Мне не лень оформлять (Рахвалов Роман)

Login: root

Password: toor

Для клиента: пароль от user – user

Для того, чтобы на клиенте зайти в root, написать su- в терминале и ввести пароль toor

<https://jodies.de/ipcalc> - ip-калькулятор

ip a – выводит список интерфейсов

ls -l “директория” – выводит список папок в директории

cat “директория и в конце название файла” – показывает, что находится в файле

cd "директория" – переход в директорию

/etc/net/ifaces

apt-get update

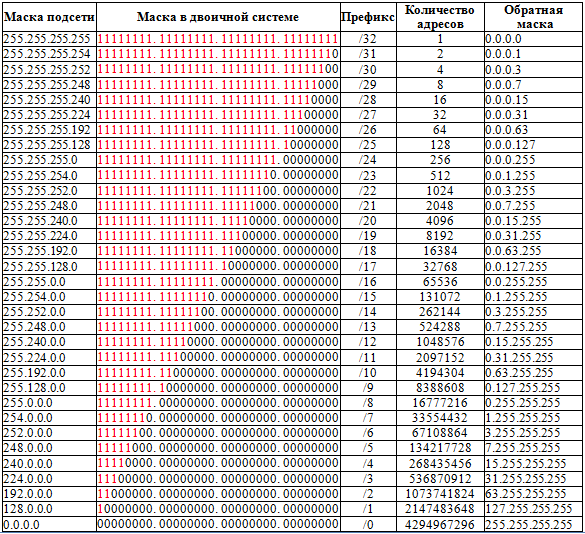
systemctl restart network

Если что-то не получается, не пингуется сеть или ещё что-то, то сначала нужно проверить настройки самой виртуалки. Нажать правой кнопкой мыши и выбрать “Edit settings”, посмотреть соединения, проверить MAC-адреса.

**Таблица адресов:**



# Таблица масок





# МОДУЛЬ 1

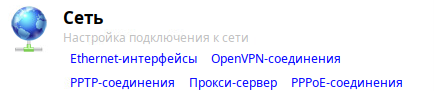
# 1. Смена имени хоста

На устройствах нужно поменять имя хоста. Сделать это нужно в файле **hostname** в директории /etc. Для ISP оставим просто isp. Для остальных устройств нужно писать полное доменное имя: /etc/hostname

| **Устройство** | **Запись** | **Тип** |
| --- | --- | --- |
| HQ-RTR | hq-rtr.au-team.irpo | A,PTR |
| BR-RTR | br-rtr.au-team.irpo | A |
| HQ-SRV | hq-srv.au-team.irpo | A,PTR |
| HQ-CLI | hq-cli.au-team.irpo | A,PTR |
| BR-SRV | br-srv.au-team.irpo | A |
| HQ-RTR | moodle.au-team.irpo | CNAME |
| HQ-RTR | wiki.au-team.irpo | CNAME |

Проверить имя хоста можно командой hostnamectl

На HQ-CLI сменить имя в графике. Нажимаем лкм на пуск («Меню»). Затем «Центр управления», далее «Центр управления системой». В нём найти «Сеть» и выбрать «ethernet-интерфейсы».



Изменить имя компьютера, применить

Сделать таблицу адресов, а потом занести эти данные в отчёт (пример таблица 3)

# 2. Настройка ISP

**По заданию:**

* интерфейс, который подключён к облаку «Internet», получает адрес по DHCP.
* Интерфейс, к которому подключён HQ-RTR, подключён к сети 172.16.4.0/28
* Интерфейс, к которому подключён BR-RTR, подключён к сети 172.16.5.0/28
* На ISP должны быть настроены сетевая трансляция в сторону HQ-RTR и BR-RTR и интернет

**Выполнение задания:**

Проверяем какие интерфейсы у нас есть при помощи команды:

[root]# ip a

В выводе команды у нас есть несколько разных интерфейсов. «lo» нас не интересует. Остаются «en или ens…» что-то там.

Затем нам нужно отредактировать файл конфигурации этого интерфейса. Здесь есть 2 путя (как в анекдоте). Можно редактировать через vim. Можно средствами командной строки. Так как я задрот, а за vim не шарю, то предлагаю второй путь.

Проверяем что есть в директории с интерфейсами:

[root]# ls -l /etc/net/ifaces

Если нет нужной директории, то создаём её:

[root]# mkdir -p /etc/net/ifaces/наш\_интерфейс (ens192)

После того как создали директорию, нужно в неё зайти командой:

[root]# cd /etc/net/ifaces/наш\_интерфейс

Далее нужно создать в директории файл options:

[root]# touch options

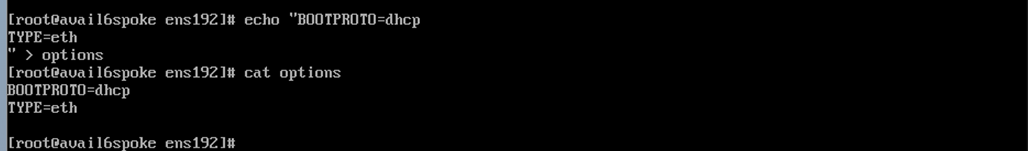
Редактируем файл при помощи команды echo:

[root]# echo "BOOTPROTO=dhcp(нажимаем Enter)

TYPE=eth (нажимаем Enter)

DISABLED=no (нажимаем Enter)

CONFIG\_IPV4=yes (нажимаем Enter)

" > options

Разберём эту команду:

echo (буквально «эхо») выводит текст в кавычках на экран.

Символ «>» (> options) – перенаправляет вывод в файл, то есть указываем стрелочкой куда записать информацию (типо выводил на экран, теперь в файл).

options – это наш файл. И в конце файла должна быть пустая строка (потому что линукс).

Проверяем содержимое файла options (в котором пока ничего нет):

[root]# cat options

Перезапустим сеть командой:

[root]# systemctl restart network

Проверим интернет:

[root]# ping 77.88.8.8 или 8.8.8.8

Если пингуется, то интернет есть. А если есть интернет, то это значит, что можно скачать mc и накатить обновления:

[root]# apt-get update

~~# apt-get dist-upgrade (опционально)~~

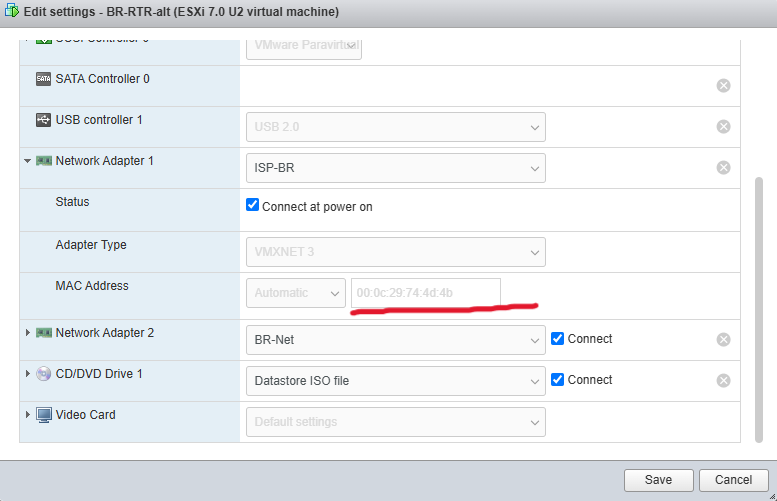
Скачиваем mc:

[root]# apt-get install mc

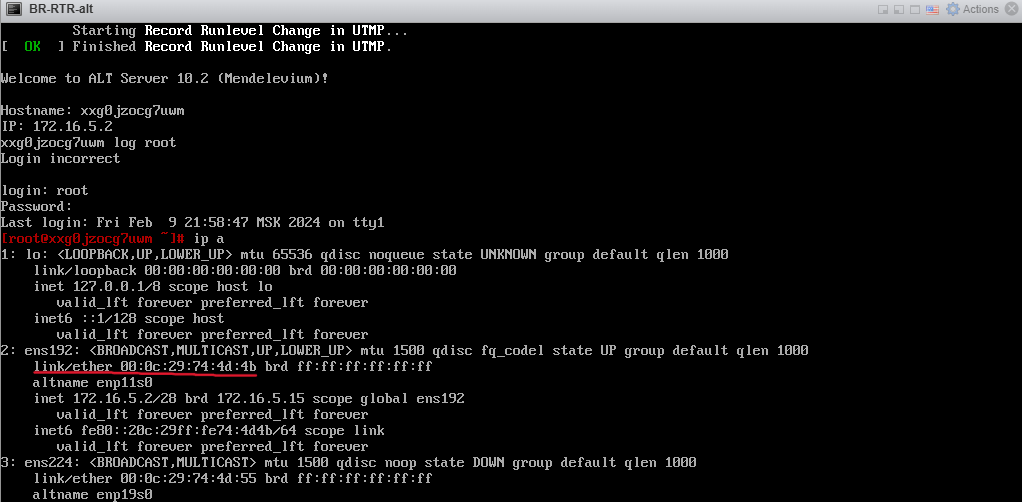
**С этого момента всё, что можно сделать в mc, мы делаем в mc, потому что на остальных устройствах mc УЖЕ УСТАНОВЛЕН.**

Теперь нужно создать 2 директории под 2 интерфейса. Мы нормальные и скачали mc, поэтому мы создаём директории при помощи него. В этих директориях нужно создать 2 файла – options (который создавался ранее) и ipv4address

**ВАЖНО. Прежде чем назначать ip-адреса интерфейсам, нужно сверить MAC-адреса и сопоставить с соединением роутера**



MAC-адрес интерфейса роутера в настройках esxi



MAC-адрес при выводе команды ip a

Создаём файл **ipv4address**, в котором прописываем статическую настройку:

[root]# touch ipv4address (в директории интерфейса ( не ens192))

И в файле прописываем адрес нашей сети (например, 172.16.4.1/28):



[root]# touch options

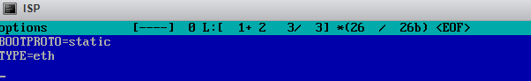
В этом файле прописываем:

BOOTPROTO=static

TYPE=eth

DISABLED=no

CONFIG\_IPV4=yes



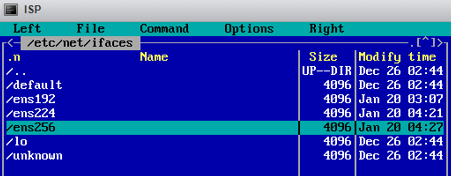
**//Не забываем про то, что последняя строка должна быть пустая//**

Те же самые инструкции повторяем для второго интерфейса, а сеть прописываем другую (172.16.5.1/28)

[root]# mkdir etc/net/ifaces/название\_2ого\_интерфейса/

[root]# touch ipv4address

[root]# touch options



Директории интерфейсов с файлами настроек

В завершении настройки ISP в файле sysctl.conf в директории /etc/net включим форвардинг.

В файле в строчке «net.ipv4.ip\_forward = 0» изменить 0 на 1.

# **2.2 Установка и настройка nftables на ISP**

Устанавливаем nftables:

apt-get update

apt-get install -y nftables

Включаем и добавляем в автозагрузку службу nftables:

systemctl enable --now nftables (перед now два маленьких тире -)

**Настройка nftables:**

Далее создаём необходимую структуру для nftables (семейство, таблица, цепочка) для настройки NAT:

Cоздаём в семействе ip таблицу nat:

nft add table ip nat

Cоздаём цепочку postrouting в таблице nat семейства ip, также задаём hook и priority:

nft add chain ip nat postrouting ‘{ type nat hook postrouting priority 0; }’

Cоздаём правила настройки NAT в семействе ip, таблице nat, цепочке postrouting:

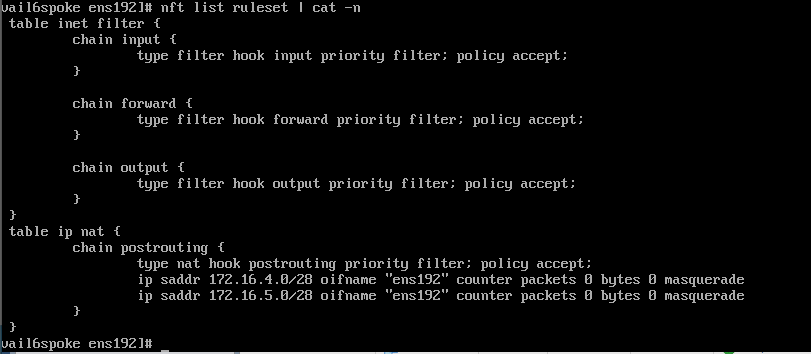
nft add rule ip nat postrouting ip saddr 172.16.4.0/28 oifname “ens192” counter masquerade

nft add rule ip nat postrouting ip saddr 172.16.5.0/28 oifname “ens192” counter masquerade

**//вместо 172.16.4.0/28 написать подсети роутеров, а вместо «ens192» написать интерфейс, который получает dhcp(интернет)//**

После этого нужно проверить командой:

nft list ruleset | cat -n



nftables с нашими сетями

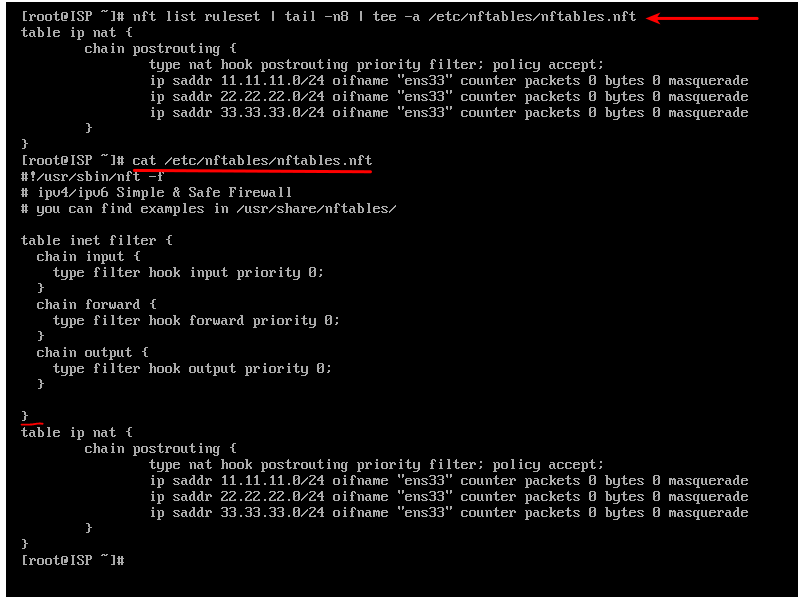
Сохраняем правила nftables:

Так как в конфигурационном файле /etc/nftables/nftables.nft уже есть информация о таблице filter – необходимо дописать только что созданную информацию о таблице nat:

дозапишем в конфигурационный файл /etc/nftables/nftables.nft последние 7 строк (от 14 до 21) вывода команды nft list ruleset:

nft list ruleset | tail -n7 | tee -a /etc/nftables/nftables.nft ( **если 2 подсети - ISP и HQ-RTR**)

nft list ruleset | tail -n6 | tee -a /etc/nftables/nftables.nft (**если 1 подсеть - BR-RTR**)

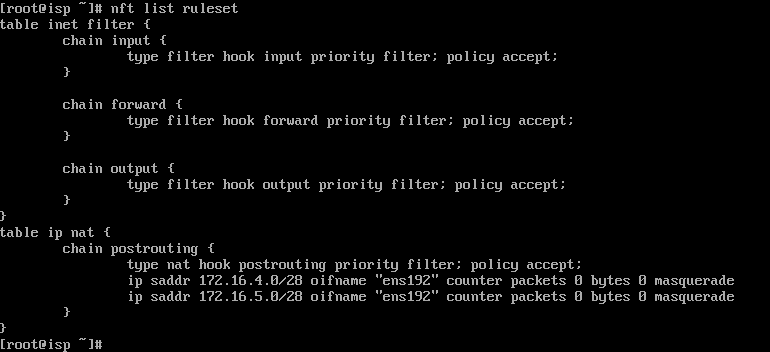
  
Пример из гайда

Для проверки перезагружаем службу nftables:

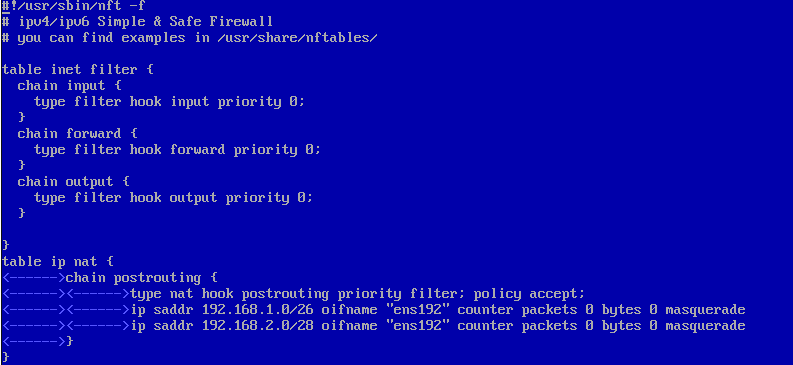
systemctl restart nftables

Смотрим правила:

nft list ruleset

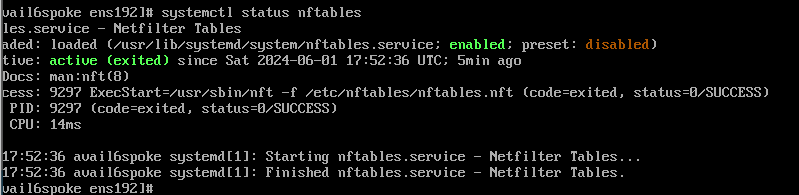


Может быть такое, что nftables могут не работать из-за лишней скобки. Для этого идём в конфиг в директории /etc/nftables/**nftables.nft** и проверяем. Если есть лишняя скобка, то удаляем её в конфиге, сохраняем, перезапускаем службу командой systemctl restart nftables.



пример конфига nftbales.nft в mc

Проверить работу можно командой systemctl status nftables



# Задание 4. Виртуальный коммутатор

**Примечание.** Так как площадки изменились, то действия до 6 рисунка делать не нужно.

Заходим в боковую панель ESXI с иконкой интернет («Networking») и выбираем «Virtual Switches». Нажимаем «Add standard virtual switch».

Создаём коммутатор с любым названием (например, HQ). И настраиваем как на картинке.

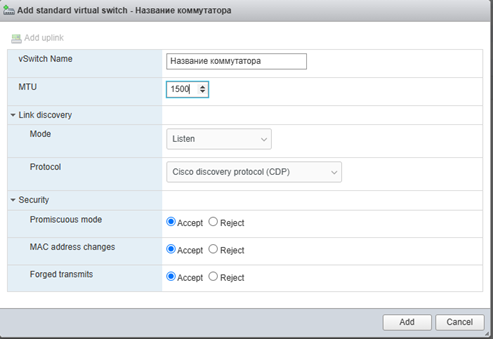


Рисунок 1 - настройка Virtual switch

Далее переходим в «Port groups» и нажимаем «Add port group». Создаём сеть с любым названием (HQ) и конфигурацией с рисунка 2. Во вкладке Virtual switch выбираем наш HQ

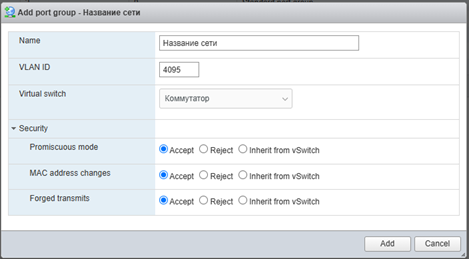


Рисунок 2 - конфигурация группы портов

Теперь переходим в настройки виртуалок, чтобы изменить их подключение. В HQ-RTR, HQ-SRV и HQ-CLI в Network Adapter 2 выбираем подключение HQ.

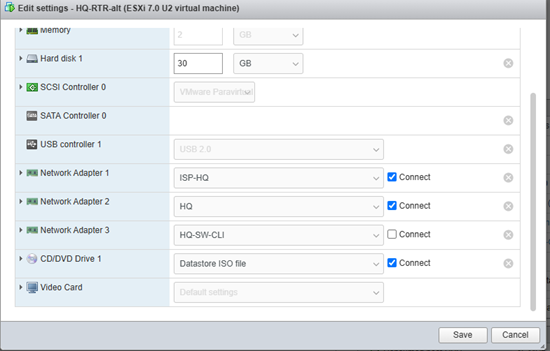


Рисунок 3 – сетевые адаптеры на HQ-RTR

Выбираем сетевые адаптеры на HQ-SRV как на рисунке 4

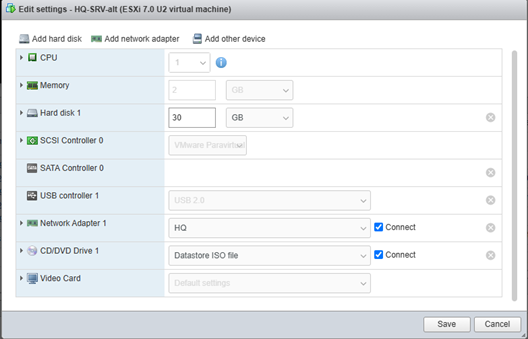


Рисунок 4 - сетевые адаптеры на HQ-SRV

Выбираем сетевые адаптеры на HQ-CLI как на рисунке 5

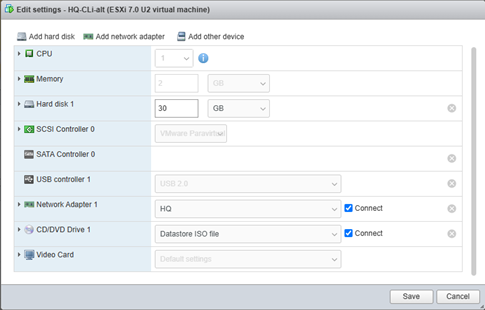


Рисунок 5 - сетевые адаптеры на HQ-CLI

Сеть должна выглядеть так как на рисунке

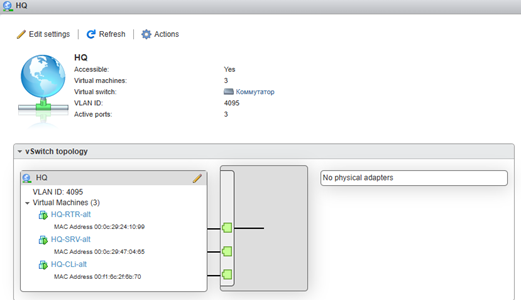


Рисунок 6

**Заходим в HQ-RTR**. Сетевые интерфейсы должны выглядеть как на рисунке 7 их должно быть 3:

100 - на HQ-SRV

200 - на HQ-CLI

999 - админский vlan

Обязательно убираем ip address у ens224 (Можно закомментировать #)

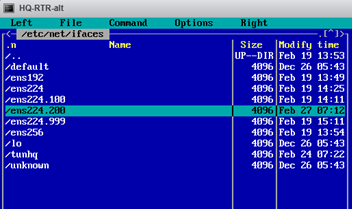


Рисунок 7 - директории с виртуальными портами на HQ-RTR

Конфигурация состоит из 2 файлов **ipv4address**(IP address) и **options.** Чтобы виртуальные интерфейсы поднялись, нужно написать в интерфейсе-хосте (ens224) файл **options** со стандартными настройками.

Файл **options** для виртуальных интерфейсов должен выглядеть как на рисунке 8 (для ens224.100 (VLAN 100)). Строка VID должна совпадать с названием интерфейса у ens224.100(VID=100), у ens224.200(VID=200), у ens224.999(VID=999)

В **ipv4address** пишем адреса в соответствии с вашей таблицей IP-адресов. Например, локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов, то есть 192.168.10.1/26. Для VLAN200 192.168.20.1/28. Для VLAN999 192.168.99.1/29

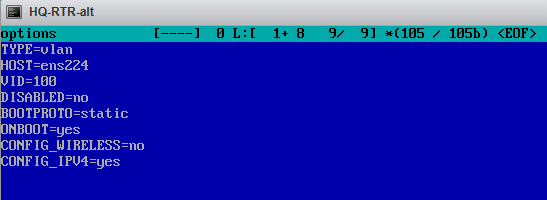


Рисунок 8 - настройка файла options для виртуального интерфейса

После всего мы перезагружаем network (systemctl restart network) и смотрим ip адреса (ip a) должно получиться как на рисунке 9

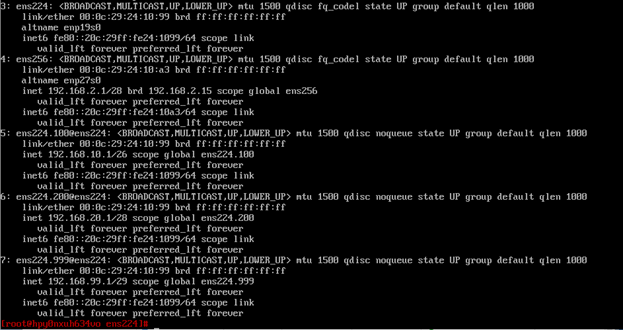


Рисунок 9 - вывод команды ip a на HQ-RTR

**Переходим на HQ-SRV**

Проделываем всё так же, как и на HQ-RTR, чтобы получилось, как на рисунке 10. IP-адреса в файлах **ipv4address** должен быть в одной подсети, что и IP-адреса на HQ-RTR. Т.е. если на HQ-RTR VLAN100 192.168.10.1/26, то на HQ-SRV 192.168.10.2/26

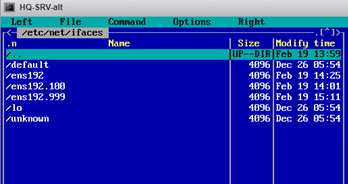
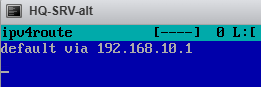


Рисунок 10

Ещё нужно создать **ipv4route,** в котором прописываем IP-адрес HQ-RTR, находящийся в одной подсети. В случае с HQ-SRV это VLAN100.



На рисунке 11 вывод команды ip a на HQ-SRV

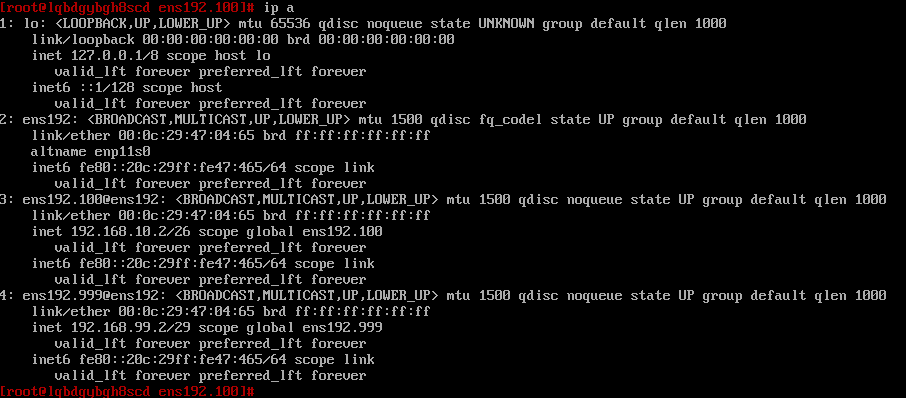


Рисунок 11

**Переходим на HQ-CLI**

И проделываем как на 2 предыдущих машинах. Интерфейс ens192 ВООБЩЕ не трогаем. Настраиваем только ens192.200. **Важно.** Прописываем команду systemctl enable --now NetworkManager

На рисунке 12 сетевые интерфейсы

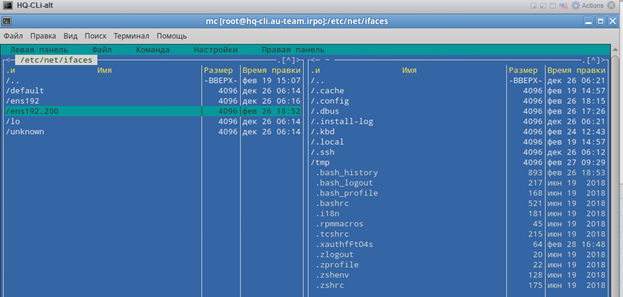
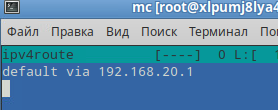


Рисунок 12

На клиенте тоже создаём **ipv4route**, в котором прописываем IP-адрес HQ-RTR, находящийся в одной подсети. В случае с HQ-CLI это VLAN200.



На рисунке 13 вывод команды ip a на HQ-CLI

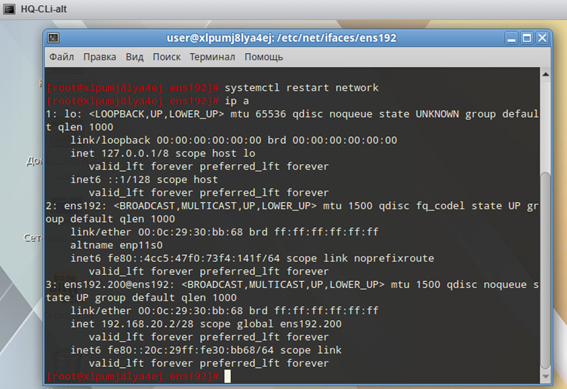


Рисунок 13

# 3. Настройка роутера HQ-RTR/BR-RTR

На роутере нужно назначить интерфейсам ip-адреса.

Смотрим интерфейсы:

[root]: ip a

Проверяем что есть в директории с интерфейсами:

[root]# ls -l /etc/net/ifaces/

Если нет нужной директории, то создаём её:

[root]# mkdir -p /etc/net/ifaces/наш\_интерфейс/

После того как создали директорию, нужно в неё зайти командой:

[root]# cd /etc/net/ifaces/наш\_интерфейс/

Далее нужно создать в директории файл **options**:

[root]# touch **options**

Редактируем файл при помощи mc и записываем следующие строчки (если не записаны):

BOOTPROTO=static

TYPE=eth

DISABLED=no

CONFIG\_IPV4=yes

**//Не забываем про то, что последняя строка должна быть пустая//**

**ВАЖНО. Прежде чем назначать ip-адреса интерфейсам, нужно сверить MAC-адреса**

Назначение IP-адресов

Нужно создать файл **ipv4address**:

[root]: touch ipv4address

Пишем в файле **ipv4address** адрес интерфейса:

172.16.4.2/28

Нужно указать шлюз по умолчанию.

Есть два путя: можно настроить по гайду А.А.: создать файл **ipv4route** и в нём написать default via 'адрес шлюза' (также желательно оставить пустую строку):

[root]: touch **ipv4route**

И пишем в файле **ipv4route** шлюз по умолчанию (адрес интерфейса ISP, к которому подключён роутер). Заходим в mc и пишем:

default via 172.16.4.1 ( шлюз )

После этого проверить командой ping и пропинговать шлюз

**ВАЖНО.** Чтобы был интернет на роутерах, нужно включить форвардинг пакетов на роутерах и ISP. На роутере мы сделаем это следующим образом. Для этого нужно зайти в mc в файл **sysctl.conf** в директории /etc/net

В нём в строчке «net.ipv4.ip\_forward = 0» изменить 0 на 1.

То же самое делаем на ISP.

Теперь форвардинг включён на постоянке. Проверяем интернет, пингуя 77.88.8.8. Если пингуется, то интернет есть. Если не пингуется, то нужно указать DNS в файле **resolv.conf,** который находится в директории /etc

# 3.1 Указание DNS в resolv.conf

DNS-сервер на HQ-SRV, а на всех роутерах просто DNS

DNS в resolv.conf (в директории /etc)

**На ISP в resolv.conf ничего не пишем( на всех остальных роутерах пишем т.к это задание 10 и нам пока не нужно устанавливать днс)**

В файле **resolv.conf** пишем:

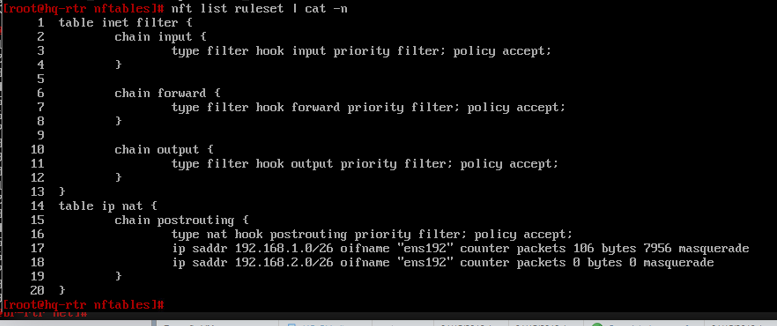
nameserver 77.88.8.8

**Если всё равно не пингуется днс или шлюз, то попробуйте прописать systemctl restart network на роутере и ISP**

# 3.2 Настройка nftbales на роутерах

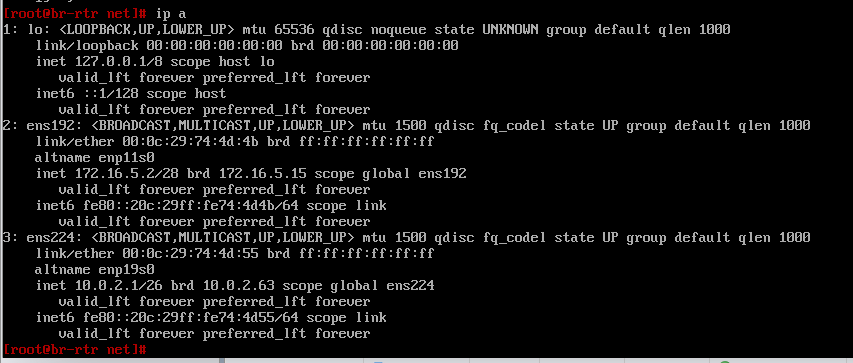
Установка такая же, как и в [пункте 2.2](#_2et92p0). Но нужно уточнить. На обоих роутерах создаём те же файлы, что при базовой настройке (options, ipv4address, ipv4route)

На HQ-RTR прописываем 2 подсети – для сервера и клиента (при выполнении 4 задания прописываем подсети VLAN100 и VLAN200)

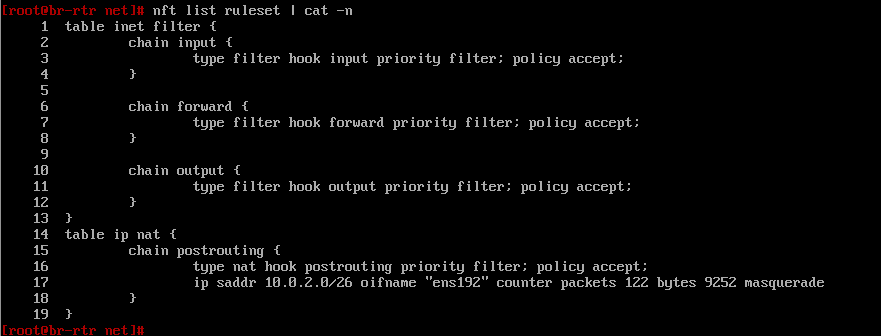


Nftables на HQ-RTR

На BR-RTR прописываем 1 подсеть и настраиваем оставшийся интерфейс



IP-адрес оставшегося интерфейса BR-RTR



nftables на BR-RTR

# 4. Настройка SRV

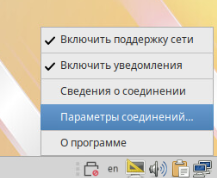
**ПРИМЕЧАНИЕ.** Если выполняется задание 4 с виртуальным коммутатором, то на HQ-SRV не нужно настраивать интерфейс, который идёт к роутеру, и не нужно создавать файлы ipv4route и ipv4address.

Базовая настройка. Настроить интерфейс, прописать адрес и шлюз, чтобы был доступ в интернет.

Создать в директории интерфейса файлы **options** (если не создан), **ipv4address (172.16.4.2/28), ipv4route (default via 172.16.4.1)**

# 5. Настройка клиента HQ-CLI (завершение пункта задания 8 про интернет на всех устройствах)

Для того, чтобы настроить IP-адрес на клиенте, нужно нажать ПКМ на значок сетевого соединения с двумя мониторами.



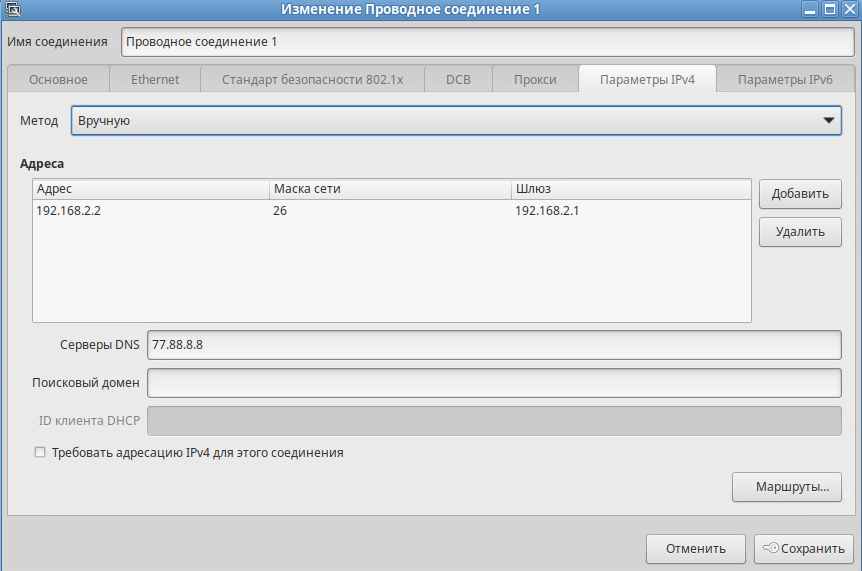
Далее нужно зайти в «параметры соединений» и выбрать проводное подключение. Основная настройка происходит в «Параметры IPV4». Выбрать метод «вручную». Прописать:

адрес 192.168.2.2

маску 26

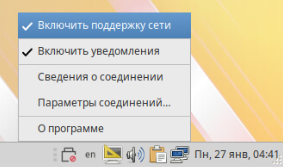
шлюз 192.168.2.1

DNS 77.88.8.8 (днс Яндекса)



Окно настроек

После этого нужно перезапустить сеть на компе. Для этого нужно включить и выключить «Поддержку сети».



После этого проверить, пропинговав шлюз и днс. Может быть такое, что пинговать не будет, потому что сетевая карта не включена и/или соединение неправильно. Сделать это нужно в «Edit settings» виртуалки.

# Задание 3. Создание локальный учётных записей (sshuser на серверах HQ-SRV и BR-SRV)

Задание 3. Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV

Условия. Пароль пользователя sshuser – P@ssw0rd. Идентификатор пользователя 1010. Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации.

Команды:

adduser sshuser -u 1010

passwd sshuser

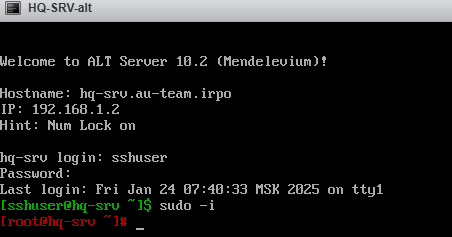
P@ssw0rd (вводим новый пароль)

P@ssw0rd (подтверждаем новый пароль)

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

usermod -aG wheel sshuser

Чтобы проверить, выходим из текущего пользователя и заходим на юзера sshuser. Для выхода из пользователя нужно написать **exit** или нажат**ь CTRL+D.** Вводим логин и пароль нового юзера. Вводим **sudo -i.** Если зашли в root пользователя, то всё правильно сделано.



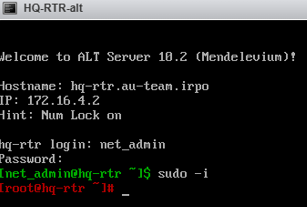
Проверка на серверах

**Вторая часть задания.** Создайте пользователя net\_admin на маршрутизаторах HQ-RTR и BR-RTR.

Те же самые команды, но только уже на роутерах.

Логин: net\_admin

Пароль: P@$$word



Проверка на роутерах

# Задание 5. Настройка безопасного удалённого доступа на серверах HQ-SRV и BR-SRV

По заданию нужно использовать порт 2024, разрешить подключение только пользователю sshuser, ограничить количество попыток до 2-ух и настроить баннер «Authorized access only».

В папке /etc создаём файл **banner:**

touch banner

Для того, чтобы выводился баннер, нужно в только что созданном файле **banner** написать «Authorized access only».

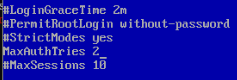


Теперь нужно отредактировать конфиг **sshd\_config**. Он находится в директории /etc/openssh.

Меняем стандартный порт ssh (который 22) на порт согласно заданию (2024). Можно сделать с помощью команды или найти в конфиге закомментированную строчку с портом, убрать решётку и написать номер порта:

sed -i «s/#Port 22/Port 2024/g» /etc/openssh/sshd\_config

Далее нужно изменить строчку MaxAuthTries 2



Написать строчку в конце конфига **AllowUsers sshuser**

Для вывода баннера добавить слово Banner с его директорией, в которой он находится:

**Banner /etc/banner**

Перезапускаем службу sshd:

systemctl restart sshd

Для подключения по ssh нужно написать следующую команду:

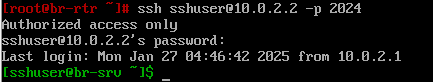
ssh sshuser@10.0.2.2 -p 2024

sshuser – имя юзера, на которого заходим

10.0.2.2 – IP-адрес

2024 – номер порта

Пароль для sshuser P@ssw0rd, который был создан в задании 3.



# Задание 6. IP-туннель

Между офисами HQ и BR необходимо сконфигурировать ip туннель. Туннель будет настраиваться на **HQ-RTR и BR-RTR**

Необходимо создать директорию для туннельного интерфейса. Создаём новую директорию tun1 в /etc/net/ifaces.

Затем создаём в этой директории файл **options**

touch options

В файле записываем следующие строчки:

TYPE=iptun

TUNTYPE=gre

TUNLOCAL=172.16.4.2

TUNREMOTE=172.16.5.2

TUNOPTIONS='ttl 64'

HOST=ens192

**TUNLOCAL –** IP-адрес интерфейса, который получает адрес от ISP

**TUNREMOTE –** IP-адрес интерфейса второго роутера, который получает адрес от ISP

Назначаем IPv4 адрес на туннельный интерфейс. Это можно сделать с помощью команды или создать файл **ipv4address** в mc**.** В нём нужно вписать адрес из диапазона частных ip-адресов (172.16.100.1/28)

или echo 172.16.100.1/28 > /etc/net/ifaces/tun1/ipv4address

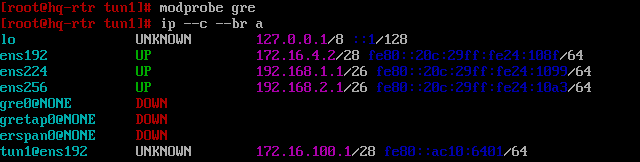
Затем перезапускаем интернет:

systemctl restart network

Включаем модуль ядра для gre:

modprobe gre

ip --c --br a



На другом роутере настройки аналогичны, но адреса TUNLOCAL и TUNREMOTE поменяны местами.

Туннель поднят, но нужно ещё настроить OSPF.

# Задание 7. Настройка OSPF

Заходим на **HQ-RTR и BR-RTR**. Установим пакет frr:

apt-get update

apt-get install -y frr

В конфигурационном файле /**etc/frr/daemons** необходимо активировать выбранный протокол для дальнейшей реализации его настройки:

строчку **ospfd=no** изменить на **ospfd=yes**

Включаем автозагрузку:

systemctl enable --now frr (перед now два тире)

Проверяем командой ss -tulpn | grep ospf



Настраиваем OSPFv2 - переходим в интерфейс frr. Для этого входим при помощи команды:

vtysh

Заходим в терминал:

configure terminal

По очереди пишем следующие команды:

router ospf

passive-interface default

network 172.16.100.0/28 area 0 (подсетка для туннеля между роутерами)

network 192.168.2.0/26 area 0 (подсетка до клиента)

network 192.168.1.0/26 area 0 (подсетка до HQ-SRV)

//**Для BR-RTR прописываем только 2 подсетки – туннельная и до BR-SRV//**

после этого заходим в интерфейс tun1:

exit

interface tun1

Для того, чтобы сделать его активным, нужно прописать следующие команды:

no ip ospf network broadcast

no ip ospf passive

ip ospf authentication-key PLAINPAS

ip ospf authentication

exit

do wr mem (сохранение конфигурации)



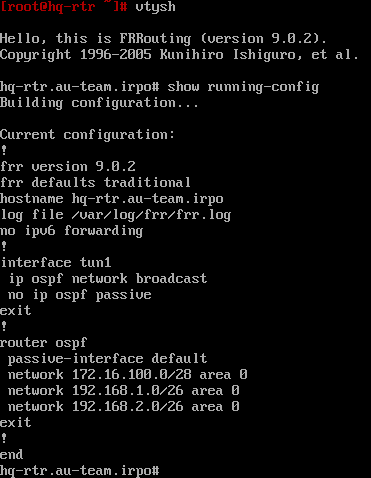
Выходим до рута и проверяем командами:

vtysh

show running-config



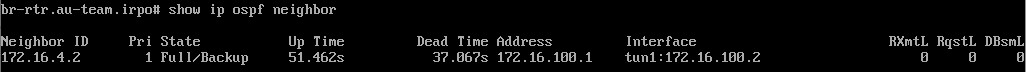
BR-RTR



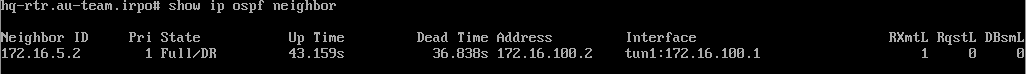
HQ-RTR

На всякий случай прописываем systemctl restart network на ISP, HQ-RTR, BR-RTR

Для проверки наших соседов вводим команду **show ip ospf neighbor**

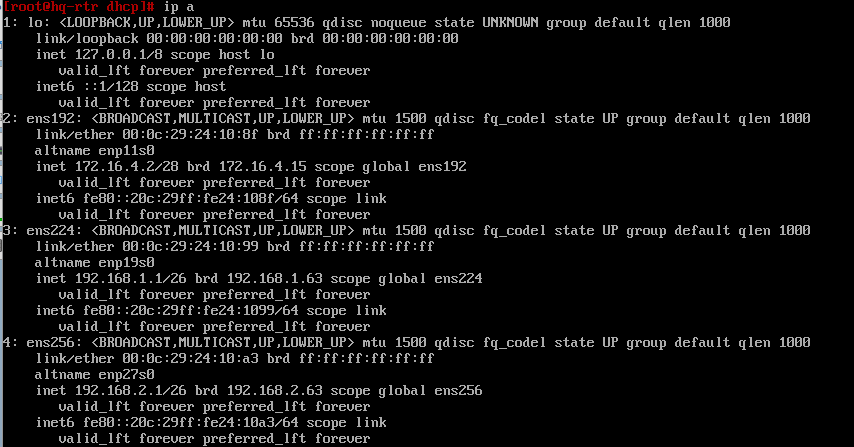


BR-RTR



HQ-RTR

Для проверки работы OSPF нужно пингануть с одного сервера другой сервер (ну или с любого устройства одной сети пингануть устройство другой сети). Если пингуется, то OSPF работает.



# Задание 8

Настройка динамической трансляции адресов.

● Настройте динамическую трансляцию адресов для обоих офисов.

● Все устройства в офисах должны иметь доступ к сети Интернет

Если IP-адреса выданы, шлюзы прописаны, днс написан, интерфейсы настроены, то интернет будет. Для проверки интернета нужно пингануть DNS:

ping 77.88.8.8 или ping 8.8.8.8

# Задание 9. DHCP

Настройка происходит на **HQ-RTR.**

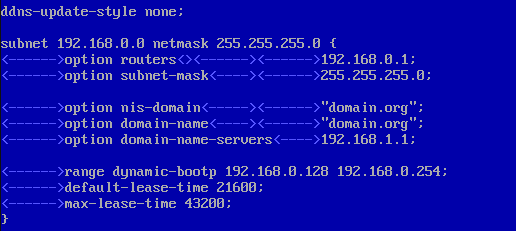
Установка dhcp:

apt-get install dhcp-server

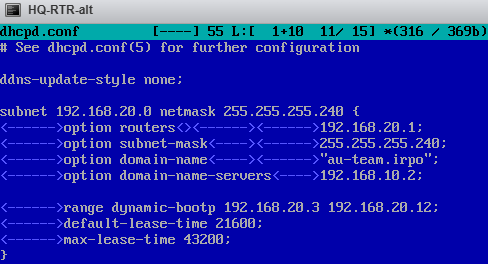
Настройка происходит в директории **/etc/dhcp**

В этой директории есть файл **dhcpd.conf.sample.** Этот файл копируем в mc при помощи сочетании клавиш **SHIFT+F5.** Меняем название на **dhcpd.conf**





Пример конфига



Пример уже настроенного конфига

В этом файле:

subnet 192.168.2.0 (подсеть, которая идёт к клиенту)

netmask 255.255.255.240 (смотрим на префикс IP-адреса и пишем маску)

option routers 192.168.2.1 (IP-адрес роутера, который направлен в сторону клиента)

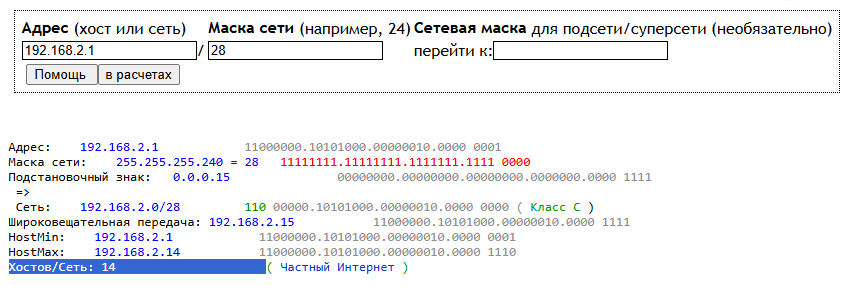
option subnet-mask 255.255.255.240 (маска)

строчку option nis-domain **удаляем**

option domain-name "au-team.irpo" (DNS-суффикс написан в задании)

option domain-name-servers 192.168.1.2 (IP-адрес HQ-SRV)

range dynamic-bootp 192.168.2.3 192.168.2.12 (так как 192.168.2.1 и 192.168.2.2 заняты, то указываем, что с 192.168.2.3, а 192.168.2.12 берём из ip-калькулятора)



Сохраняем и выходим из файла. Затем заходим в **/etc/sysconfig/dhcpd** и указываем сетевой интерфейс, на котором будет работать DHCP-сервер (выбираем тот интерфейс, который идёт к клиенту)

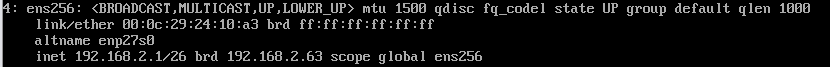
При выполнении 4 задания указываем виртуальный интерфейс HQ-RTR, который идёт к клиенту, а не физический, как это делали раньше



Стандартный интерфейс



Виртуальный интерфейс

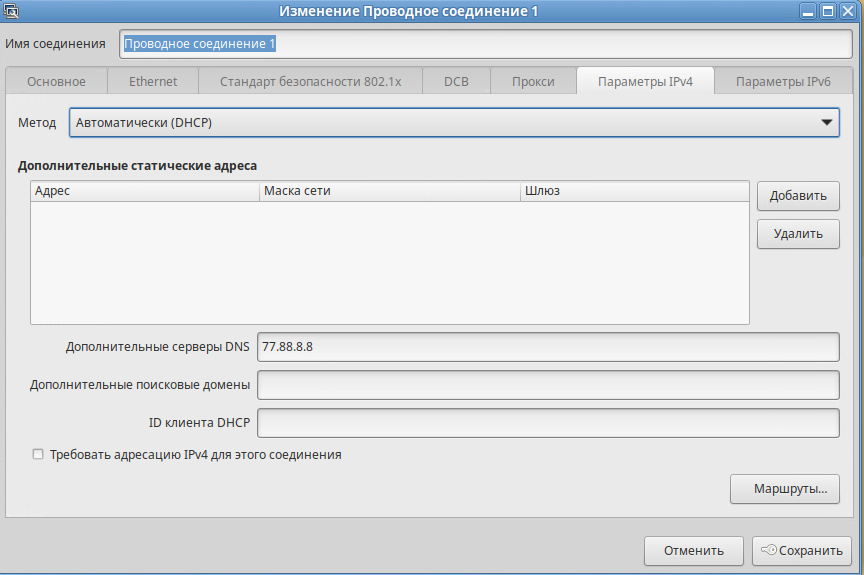


Добавление dhcp в автозагразку:

chkconfig dhcpd on

service dhcpd start

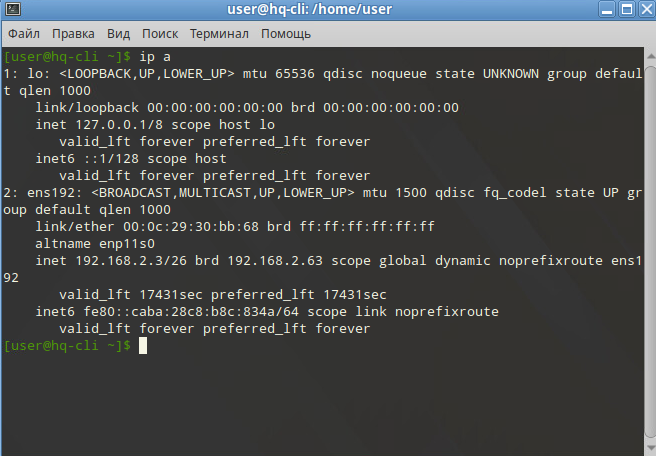
Запускаем HQ-CLI. Заходим в параметры проводных подключений. Переходим в Параметры IPv4. Выставляем метод «Автоматически (DHCP)» и удаляем статический адрес. Затем перезапускаем сеть (выключить поддержку и включить поддержку сети)



При выполнении 4 задания заходим в /etc/net/ifaces/ens192.200/options и меняем в файле **options** строчку **BOOTPROTO=static** на **BOOTPROTO=dhcp.** По идее должно работать, но если не работает, то удаляем файлы ipv4address и ipv4route

Если в файле options в строчке DISABLED указано yes, то меняем на no

Проверяем в терминале, прописав команду ip a



Изменённый IP-адрес, значит, DHCP работает

# Задание 10. Настройка DNS

DNS-сервер реализован на **HQ-SRV**.

Перед установкой на всякий случай прописать **apt-get update**

Если не скачивается, то нужно зайти в файл **resolv.conf в /etc** и написать **nameserver 77.88.8.8.** После чего перезапустить сеть

Для установки:

apt-get install bind

apt-get install bind-utils

В конфигурационном файле /etc/bind/options.conf - правим следующие параметры и убираем комментарии (комментарии это //):

listen-on { any; }

listen-on-v6 (закомментировать //)

forward first; (оставить как есть)

forwarders { 77.88.8.8; };

allow-query { any; };

Для добавления в автозагрузку написать команду:

systemctl enable --now bind (перед now два коротких тире)

systemctl restart bind

В директории /etc заходим в файл **resolvconf.conf.** В конец пишем строчку:

name\_servers=127.0.0.1

Далее пишем команду:

resolvconf -u

Для проверки интернета пишем cat /etc/resolv.conf и пингуем 77.88.8.8

В директории /etc/bind/ заходим в файл **local.conf** и описываем необходимые зоны согласно заданию (между зонами желательно Enter):

zone "au-team.irpo" { type master; file "au.db"; };

zone "1.168.192.in-addr.arpa" { type master; file "1.db"; };

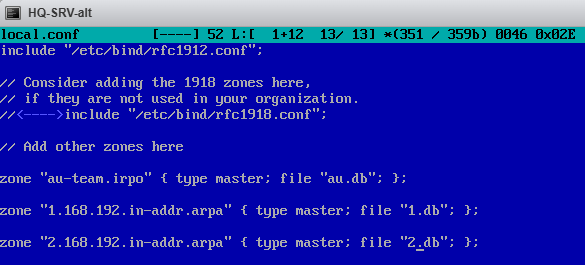
zone "2.168.192.in-addr.arpa" { type master; file "2.db"; };

**au-team.irpo –** название из таблицы 2

**1.168.192 –** взять ip-адресацию между HQ-RTR и HQ-SRV и написать адрес обратной зоны (192.168.1.0 > 1.168.192)

**2.168.192 –** взять ip-адресацию между HQ-RTR и HQ-CLI и написать адрес обратной зоны (192.168.2.0 > 2.168.192)

**au.db, 1.db, 2.db –** названия файлов, назвать можно по-разному



Копируем примеры файлов для зон прямого просмотра по пути **/etc/bind/zone:**

cp /etc/bind/zone/{localdomain,au.db}

//**au.db, 1.db, 2.db –** названия файлов//

Копируем примеры файлов для зон обратного просмотра:

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

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

Задаём необходимые права:

chown root:named /etc/bind/zone/{au,1,2}.db

После этого нужно зайти в зону прямого просмотра **au.db,** находящийся в директории /etc/bind/zone/

В строке с SOA меняем localhost на au-team.irpo. Строчка должна быть такой:

au-team.irpo. root.au-team.irpo.

В строке с NS localhost меняем на au-team.irpo

А вот сейчас начинается самое “весёлое”.

строчку с записью типа CNAME localhost стереть

[Используя таблицу 2](#_1fob9te), записи пишутся следующим образом **(во всех файлах оставляем последнюю строку пустой, потому что Линукс)**:

hq-rtr нажимаем Tab IN нажимаем Tab A нажимаем Tab 192.168.1.1

**hq-rtr -** имя устройства

**IN -** надо

**A -** тип записи

**192.168.1.1 -** IP-адрес устройства во внутренней сети

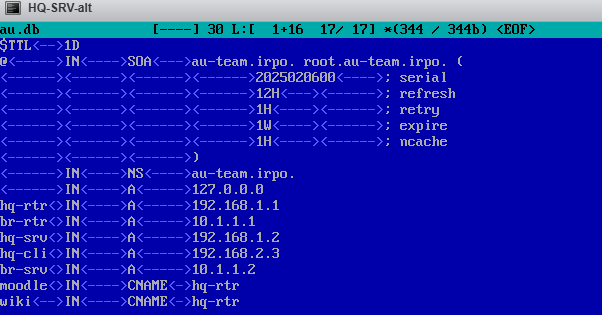
Последние 2 записи CNAME пишутся так:

moodle нажимаем Tab IN нажимаем Tab CNAME нажимаем Tab hq-rtr

**moodle -** имя

**CNAME -** тип записи

**hq-rtr -** имя устройства



пример конфига **au.db**

Переходим к настройке зон обратного просмотра - **1.db, 2.db**

С первыми строчками то же самое, но записываются только записи PTR. По заданию их 3. Записываются они так:

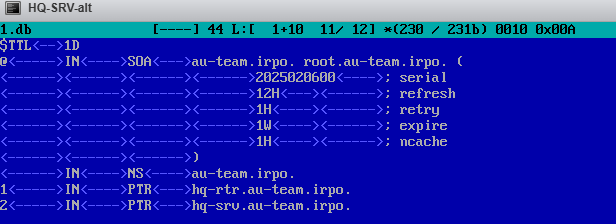
1 нажимаем Tab IN нажимаем Tab PTR нажимаем Tab hq-rtr.au-team.irpo.

**1 -** последняя цифра IP-адреса устройства

**IN -** надо

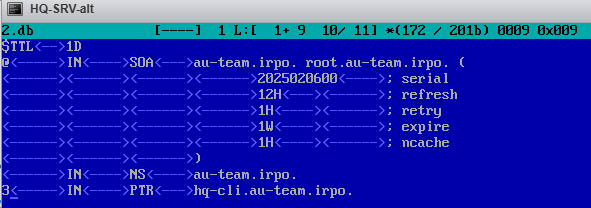
**PTR -** тип записи

**hq-rtr.au-team.irpo. -** полное имя устройство **с точкой на конце** (из таблицы 2)



В обратной зоне **2.db** записываем только клиента:

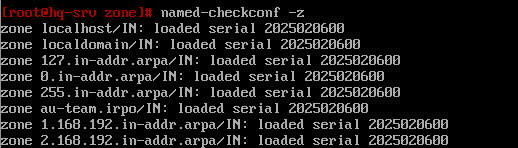
3 нажимаем Tab IN нажимаем Tab PTR нажимаем Tab hq-cli.au-team.irpo



пример настроенного конфига

Проверка:

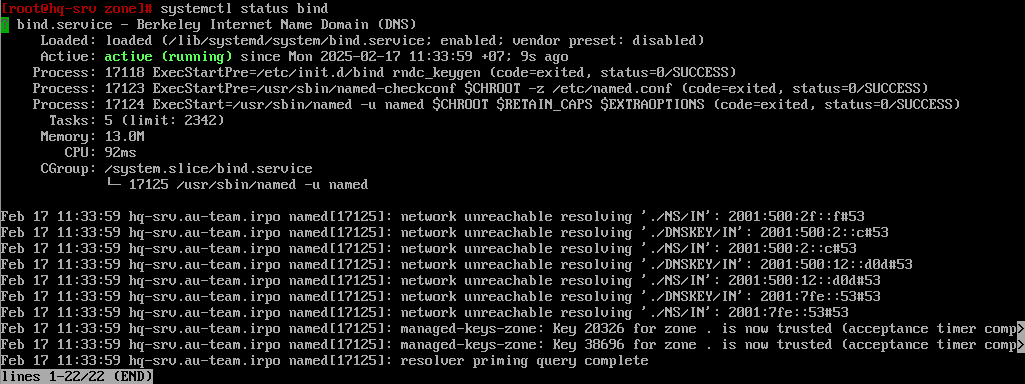
named-checkconf -z



в выводе должны быть 1 прямая зона и 2 обратные зоны

systemctl restart bind

systemctl status bind



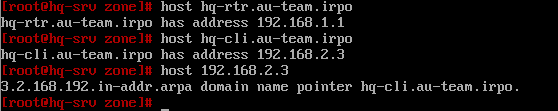
Проверяем, выполняет ли свою работу DNS:

host hq-rtr.au-team.irpo

host hq-cli.au-team.irpo

host 192.168.2.3 (IP-адрес клиента)

Если после ввода имени устройства в выводе написаны IP-адреса, и наоборот тоже получается, то всё в поряде.



# 

# Задание 11. Настройка часового пояса

Где-то часовой пояс Новосибирска уже установлен, а где-то нет. Если установлен, то можно сразу перейти к выбору пояса. Если же не установлен, то устанавливаем пакеты часовых поясов:

apt-get install tzdata

И выбираем пояс:

timedatectl set-timezone Asia/Novosibirsk

Проверяем время через команду:

timedatectl

**На клиенте**

Нажимаем ЛКМ на окошко с датой и временем



Нажимаем “Изменить” и переходим в “Расположения”. Нажимаем “Добавить”. В названии расположения написать Новосибирск. После этого нужно снова нажать на окошко с датой и временем, справа от циферблата выбрать кнопку “Установить”. После этого на клиенте будет нужный часовой пояс

**МОДУЛЬ 2**

# Задание 1. Доменный контроллер Samba

Samba настраивается на BR-SRV. Что нужно сделать:

* создать 5 пользователей для офиса HQ. Имена пользователей формата user№.hq
* создать группу hq, в которую нужно ввести созданных пользователей
* ввести в домен HQ-CLI
* пользователи группы hq имеют право аутентифицироваться на клиентском ПК
* пользователи группы hq должны иметь возможность повышать привилегии для выполнения огр. набора команд: cat, grep, id. Запускать другие команды с повышенными привилегиями пользователи группы не имеют права
* выполнить импорт пользователей из файла users.csv. Файл должен располагаться на виртуальной машине BR-SRV в папке /opt

Выполнение задания.

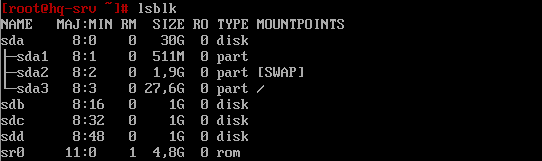
# Задание 2. Файловое хранилище

На HQ-SRV нужно сконфигурировать дисковой массив уровня 5. Если дополнительных дисков нет, то нужно их добавить в ESXI. Выключаем машину. Нажимаем ПКМ и выбираем “Edit settings”. После этого нажимаем “Add a hard disk”, добавляем 3 диска и пишем размер диска, то бишь 1 гб.

Просматриваем имена дисков:

lsblk

Вывод будет примерно таким:



Пишем следующее (b, c, d - названия дисков):

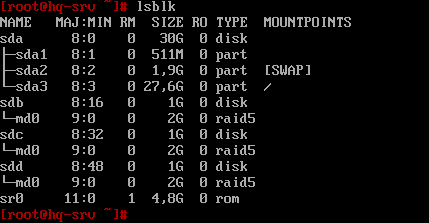
mdadm --zero-superblock --force /dev/sd{b,c,d}

wipefs --all --force /dev/sd{b,c,d}

Затем создаём RAID. Пишем команду:

mdadm --create /dev/md0 -l 5 -n 3 /dev/sd{b,c,d}

Проверяем командой lsblk. Вывод должен быть таким:



Создаём файловую систему:

mkfs -t ext4 /dev/md0

Далее создаём файл **mdadm.conf** в директории /etc:

touch mdadm.conf

Для заполнения файла информацией пишем следующие команды:

echo "DEVICE partitions" > /etc/mdadm.conf

mdadm --detail --scan | awk '/ARRAY/ {print}' >> /etc/mdadm.conf

Создаём директорию для монтирования массива:

mkdir /mnt/raid5

**И вот тут внимательно**, пожалуйста, так как если неправильно заполните файл, то система может не запуститься в следующий раз. В файл **fstab,** который находится в /etc, добавляем строку:

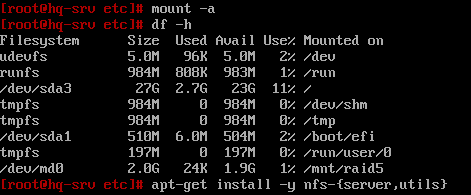
/dev/md0 нажимаем Tab /mnt/raid5 нажимаем Tab ext4 нажимаем Tab defaults нажимаем Tab 0 нажимаем Tab 0

Сохраняем и выходим. Пишем:

mount -a

df -h

Вывод должен быть таким:



Далее идёт настройка NFS.

Установка:

apt-get install -y nfs-{server,utils}

Создаём директорию для общего доступа:

mkdir /mnt/raid5/nfs

Далее пишем следующее:

chmod 766 /mnt/raid5/nfs

Заходим в файл **exports**, находящийся в директории /etc, и добавляем:

/mnt/raid5/nfs 192.168.20.0/28(rw,no\_root\_squash)

//192.168.20.0/28 - клиентская сеть//

Экспортируем файловую систему:

exportfs -arv

Добавляем в автозагрузку NFS-сервер:

systemctl enable --now nfs-server

**Заходим на HQ-CLI.**

Устанавливаем NFS:

apt-get update && apt-get install -y nfs-{utils,clients}

Создаём директорию для общего ресурса:

mkdir /mnt/nfs

Выдаём права:

chmod 777 /mnt/nfs

Заходим в файл **fstab** в директории /etc. Пишем строчку:

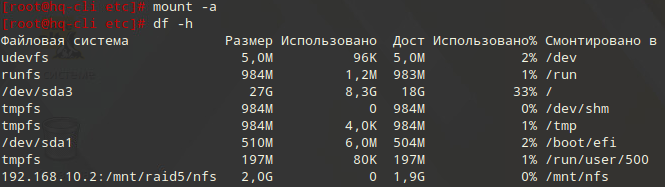
192.168.100.62:/mnt/raid5/nfs нажимаем Tab /mnt/nfs нажимаем Tab nfs нажимаем Tab defaults нажимаем Tab 0 нажимаем Tab 0

Затем пишем команды:

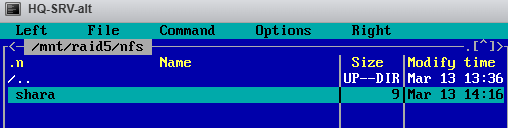
mount -a

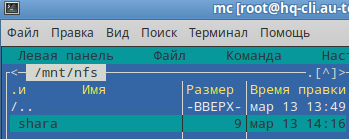
df -h

После команд вывод должен быть таким:



Для проверки на сервере создаём в папке /mnt/raid5/nfs какой-нибудь файл. Если всё правильно, то на клиенте в папке /mnt/nfs этот файл должен появиться.





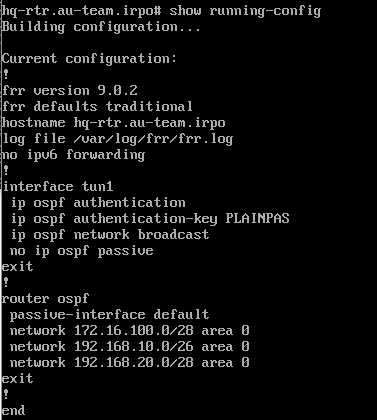
# Задание 3. Служба сетевого времени

Настройка выполняется на HQ-RTR.

Перед выполнением задания можно (то есть опционально) проверить настройку OSPF с помощью команд:

vtysh

show running-config



Пример настройки OSPF

Заходим в файл **chrony.conf**, находящийся в директории /etc

В файле комментируем все строки (то есть все строчки без #)

Можно командой:

sed -i “s/^/#&/g” /etc/chrony.conf

И пишем следующие строчки в конец файла:



После этого перезапускаем службу:

systemctl restart chronyd

Далее переходим к настройке клиентов - это HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.

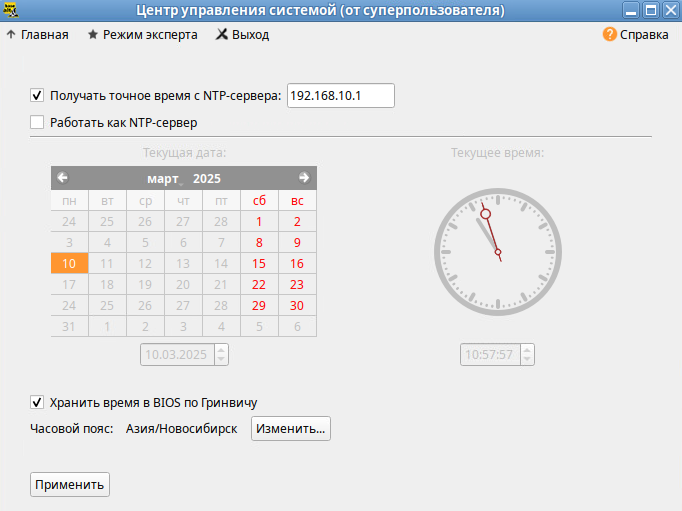
На них заходим в файл **chrony.conf** в директории /etc. Комментировать строки не нужно. Нужно только написать следующую строчку:

server 192.168.10.1 iburst prefer (в качестве ip-адреса берём ip-адрес HQ-RTR, который идёт в сторону VLAN100)

После этого перезапускаем службу:

systemctl restart chronyd

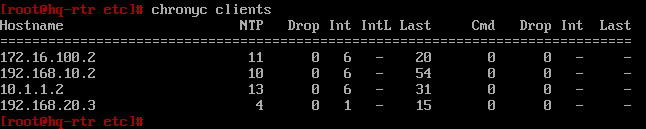
На HQ-CLI нажимаем на пуск, заходим “Центр управления системой”. Выбираем “Дата и время”. В строчке “Получить точное время с NTP-сервера” пишем ip-адрес HQ-RTR, который писали ранее



Для проверки заходим на HQ-RTR и пишем команду:

chronyc clients

Должны показываться ip-адреса клиентов (HQ-SRV, HQ-CLI, BR-RTR, BR-SRV)



# Задание 9. Установка Яндекс.браузера

Для этого нужно ввести 2 команды:

apt-get update

apt-get install yandex-browser-stable

# Модуль 1 со скриптами

**Внимание!** Скрипты используйте только в том случае, если вы знаете, как что-то исправить, если это что-то пошло не так, то есть если вы умеете заниматься дебагингом. **Если не умеете, то лучше не трогайте скрипты**, иначе они вам сломают настройку, а вы будете сидеть и не понимать, как это исправить.

**ISP**

Перед скриптом нужно сделать предварительную настройку. Создаём директорию ens192:

mkdir -p /etc/net/ifaces/наш\_интерфейс (ens192)

Заходим в созданную директорию:

cd /etc/net/ifaces/ens192

Далее создаём файл **options:**

touch options

Редактируем файл:

echo "BOOTPROTO=dhcp(нажимаем Enter)

TYPE=eth (нажимаем Enter)

DISABLED=no (нажимаем Enter)

CONFIG\_IPV4=yes (нажимаем Enter)

" > options

Перезапускаем сеть:

systemctl restart network

Проверяем доступ в интернет:

ping 77.88.8.8 или 8.8.8.8

Обновляем и скачиваем mc:

apt-get update && apt-get install mc

**Скрипт для ISP**

Скачиваем утилиту:

apt-get install wget

Скачиваем скрипт:

wget <https://github.com/Dima-Ferz/-/raw/refs/heads/main/isp_all.bash>

Пишем команду:

chmod +x ./isp\_all.bash

После пишем:

.isp\_all.bash

Команда выдаст, как нужно правильно написать:

“Biven, nado tak: interface1(dhcp) int2 int3 ip\_addr\_int2 ip\_addr\_int3 hostname"

**Пояснение**:

Int1 это - ens192, int2 это - ens224, int3 это - ens256, ip addr int2- это ipшник 2-го интерфейса, ip addr int3 –это ip 3-го интерфейса, hostname – это имя нашего устройства

Через пробел пишем всё, что написано в команде:

./isp\_all.bash ens192 ens224 ens256 172.16.5.1/28 172.16.4.1/28 isp

Если не заработал nftables, то, скорее всего, нужно убрать скобку в конфиге /etc/nftables/nftables.nft

**HQ-RTR**

Перед скачиванием wget нужно настроить ens192, то есть создать в этой директории файлы **ipv4address (172.16.4.2/28)** и **ipv4route (default via 172.16.4.1).** Также прописываем в файле /etc/**resolv.conf** следующую строчку: nameserver 77.88.8.8

Пишем systemctl restart network и скачиваем wget:

apt-get update && apt-get install wget