**Рассчитываем ip-адресы сети согласно условиям**

|  |  |  |
| --- | --- | --- |
| Имя устройства | IP-адрес | Шлюз по умолчанию |
| ISP | dhcp |  |
| 172.16.4.14/28 |  |
| 172.16.5.14/28 |  |
| HQ-RTR | 172.16.4.1/28 | 172.16.4.14 |
|  | 192.168.0.62/26 |  |
|  | 192.168.0.78/28 |  |
|  | 192.168.0.86/29 |  |
| HQ-SRV | 192.168.0.1/26 | 192.168.0.62 |
| HQ-CLI | 192.168.0.65/28 | 192.168.0.78 |
| HQ-SW | 192.168.0.81/29 | 192.168.0.86 |
| BR-RTR | 172.16.5.1/28 | 172.16.5.14 |
|  | 192.168.1.30/27 |  |
| BR-SRV | 192.168.1.1/27 | 192.168.3.30 |

**1. Переименовать компьютеры**

**Настройка имени устройства (делается на всех устройствах)**

Заходим под пользователем root (рис. 1.1).

***root*** – ввод (Enter), ***toor*** – ввод (Enter)

рис. 1.1

Для смены имени устройства используется утилита hostnamectl ввод команды (рис. 1.2):

***hostnamectl set-hostname НОВОЕ\_ИМЯ; exec bash*** – ввод (Enter)

Рис. 1.2

**ВСЕ УСТРОЙСТВА кроме isp ИМЕНА ПРИСВАИВАЮТСЯ С ДОМЕННЫМ рис.1.3 (дан в задании «au-team.irpo») СУФФИКСОМ КРОМЕ ISP!!!!!**

**Рис. 1.3**

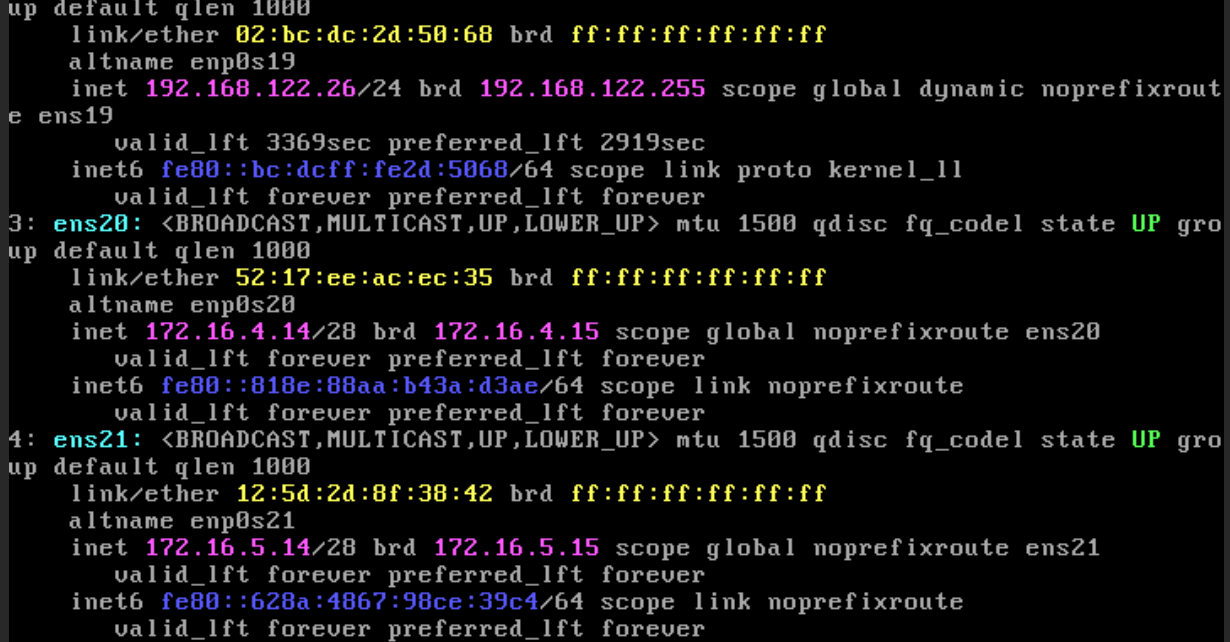
Имя устройства изменено.

**Данную операцию необходимо сделать на всех устройствах!**

**2. Настройка интернет интерфейсов (на ISP, HQ-R, BR-R)**

1) Проверить название и МАК адреса на соответствие с сетевыми картами, с помощью команды ip a (рис. 2.1):

***ip -c a*** – ввод (Enter)

Рис. 2.1

1- название интерфейса.

2- MAK-адрес

в) Для настройки с помошью nmtui

запускаем настройку интерфейсов командой nmtui (рис. 2.2):

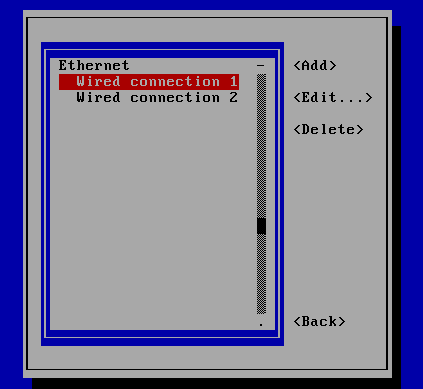
***nmtui*** – ввод (Enter)

Рис. 2.2

ё) Выбираем пункт ***Edit a connection*** (рис. 2.3):

Рис. 2.3

Выбираем соединения «Проводное соединение 1» нажимаем ввод (Enter) ( делаем со всем остальными проводными соединениями) (рис. 2.4).

Рис. 2.4

Настраиваем интерфейсы (рис. 2.5), выберем Manual или automatic в зависимости от необходимости.

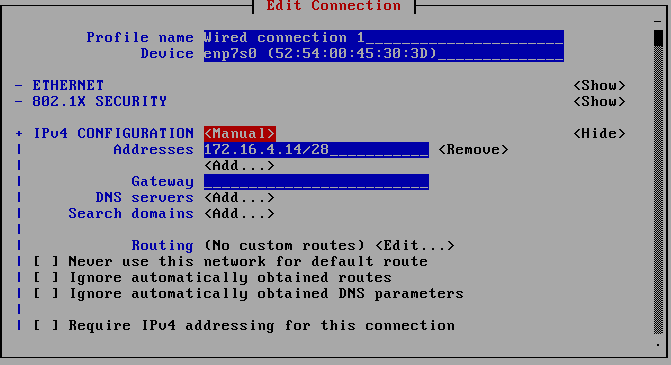
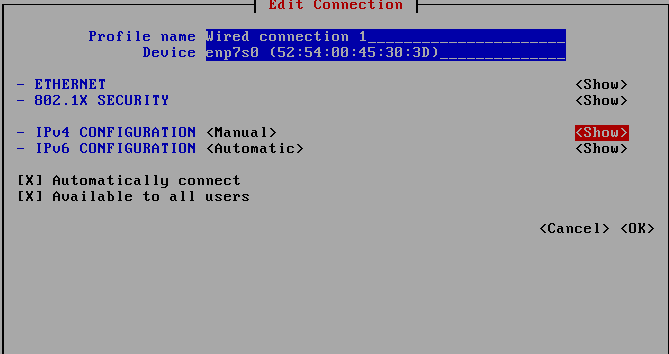
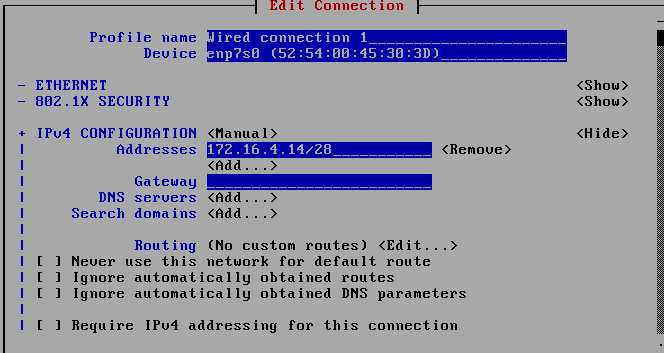


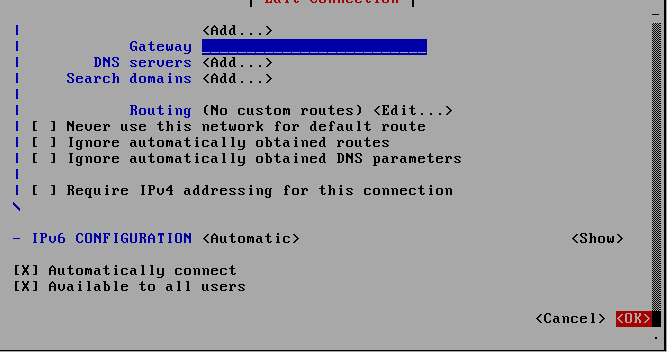
Рис. 2.5

нажимаем Show (рис.2.6)напротив необходимой версии протокола ( ipv4 или ipv6), настраиваем адресацию (ip, маску, шлюз (при необходимости) сохраняем нажатием кнопки «ОК» (рис. 2.7).



Рис. 2.7

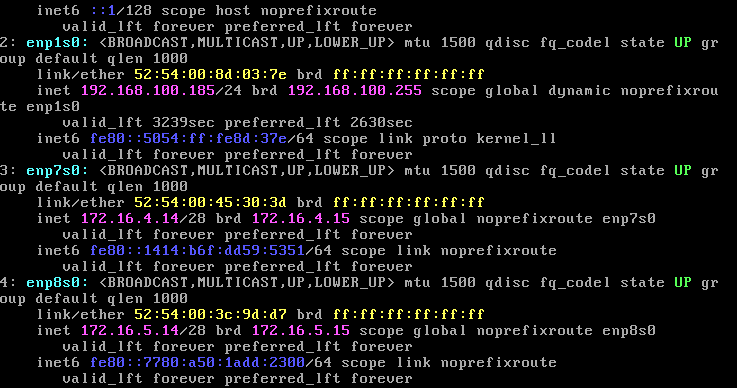
**Сохарянем параметры кнопкой «ОК» (рис. 2.8)**

Рис. 2.8

Перезапускаем NetworkManager (рис.2.9)

Проверяем настройку командой ip a (рис. 2.10).

***ip -с a*** – ввод (Enter)

Рис.2.10

Настройка адаптеров завершена.

**!!!НА HQ-RTR настраиваем только интерфейс смотрящий на ISP!!!!!!!**

**Проделываем данную операцию со всеми интерфейсами! На всех устройствах.**

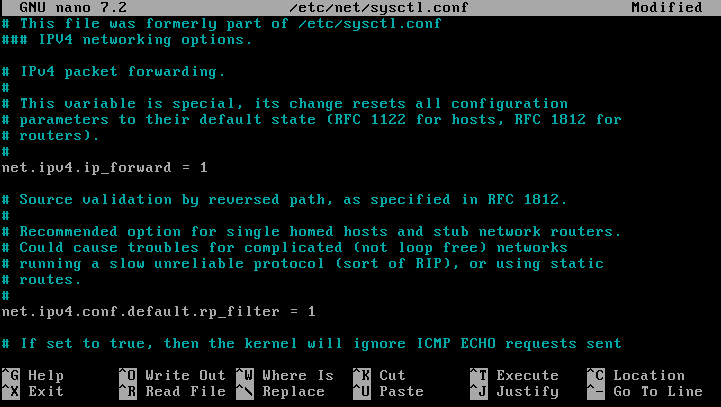
**3. Включение маршрутизации маршрутизаторах**

Включаем forwarding для IPv4 посредством редактирования файла по пути /etc/net/sysctl.conf (рис. 3.1):

***nano /etc/net/sysctl.conf*** – ввод (Enter)

Рис. 3.1

меняем параметр net.ipv4.ip\_forward=0 на 1. (рис. 3.2).

Рис. 3.2

сохраняем изменения ***ctrl+o, enter***.

Выходим ***ctrl+x***.

Вводим команду ***sysctl -p***.

**4. Выполняется для настройки доступа в Интернет из сетей (настраивается на ISP, HQ-R и BR-R):**

Включаем и добавляем в автозагрузку службу nftables (рис. 4.1):

***systemctl enable --now nftables*** – ввод (Enter)

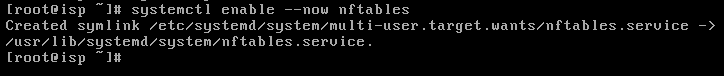


Рис. 4.1

Необходимо настроить файл конфигурации находящийся по адресу /etc/nftables/nftables.nft (рис. 4.2):

***nano /etc/nftables/nftables.nft***  – ввод (Enter)

Рис. 4.2

Далее необходимо добавить следующие таблицы и параметры (рис 4.3):

table inet nat {

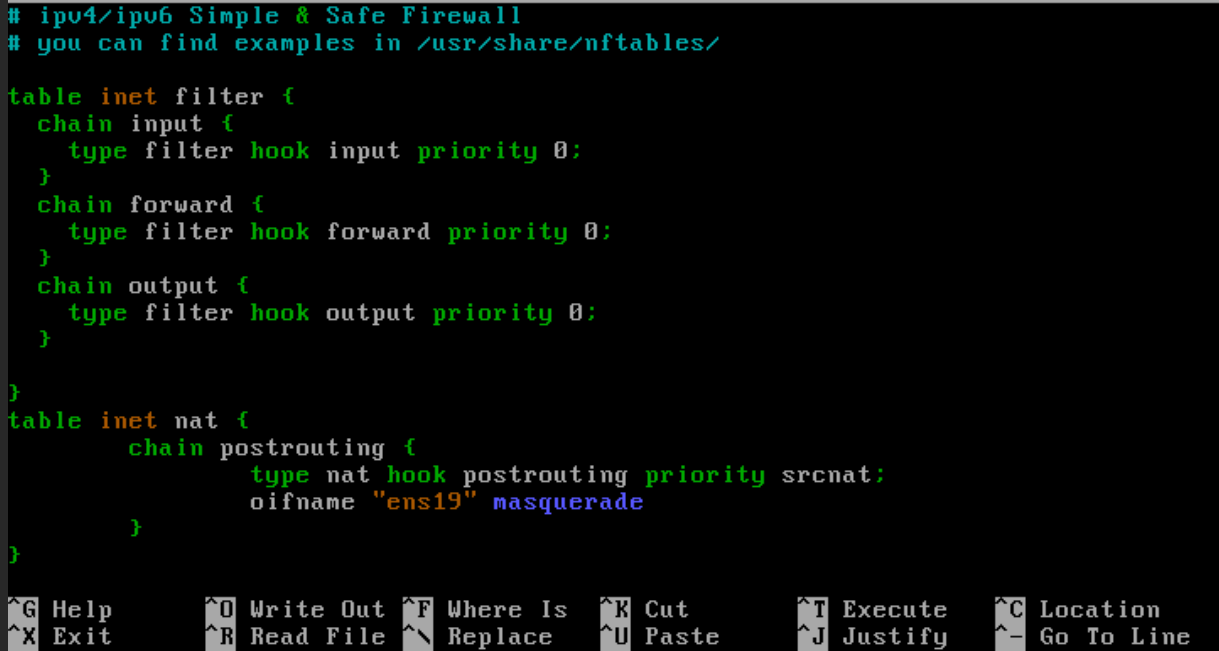
chain postrouting {

type nat hook postrouting priority srcnat;

oifname “ens19” masquerade

}

}

Рис. 4.3

Сохраняем конфигурацию и пере запускаем службу systemctl restart nftables (рис. 4.4):

**systemctl restart nftables** – ввод (Enter)

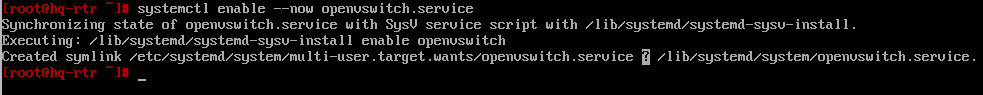
Рис. 4.4

**Настраиваем по аналогии на HQ-R и BR-R!**

**5. Настройка VLAN (ТОЛЬКО НА HQ-RTR)!!!**

Добавляем в автозагрузку и запускаем (рис. 5.2)

systemctl enable --now openvswitch

Рис.5.2

Создаем мост (виртуальный коммутатор) hq-sw, Добавляем порт ens20 к **hq-sw** и назначаем ему vlan100, Добавляем порт ens21 к **hq-sw** и назначаем ему vlan200, Добавляем порт ens22 к **hq-sw** и назначаем ему vlan999, Добавляем внутренний порт vlan100, vlan200, vlan999 к мосту ****hq-sw**** (рис. 5.3).

***ovs-vsctl add-br hq-sw***

***ovs-vsctl add-port hq-sw ens20 tag=100***

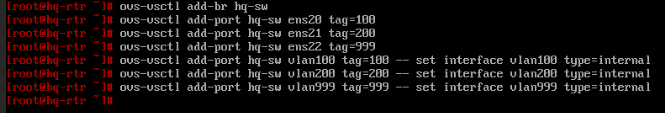
***ovs-vsctl add-port hq-sw ens21 tag=200***

***ovs-vsctl add-port hq-sw ens22 tag=999***

***ovs-vsctl add-port hq-sw vlan100 tag=100 -- set interface vlan100 type=internal***

***ovs-vsctl add-port hq-sw vlan200 tag=200 -- set interface vlan200 type=internal***

***ovs-vsctl add-port hq-sw vlan999 tag=999 -- set interface vlan999 type=internal***

Рис.5.3

**Перезагружаем openvswitch и NetworkManager (рис.5.4)**

***systemctl restart openvswitch***

***systemctl restart NetworkManager***

Рис.5.4

**Включаем мост (рис. 5.6)**

*****ip link set hq-sw up*****

****Рис.5.6****

**Создаем скрипт для настройки и восстановления настройки ip-адресов VLAN после перезагрузки!!!**

создаем скрипт

**nano ip.sh**

****

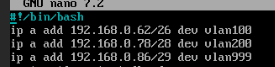
пишем текст скрипта:

**#!/bin/bash/**

**ip a add 192.168.0.62/26 dev vlan100**

**ip a add 192.168.0.78/28 dev vlan200**

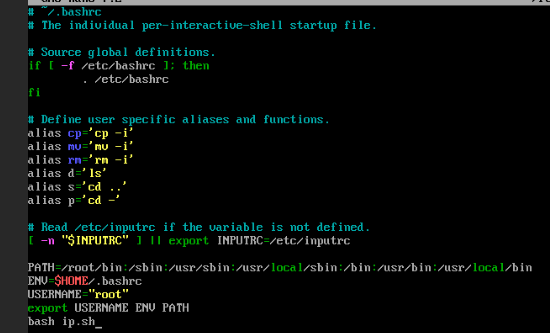
*****ip a add 192.168.0.86/29 dev vlan999*****

заходим добавляем запуск при загрузке

**nano `/.bashrc**

добавляем строчку, и сохраняем.

**bash ip.sh**

****

Запускаем скрипт

***bash ip.sh***

****

***Внимание!!!! при перезагрузки службы NM настройка IP слетают необходимо* ***необходимо в ручную запустить скрипт ip.sh или перегрузить ПК.*****

***6.***  **Настройте локальные учётные записи на устройствах в соответствии с заданием (на серверах пользователь sshuser c id 1010, на маршрутизаторах net\_admin)**

**Cервера (рис.6.1)**

***adduser sshuser -u 1010 -s /bin/bash***

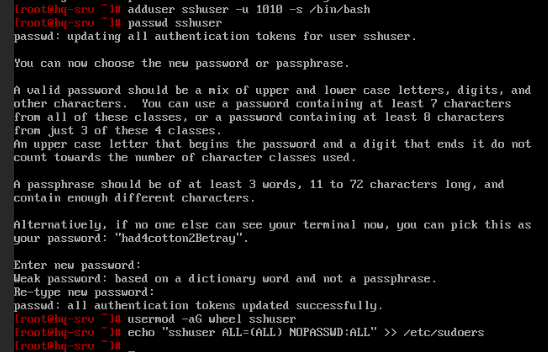
***passwd sshuser***

***P@ssw0rd***

***P@ssw0rd***

***usermod -aG wheel sshuser***

***echo "sshuser ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers***

***рис.6.1***

**Маршрутизатор (рис.6.2)**

***adduser net\_admin -s /bin/bash***

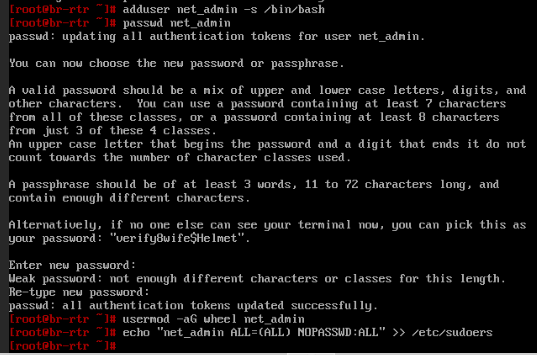
***passwd net\_admin***

***P@$$word***

***P@$$word***

***usermod -aG wheel net\_admin***

***echo "net\_admin ALL=(ALL:ALL) NOPASSWD: ALL" >> /etc/sudoers***

Рис. 6.2

**6. Настраиваем GRE-туннель между HQ-R и BR-R**

запускаем настройку интерфейсов командой nmtui (рис. 6.1):

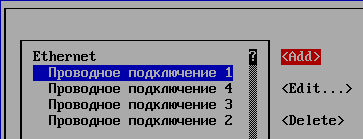
***nmtui*** – ввод (Enter)

Рис. 6.1

Выбираем "Edit a connection" (рис. 6.2):

Рис. 6.2

Выбираем "Add" (рис.6.3):

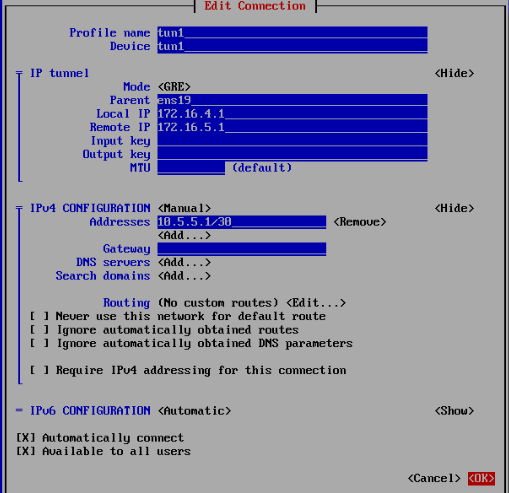
Рис. 6.3

Выбираем "IP tunnel" (рис. 6.4):

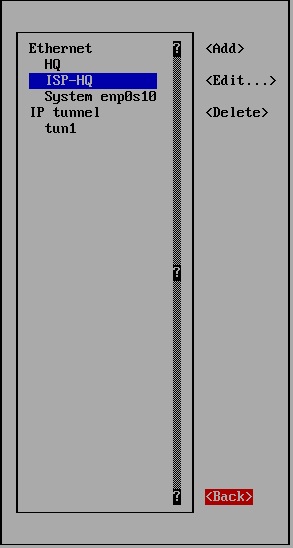
Рис. 6.4

Задаём имя тунеля tun1 -> в "Режим работы" выбираем "GRE" -> в "Родительский" указываем интерфейс ens19 (в сторону ISP) -> задаём "Локальный IP" -> задаём "Удалённый IP" , Переходим к конфигурации IPv4 , задаём параметр “Manual” прописываем адреса IPv4 для туннеля -> нажимаем "ОК" (рис. 6.5):

Рис. 6.5



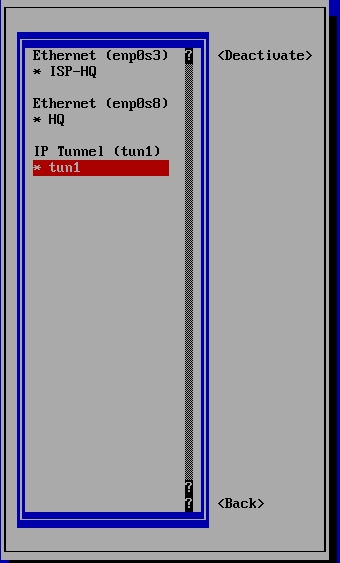
Выходим из редактирования туннеля «<Back>” (рис. 5.7)

Рис. 5.7

заходим в раздел «Activete a connection” (рис. 5.8)

Рис. 5.8

Выбираем туннель tun1 (параметр стоит «Deactivate») и нажимаем enter, выберем снова tun1 (\*параметр стоит «Activate») и нажимаем enter (рис. 5.9)

Рис. 5.9

Выходим из раздела «<Back>”.

Для корректной работы протокола динамической маршрутизации требуется увеличить параметр TTL на интерфейсе туннеля используется команда (рис. 6.10):

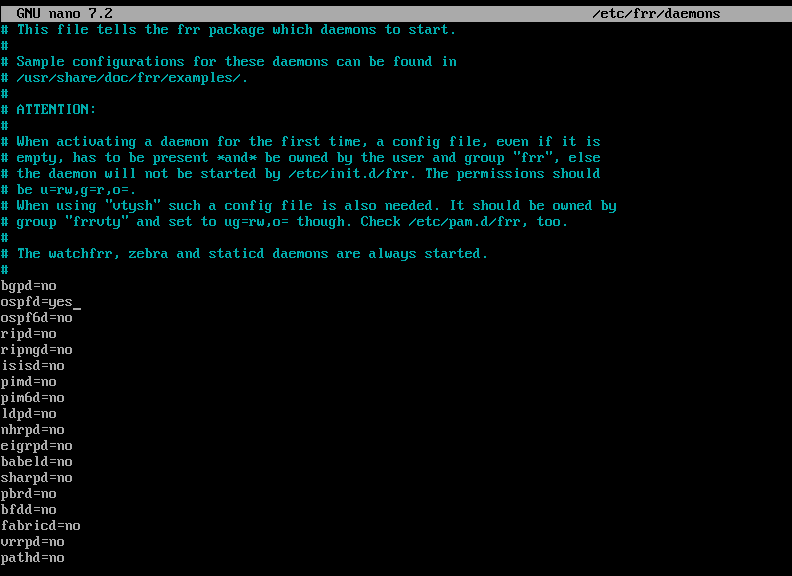
***nmcli connection modify tun1 ip-tunnel.ttl 64*** – ввод (Enter)

Рис.6.10

**Настройка динамической (внутренней) маршрутизации средствами frr.**

В конфигурационном файле "/etc/frr/daemons" (рис.6.11) необходимо активировать выбранный протокол OSPFv2. Переводим ospfd=no в ospfd=yes - для OSPFv2 (IPv4).

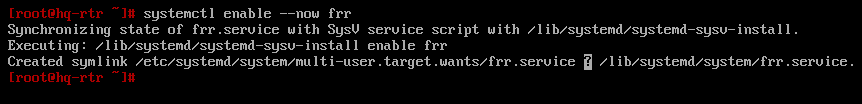
***nano /etc/frr/daemons*** – ввод (Enter)

Рис. 6.11

Сохраняем конфигурацию.

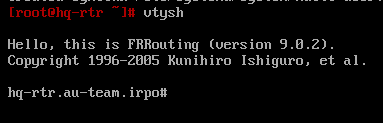
Включаем и добавляем в автозагрузку службу frr (рис. 5.12)

***systemctl enable --now frr*** – ввод (Enter)

Рис.5.12

Настраиваем OSPFv2 - переходим в интерфейс frr при помощи "vtysh" (рис. 5.13):

**vtysh** – ввод (Enter)

Рис. 5.13

переходим в режим конфигурирования (рис. 6.14) ***conf t*** – ввод (Enter). Командой router ospf переходим в конфигурирования протакола OSPFv2, переводим все интерфейсы в пассивный режим командой passive-interface default

***conf t***– ввод (Enter)

***route ospf***– ввод (Enter)

***passive-interface default*** – ввод (Enter)

***network 10.5.5.0/30 area 0*** – ввод (Enter), адрес сети тунеля

***network 192.168.0.0/26 area 0*** – ввод (Enter), адрес сети (внутренней сети в сторану HQ-SRV)

***network 192.168.0.64/28 area 0*** – ввод (Enter), адрес сети (внутренней сети в сторану HQ-CLI)

***network 192.168.0.80/29area 0*** – ввод (Enter), адрес сети (внутренней сети в сторану SW)

***area 0 authentication*** – ввод (Enter) Настройка аутентификации для области

***ex*** – ввод (Enter)

Переходим в конфигурацию тунеля (рис. 5.14), сохраняем настройку командой wr.

***interface tun1*** – ввод (Enter)

***no ospf network broadcast*** – ввод (Enter)

***no ip ospf passive*** – ввод (Enter)

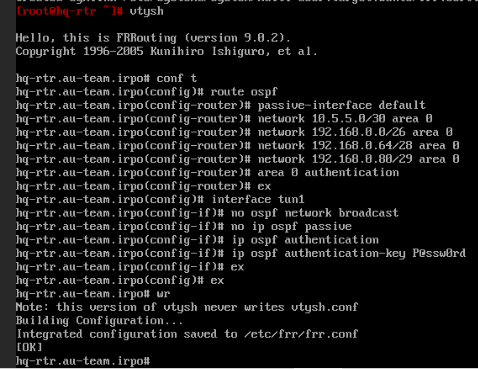
***ip ospf authentication*** – ввод (Enter) Настройка аутентификации

***ip ospf authentication-key*** [***P@ssw0rd***](mailto:P@ssw0rd)– ввод (Enter) задаем пароль P@ssw0rd

***ex*** – ввод (Enter)

***ex*** – ввод (Enter)

***wr*** – ввод (Enter)

Рис. 5.14

Выходим из vtysh

***ex*** – ввод (Enter)

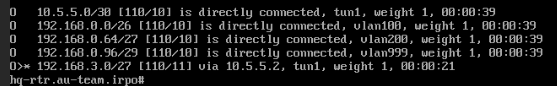
Перезапускаем FRR

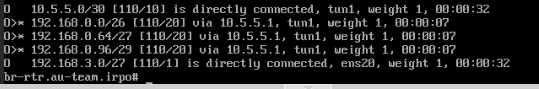
***systemctl restart frr***

ПРИМЕЧАНИЕ!!! может потребоваться перезагрузка BR-RTR и HQ-RTR, после нее канал поднимится.

Проверяем конфигурацию заходим во vtysh, если есть ip-адреса всех сетей со звездочкой адреса удаленных подсетей (рис. 5.16):

***show ip route ospf*** – ввод (Enter)

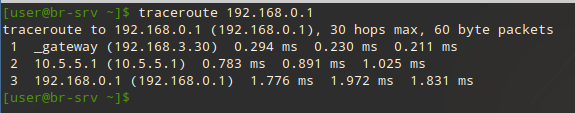
Рис. 5.17 а (br-rtr)

Рис.5.17 б (hq-rtr)

выходим из VTYSH командой **ex**.

Проверяем маршрут с BR-SRV до HQ-SRV (рис. 5.19) через терминал :

***traceroute 192.168.0.1*** – ввод (Enter)

Рис. 5.19

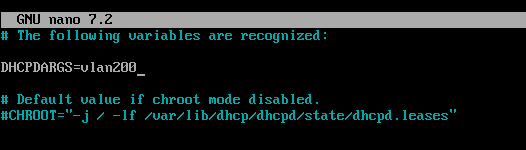
Настройка завершена.

**6 . Настройка DHCP-сервера для IPv4**

Укажим сетевой интерефейс для IPv4, через который будет работать DHCP-сервер

***nano /etc/sysconfig/dhcpd*** – ввод (Enter)

В пункт DHCPDARGS= необходимо добавить имя сетевого интерфейса vlan200 смотрящий в локальную сеть офиса HQ (рис. 6.1):

Рис. 6.1

Сохраняем параметр и выходим.

Следующим шагом настраиваем сервер:

копируем настройки по умолчанию (рис.6.2)

***cp /etc/dhcp/dhcpd.conf.example /etc/dhcp/dhcpd.conf*** – ввод (Enter)

подтверждаем

***y*** – ввод (Enter)

Рис. 6.2

Заходим в файл настройки

***nano /etc/dhcp/dhcpd.conf***– ввод (Enter)

Вносим параметры (рис. 6.3), остальные закоменчиваем:

***subnet 192.168.0.64 netmask 255.255.255.240 {***

***range 192.168.0.65 192.168.0.75;***

***option routers 192.168.0.78;***

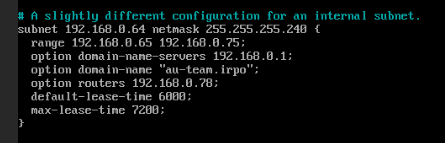
***option domain-name-servers 192.168.0.1;***

***option domain-name "au-team.irpo";***

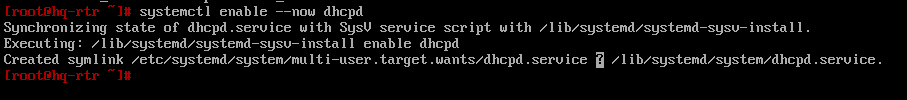
***default-lease-time 6000;***

***max-lease-time 7200***

***}***

рис. 6.3

***systemctl enable --now dhcpd*** – ввод (Enter)

 Рис. 6.4

Настраиваем динамическое получения ip-адреса на HQ-SRV (рис).

Заходим на сервер и проверяем полученый ip-адрес (рис. 6.13)

***ip a*** – ввод (Enter)

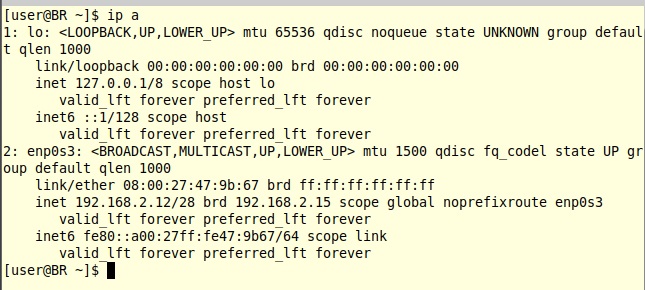


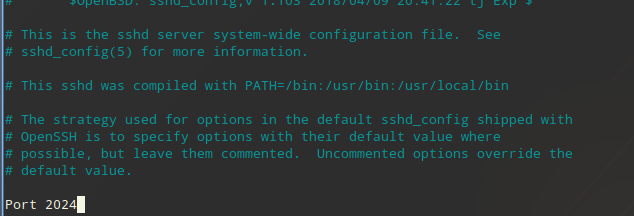
Рис. 6.13

**7. Настройте подключение по SSH для удалённого конфигурирования устройства HQ-SRV и BR-SRV .** (рис. 7.1):

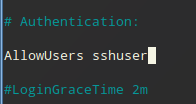
***nano /etc/openssh/sshd\_config*** – ввод (Enter)

Рис. 7.1

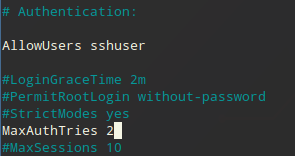
Комментируем Port и изменим 22 на 2024 (рис. 7.2)

Рис. 7.2

Добавляем следующую строку: AllowUsers sshuser (рис.7.3)

Рис.7.3

Находим директиву MaxAuthTries - количество попыток ввода паролю, снимаем комент и ставим значение 2 (рис. 7.4)

Рис.7.4

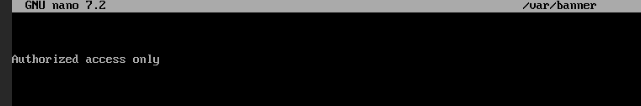
Находим директиву # Banner none. Снимаем комментарий и указываем путь к файлу /var/banner, который будет содержать текст баннера (рис.7.5).

Рис.7.5

сохраняем файл.

Заходим в banner и редактируем его (Рис.7.6)

nano /var/banner

Рис.7.6

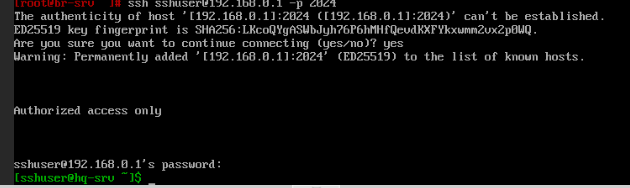
Сохраняем.

Перезапустим службу ssh (рис. 7.7):

***systemctl restart sshd*** – ввод (Enter)

Рис. 7.7

Проверяем настройку с любого устройства, через терминал подключаемся к HQ-SRV (рис.7.8)

Рис 7.8

****8. Настройка DNS для офисов HQ и BR.****

* Основной DNS-сервер реализован на HQ-SRV.
* Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 2
* В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер

# Редактируем конфигурационный файл /etc/bind/options.conf

nano /etc/bind/options.conf

****В данном файле необходимо изменить следующие строки, содержащие****

****listen-on port 53 {127.0.0.1; 192.168.0.0/26; 192.168.0.64/28; 192.168.1.0/27; 192.168.0.80/29;};****

****listen-on-v6 { none; };****

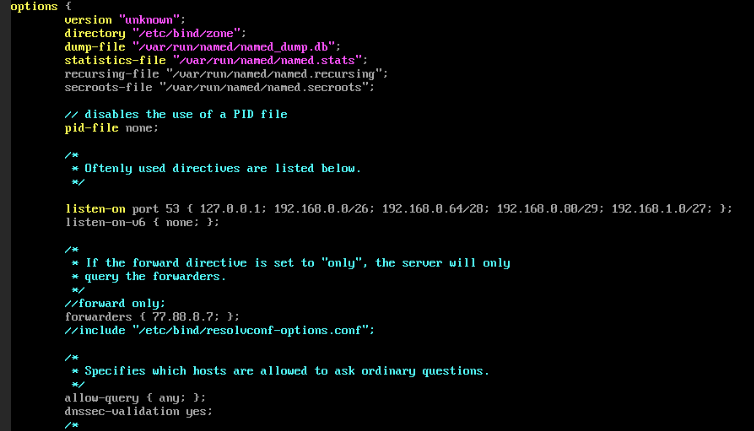
****forvarders { 77.88.8.7;}:** - снять комментирование и добавить ip**

****// include /etc/bind/resolfconf-options.conf;** - закомментировать!!!!**

****allow-query { any; };****

****dnssec-validation yes****

****и привести их к виду****

****

**Объявляем файлы зон, дописываем в конец файла /etc/bind/local.conf следующие строки, комментируем строки как указано на рисунке.**

****где:****

****Прямая зона****  
****zone "au-team.irpo"{ ... };**** определения зоны au-team.irpo. В кавычках указывается имя зоны, которое следует разрешать на этом сервере.

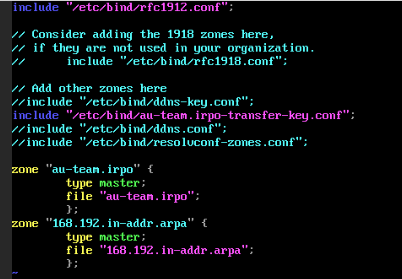
****type master**** ; Указывает тип зоны. type master означает, что эта зона является мастер-зоной, то есть она содержит авторитетные записи, которые могут быть изменены и обновлены на этом сервере.

****file "au-team.db";**** Указывает путь к файлу, который содержит данные зоны au-team.irpo. Файлы зоны используются для хранения записей DNS, таких как A-записи, CNAME-записи, MX-записи и т. д.

****Обратная зона****  
****zone "0.168.192.in-addr.arpa"{ ... };**** определения обратной зоны au-team.irpo.

****type master****; Указывает тип зоны. type master означает, что эта зона является мастер-зоной, то есть она содержит авторитетные записи, которые могут быть изменены и обновлены на этом сервере.

****file "au-team\_rev.db";**** Указывает путь к файлу обратной зоны, который содержит данные обратной зоны au-team.irpo.

****

## Создание локальных зон DNS

****Зона прямого просмотра****

Для сокращения времени написания файла прямой зоны (au-team.irpo) скопируем шаблон и отредактируем его

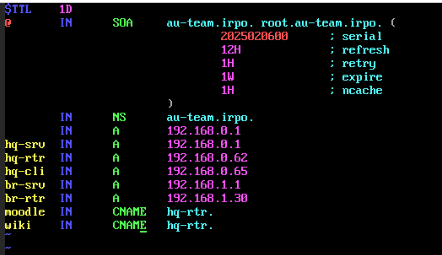
# cp /etc/bind/zone/localdomen /etc/bind/zone/au-team.irpo



Открываем на редактирование файл зоны au-team.irpo

nano /etc/bind/zone/au-team.irpo

****И приводим его к следующему виду****

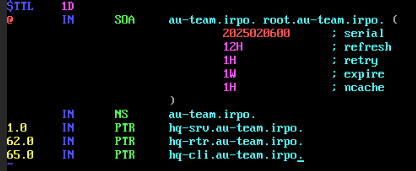
****Зона обратно********го просмотра****

Для сокращения времени написания файла обратной зоны (0.168.192.in-addr.arpa) скопируем шаблон и отредактируем его

***# cp /etc/bind/zone/127.in-addr.arpa /etc/bind/zone/.168.192.in-addr.arpa***

Открываем на редактирование файл зоны *168.192.in-addr.arpa и 3.168.192.in-addr.arpa*

nano /etc/bind/zone/*168.192.in-addr.arpa*

И приводим его к следующему виду

****С помощью утилиты**** named-checkconf ****проверяется наличие ошибок в конфигурационном файле, если результат выполнения команды пуст - ошибок нет.****

***Named-checkconf***

******

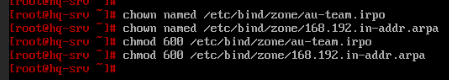
**Назначаем владельца и права.**

*****chown named /etc/bind/zone/au-team.irpo.db*****

*****chown named /etc/bind/zone/0.168.192.in-addr.arpa*****

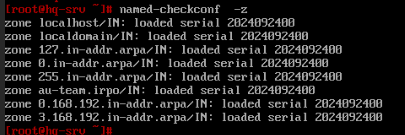
*****chmod 600 /etc/bind/zone/au-team.irpo.db*****

*****chmod 600 /etc/bind/zone/0.168.192.in-addr.arpa*****

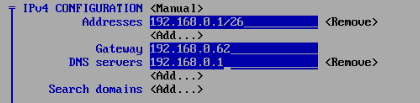
******

****С помощью утилиты**** named-checkconf -z ****проверяется наличие ошибок в конфигурационном файле и файлах зон.****

*****named-checkconf -z*****



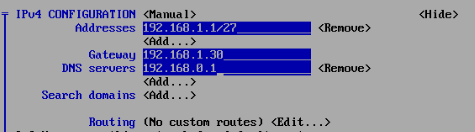
На HQ-SRV в настройках сетевого интерфейса убедиться, что в качестве первичного DNS сервера указан его собственный IP – адрес



Также необходимо проверить

на BR-SRV, что в качестве первичного DNS сервера указан IP – адрес HQ-SRV

перезапускаем службу NetworkManager

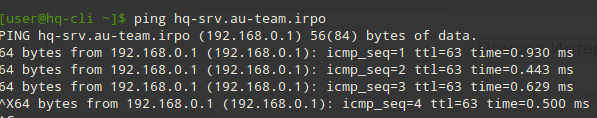


HQ-CLI - должен получать автоматически по DHC

****Запуск и добавление в автозагрузку DNS — сервера:****

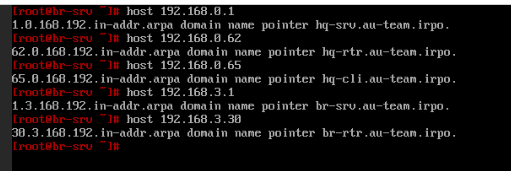
systemctl enable --now bind

***Тестирование***



****Обратная зона****

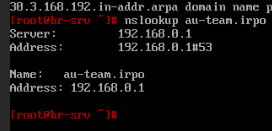
****Проверяем работу DNS на HQ-SRV с BR-SRV с помощью команды**** host



****Проверка работоспособности DNS с помощью**** nslookup

Для определения IP-адреса сервера по его доменному:

# nslookup <доменное\_имя>

****9. Настроим Московский часовой пояс (UTC +3):****

****timedatectl set-timezone Europe/Moscow****

****Проверка:****

timedatectl

