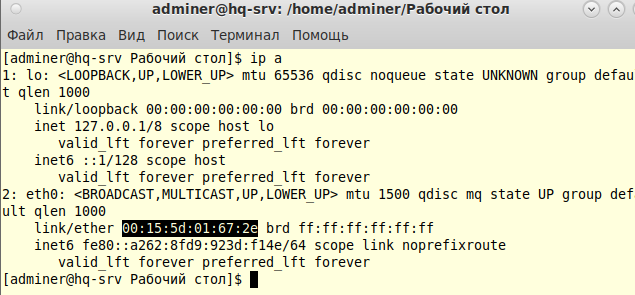


Рисунок 14 Мак-адрес

Пример содержания 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

}

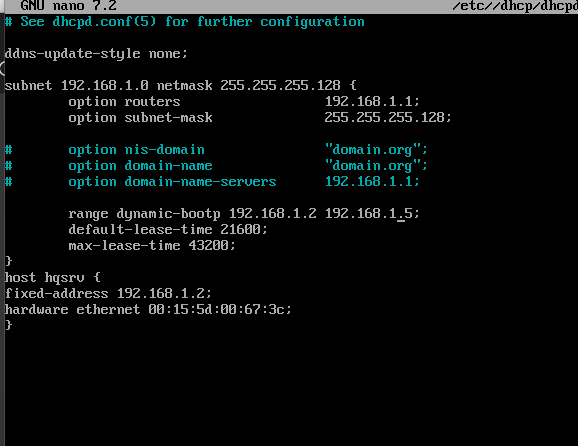


Рисунок 15 каталога /etc/dhcp/dhcpd.conf

Добавить authoritative;

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

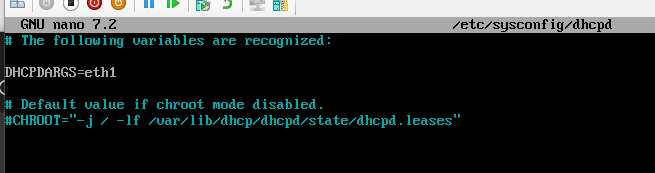


Рисунок 16 Указание порта

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

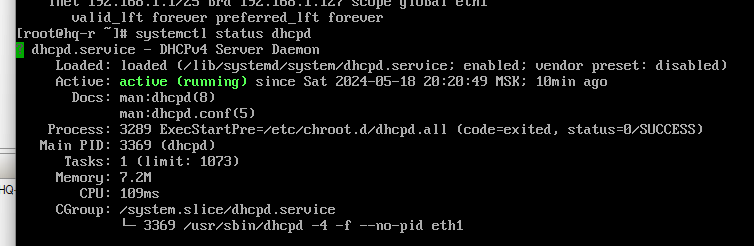
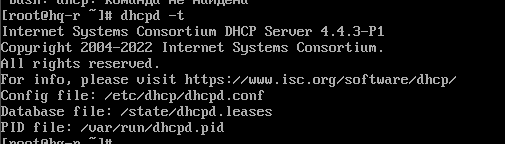


Рисунок 17 Проверка состояния службы

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



Перезапуск службы. systemctl restart frr и 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

CLI логин - пароль

admin -P@ssw0rd

HQ-SRV

admin - P@ssw0rd

HQ-R

admin - P@ssw0rd

network\_admin - P@ssw0rd

BR-SRV

branch\_admin - P@ssw0rd

network\_admin - P@ssw0rd

BR-R

network\_admin - P@ssw0rd

branch\_admin - P@ssw0rd

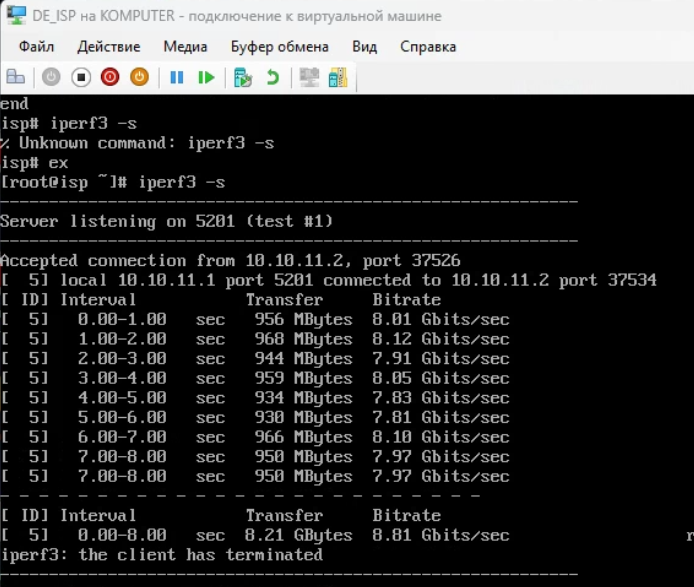
**1 модуль 5 задание**

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



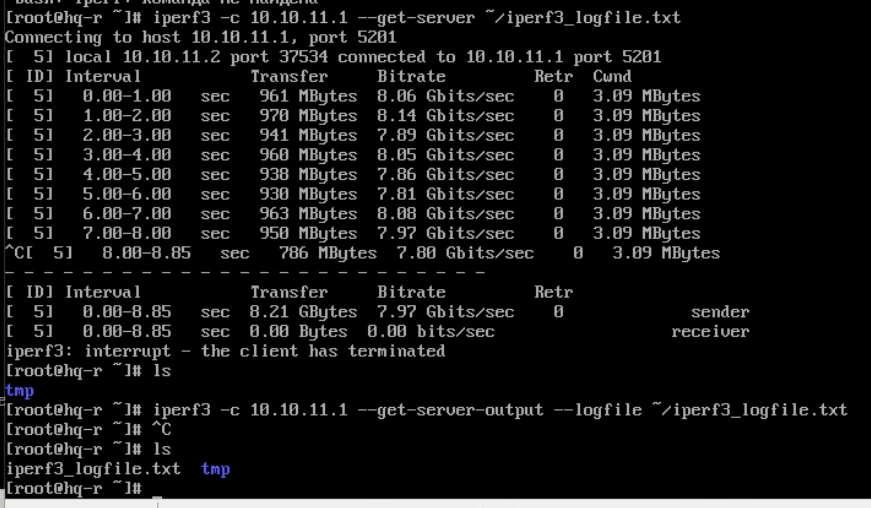
HQ-R

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

При помощи параметра "--get-server-output" - можно получить более детальный результат. При помощи параметра "--logfile /path/to/file" - можно указать путь к файлу в который записать вывод данной каманды в качестве отчёта

iperf3 -c IP\_address\_ISP --get-server-output --logfile ~/iperf3\_logfile.txt

# iperf3 -c IP\_address\_ISP



**Модуль 1 задание 6**

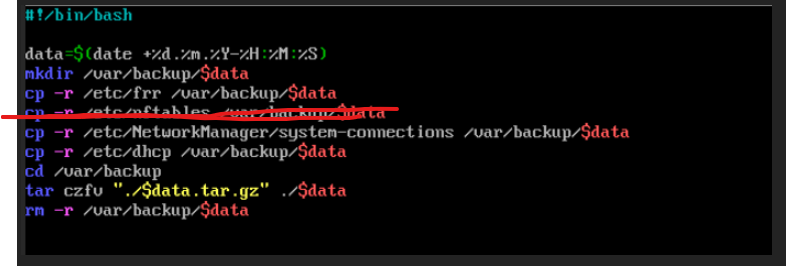
Составьте backup скрипты для сохранения конфигурации сетевых устройств, а именно HQ-R BR-R. Продемонстрируйте их работу.

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"

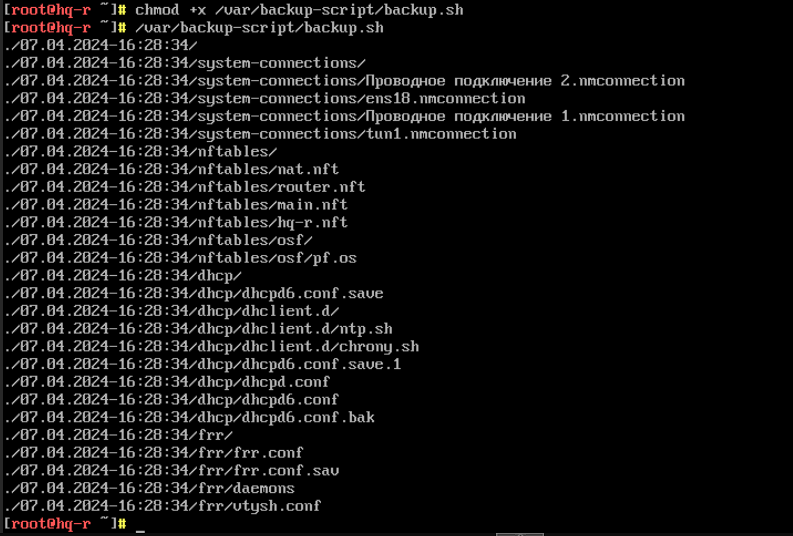
echo "Done" добавить в начало и конец

Присвоение права скрипту на выполнение:

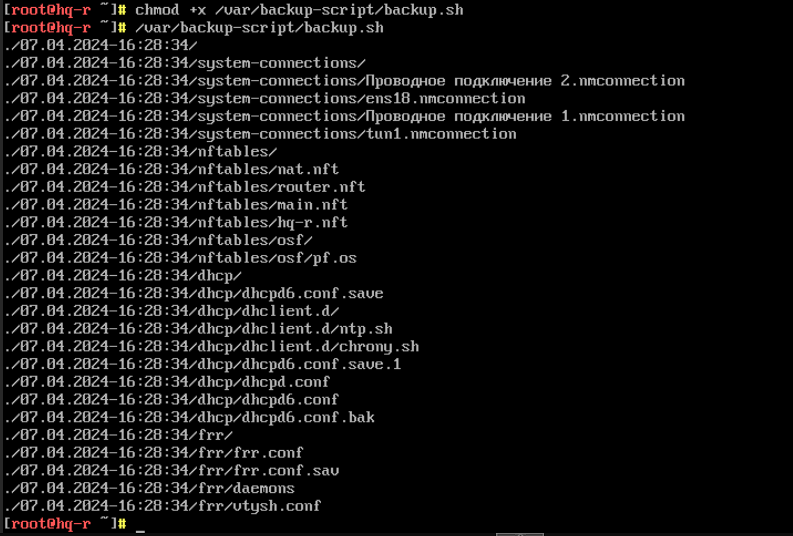
# chmod +x /var/backup-script/backup.sh

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 2020. Учтите, что вам необходимо перенаправить трафик на этот порт посредством контролирования трафика.

HQ-SRV

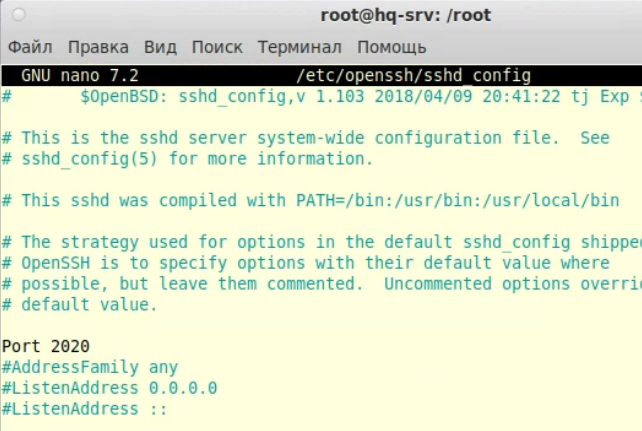
nano /etc/openssh/sshd\_config

# Раскомментируйте и измените следующую строку

PermitRootLogin yes

порт ssh прописать тот, который указан в задании

ПОРТ ЗАВИСИТ ОТ ЗАДАНИЯ



#systemctl restart sshd

Для ipv4

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

Сохранение правила iptables:

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

Сохранение правила ip6tables:

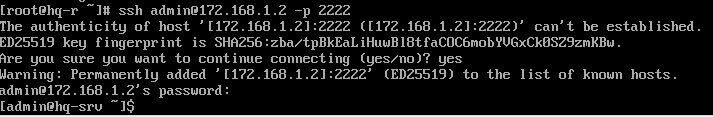
ip6tables-save >> /etc/sysconfig/iptables6

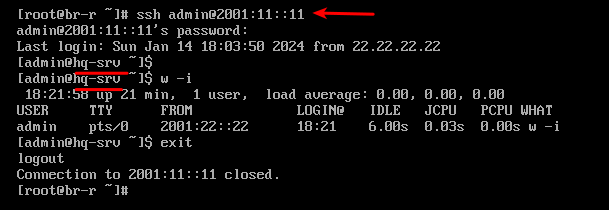
systemctl enable --now ip6tables

Перезапуск службы командой #systemctl restart sshd

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

ПОРТ ЗАВИСИТ ОТ ЗАДАНИЯ





Создадим следующее правило, которое будет перенаправлять внешние подключения на порт 22 -> на порт 2222 сервера HQ-SRV:

в таблицу nat в цепочку prerouting (до маршрутизации) добавляем правило:

iptables -t nat -A PREROUTING -i ens33(eth нужно) -p tcp --dport 22 -j DNAT --to-destination 192.168.100.1:2222

где:

-t nat - таблица nat;

-A PREROUTING - добавить правило в цепочку prerouting, выполняющееся до маршрутизации;

-i ens33 - внешний интерфейс;

-p tcp - порт TCP;

--dport 22 - порт назначения;

-j DNAT - "обратный" nat;

--to-destination - куда перенаправлять;



добавляем правило для IPv6, через ip6tables:

ip6tables -t nat -A PREROUTING -i ens33 -p tcp --dport 22 -j DNAT --to-destination [2000:100::1]:2222

Сохранение правила iptables:

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

Сохранение правила ip6tables:

ip6tables-save >> /etc/sysconfig/iptables6

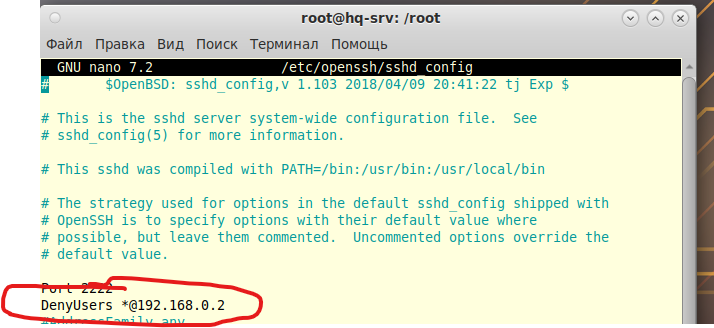
systemctl enable --now ip6tables

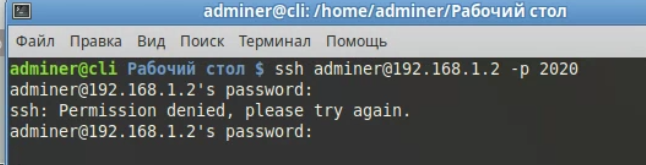
**Модуль 1 задание 8**

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

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

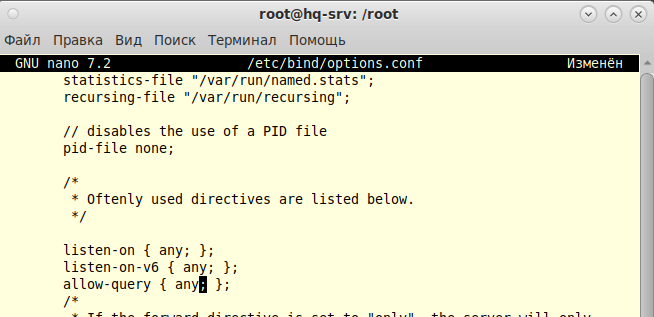
В нашем случае ip адресс 192.168.0.2





**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:

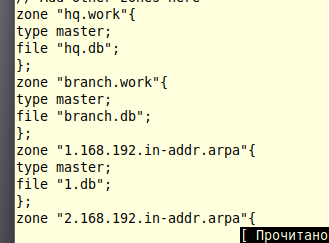
#systemctl enable --now bind

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 нужно зайти в /etc/bind/local.conf и вписать туда то, что указано на приведённом далее рисунке.



Далее необходимо прописать данные команды:

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

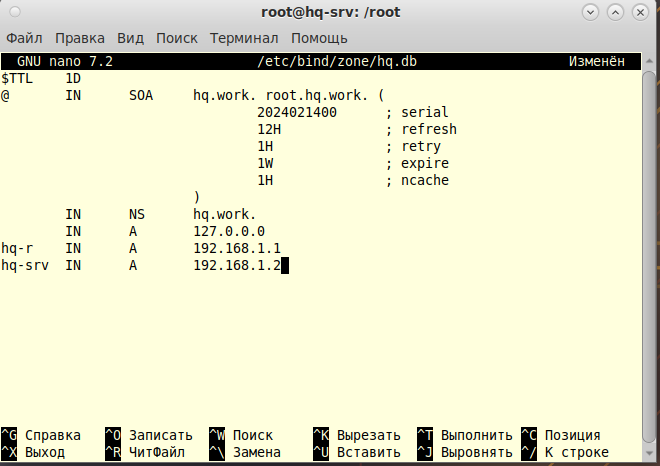
#cp /etc/bind/zone/{localdomain,branch.db}

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

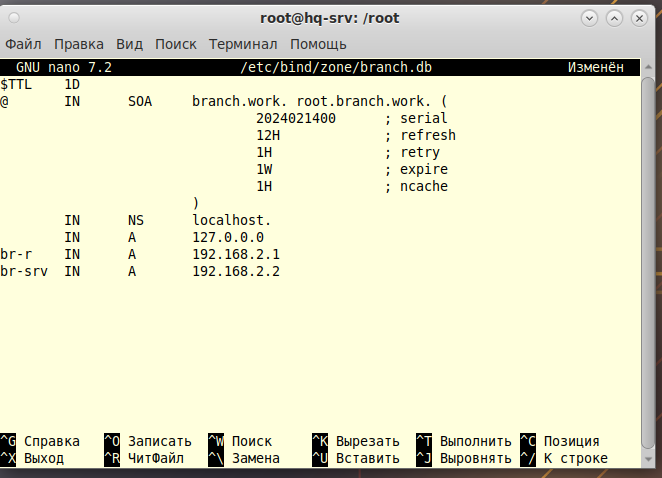
#cp /etc/bind/zone/{127.in-addr.arpa,2.db}

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

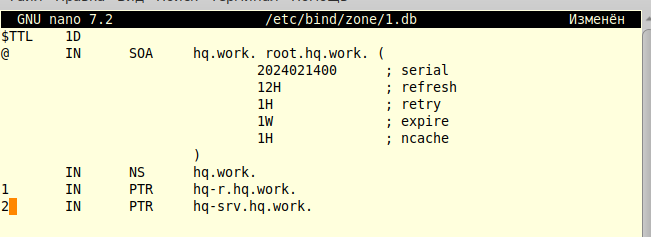
Далее нужно привести каталог /etc/bind/zone/hq.db как указано на приведённом далее рисунке.



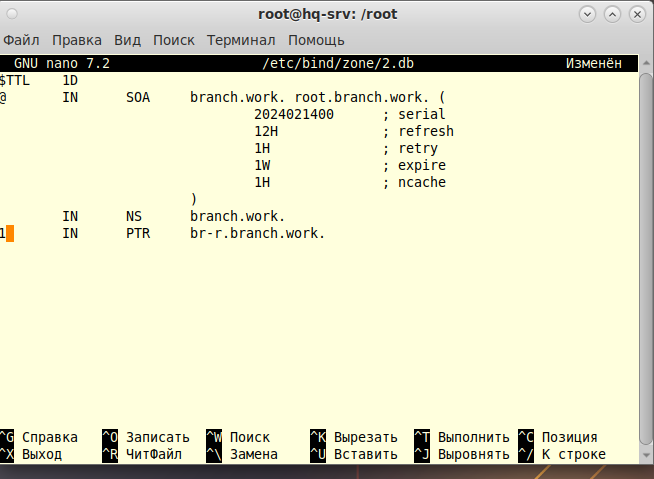
То же самое проделать в каталоге /etc/bind/zone/branch.db



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

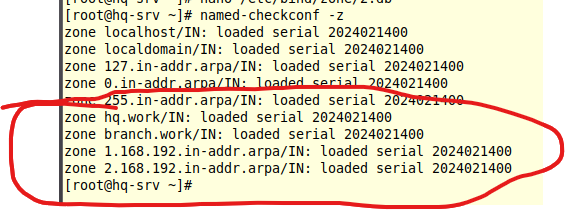


То же самое проделать в каталоге /etc/bind/zone/2.db



Проверить файлы зон можно утилитой named-checkconf:

# named-checkconf -z



Проверка

