Составление таблицы ip-адресов

Вторая и третья сетевые карты ISP имеют ip-адреса 172.16.5.1/28 и 172.16.4.1/28 соответственно.

Отталкиваясь от этого, на сетевой карте BR-RTR, смотрящей в сторону ISP (ответный ip-адрес – на второй сетевой карте ISP) будет ip-адрес 172.16.5.2/28.

И отталкиваясь от этого же, на сетевой карте HQ-RTR, смотрящей в сторону ISP (ответный ip-адрес – на третьей сетевой карте ISP) будет ip-адрес 172.16.4.2/28.

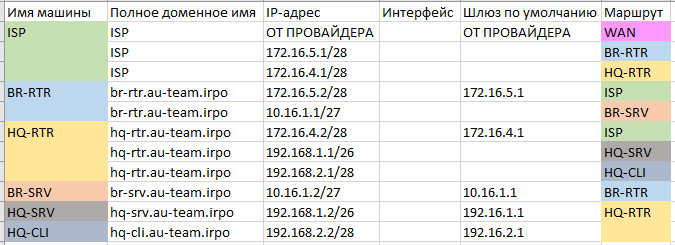
BR-подсеть будет в адресном пространстве 10.16.0.0

HQ-подсеть будет в адресном пространстве 192.168.0.0

Путь HQ-CLI – 28 префикс маски т.к. допускается не более 16 адресов.

Путь HQ-SRV – 26 префикс маски т.к. допускается не более 64 адресов.

Путь BR-SRV – 27 префикс маски т.к. допускается не более 32 адресов.



| VLAN ID | Назначение | Сеть | Маска | Количество адресов | Диапазон IP-адресов |
| --- | --- | --- | --- | --- | --- |
| 100 | Офис HQ-SRV | 192.168.10.0 | /26 | 64 | 192.168.10.0 – 192.168.10.63 |
| 200 | Офис HQ-CLI | 192.168.20.0 | /28 | 16 | 192.168.20.0 – 192.168.20.15 |
| 300 | Офис BR-SRV | 192.168.30.0 | /27 | 32 | 192.168.30.0 – 192.168.30.31 |
| 999 | Сеть управления | 192.168.99.0 | /29 | 8 | 192.168.99.0 – 192.168.99.7 |

**Настройка isp**

Делаем везде одной команой на isp надо установить tzdata командой apt-get install tzdata -y (после настройки интернета)

timedatectl set-timezone Asia/Novosibirsk

Присваиваем полные доменные имена устройствам согласно топологии:

hostnamectl set-hostname isp && exec bash

Чтобы получить интернет на isp(до перезагрузки) пишем dhcpcd

Установим в систему midnight commander, чтобы жилось проще:

*apt-get update*

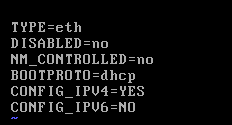
*apt-get install mc*

Создать папку интерфейса:

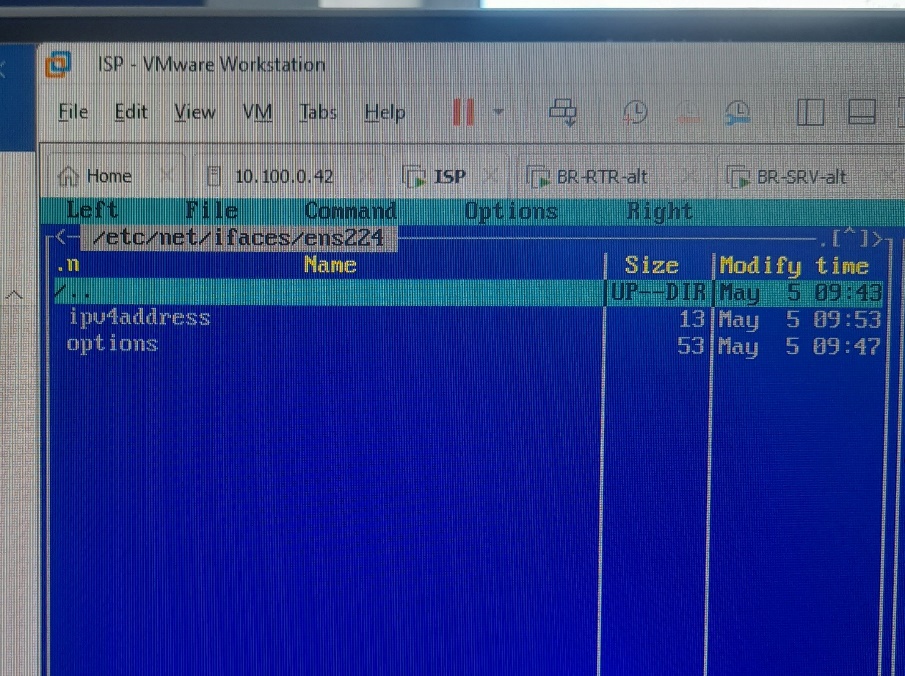
*mkdir /etc/net/ifaces/ens192*

Теперь нужно задать настройки интерфейса (команда touch)

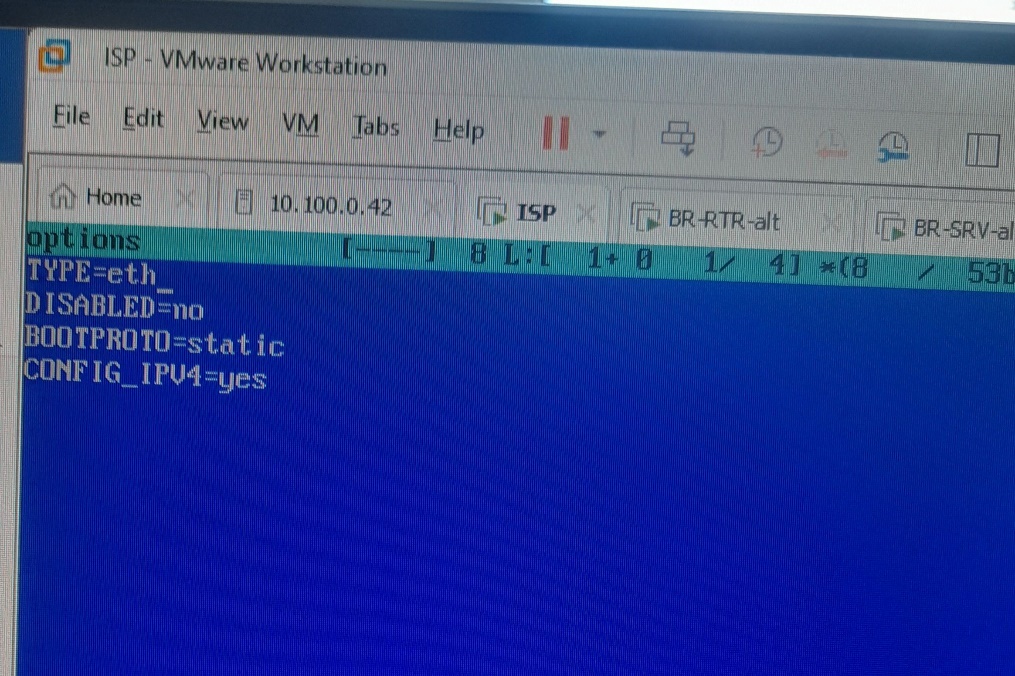
*vim /etc/net/ifaces/ens192/options*



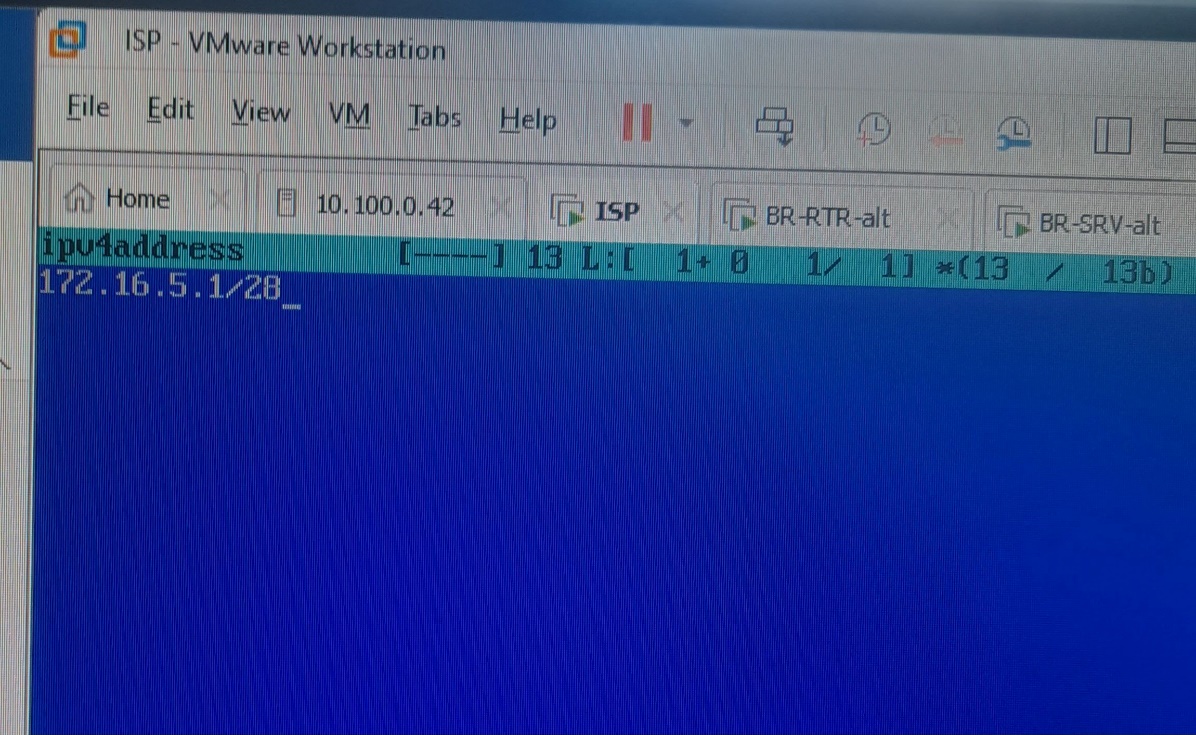
А также создаем ens224 и ens256 и пишем следующие:

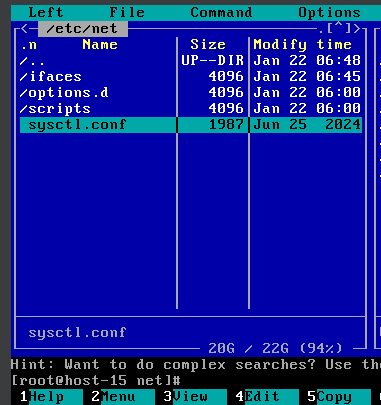


В options пишем(тут все одинаковое):

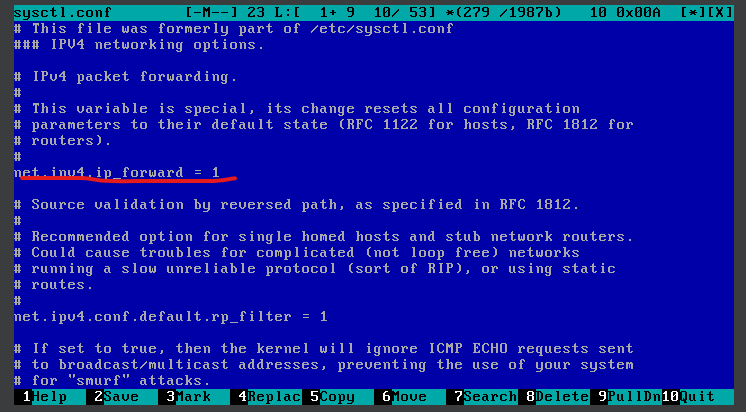


В ip пишем разные:





В скриншоте ниже указано, как должна выглядеть настройка IP-Forward.



*systemctl restart network*

Настройка NAT

Настраивать NAT нужно только на ISP и роутерах.

Скачиваем *apt-get update && apt-get install* iptables

На isp Пишем

iptables -t nat -A POSTROUTING -o ens192 -s 172.16.4.0/28 -j MASQUERADE

iptables -t nat -A POSTROUTING -o ens192 -s 172.16.5.0/28 -j MASQUERADE

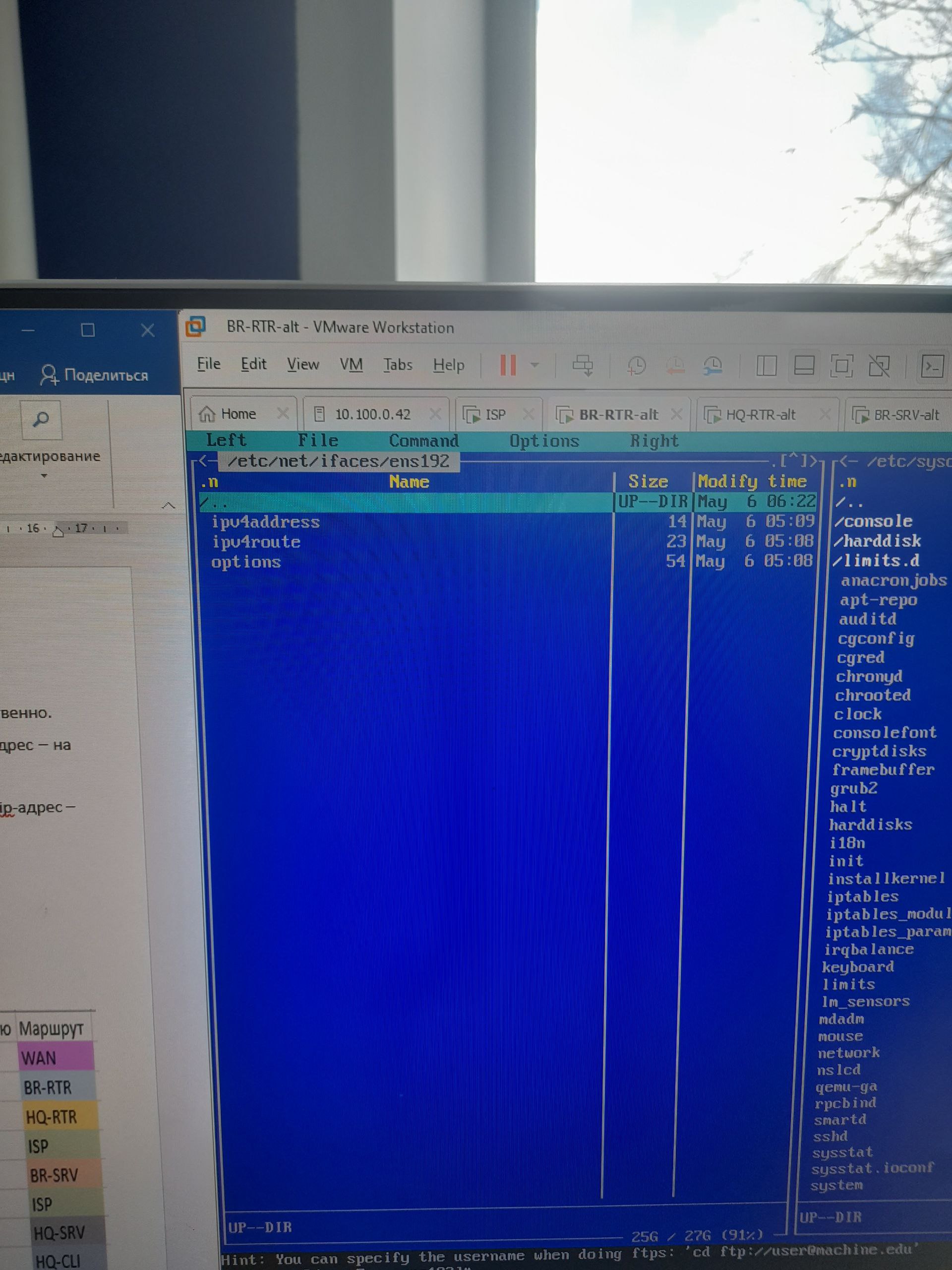
**Настройка BR-RTR**

Делаем везде одной команой на isp надо установить tzdata командой apt-get install tzdata -y (после настройки интернета)

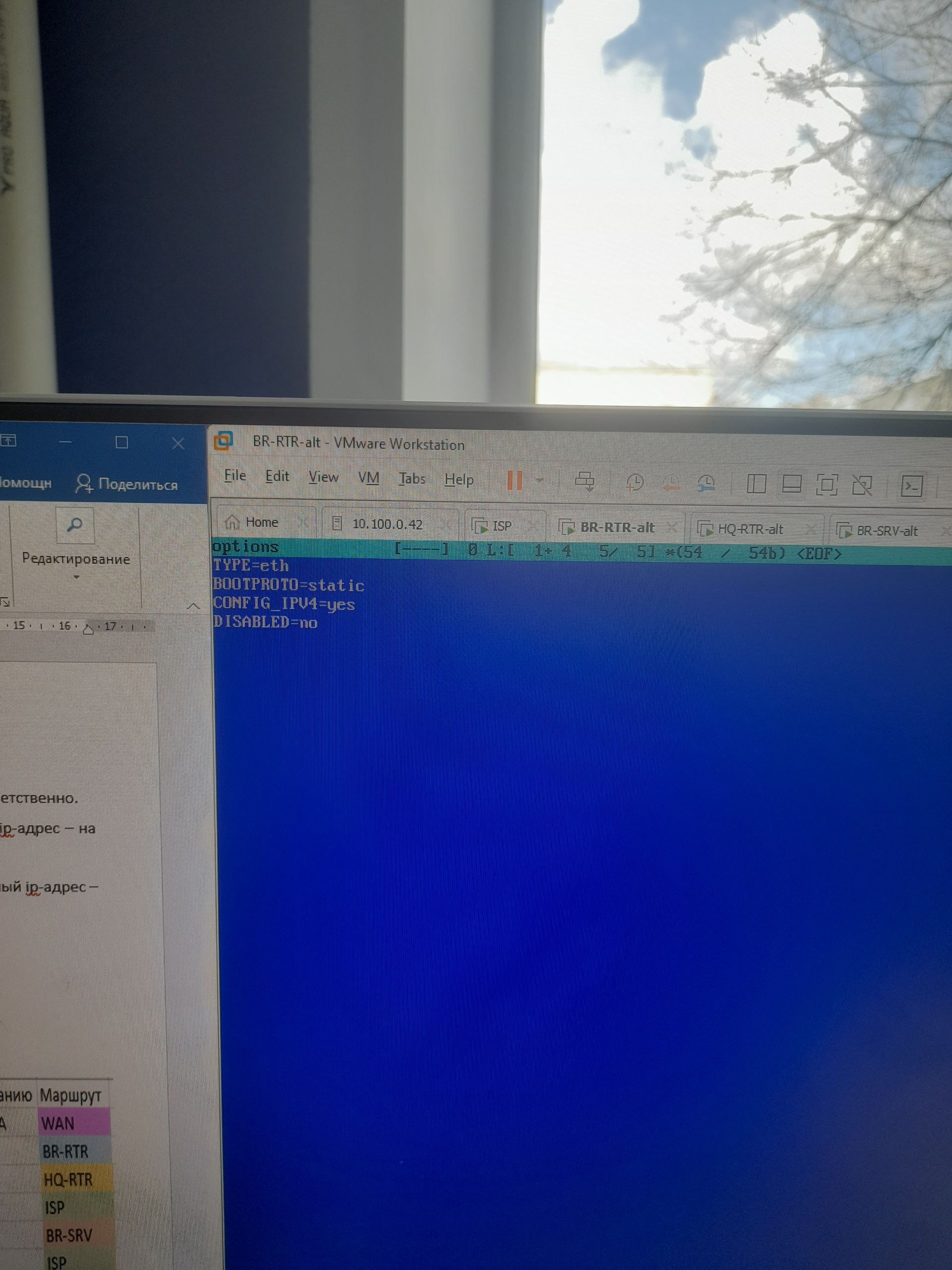
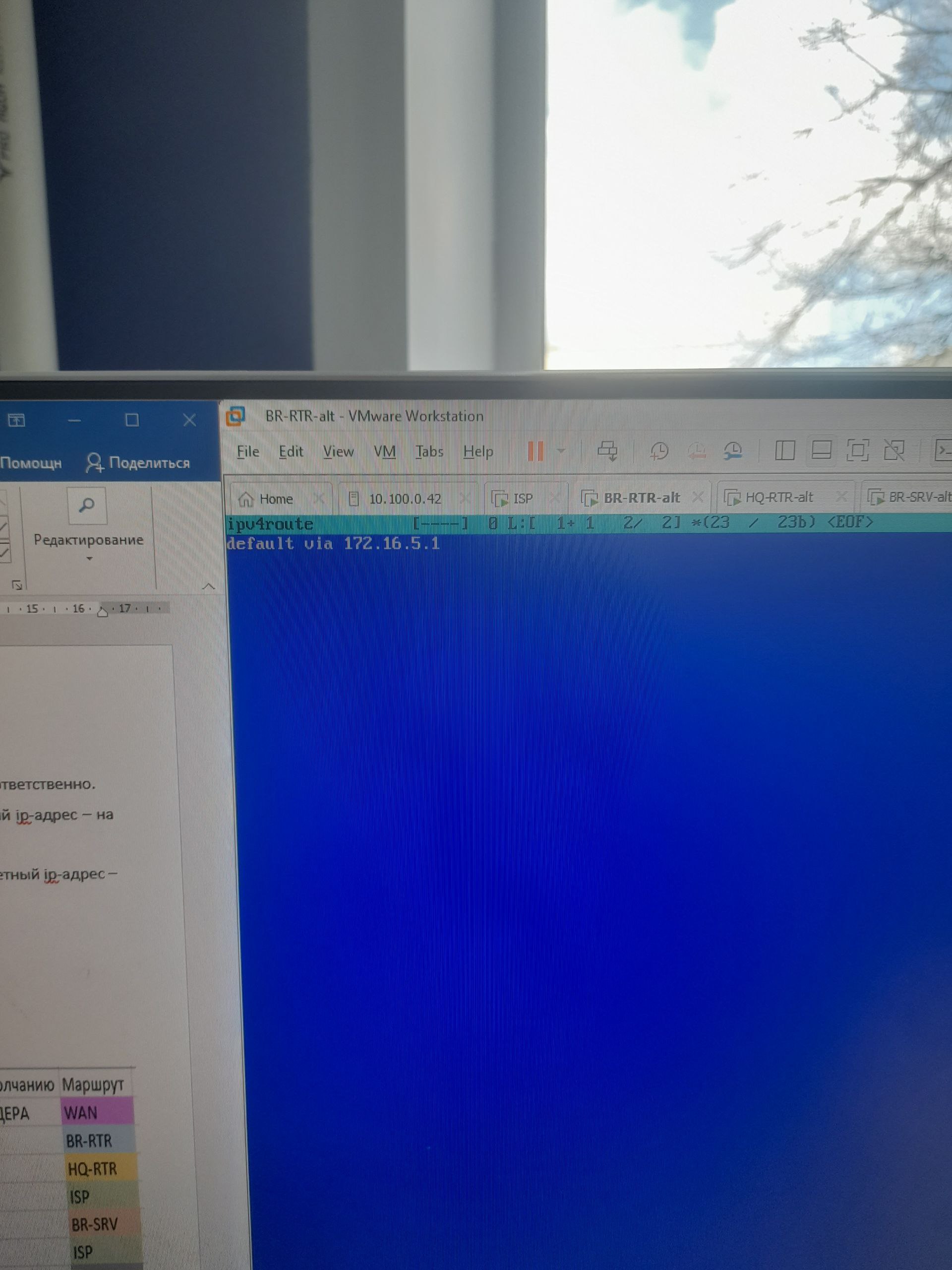
timedatectl set-timezone Asia/Novosibirsk

hostnamectl set-hostname br-rtr.au-team.irpo && exec bash

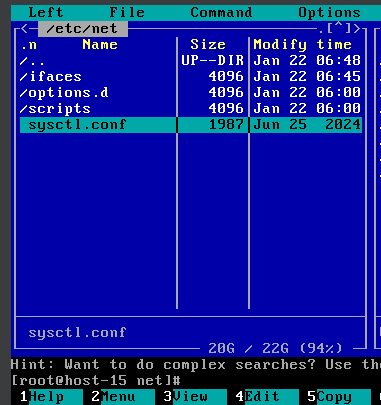
СОЗДАЕМ ENS224 (И КОЕЧТО ДАБАВЛЯЕМ В ENS192 ):



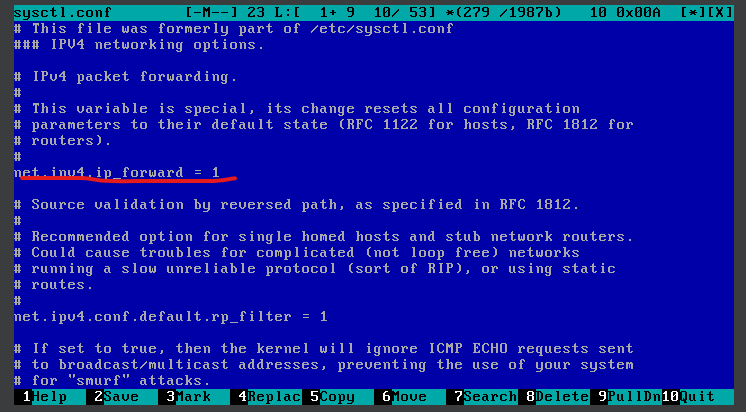
В IPV4ADDRESS ПИШИМ АДРИС 172.16.5.1/28



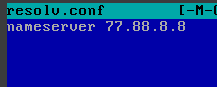
В ENS224 ПИШИЕМ ТОЖЕ САМОЕ ТОЛЬКО БЕЗ IPV4ROUTE(НУ И АЙПИ ДРУГОЙ )



В скриншоте ниже указано, как должна выглядеть настройка IP-Forward.



DNS-клиент требуется добавить на всех машинах **кроме ISP**. В **клиенте уже ничего делать не нужно**, ведь DNS-клиент мы указали там ранее вместе с ip-адресом, маской и шлюзом. В остальных же машинах мы через **mc** заходим в конфиг по пути /etc/resolf.conf. Указываем DNS-сервер Яндекса как изображено ниже.



*systemctl restart network*

Настройка NAT

Скачиваем *apt-get update && apt-get install* iptables

iptables -t nat -A POSTROUTING -o ens192 -s 172.16.6.0/27-j MASQUERADE

**Настройка BR-SRV**

Делаем везде одной команой на isp надо установить tzdata командой apt-get install tzdata -y (после настройки интернета)

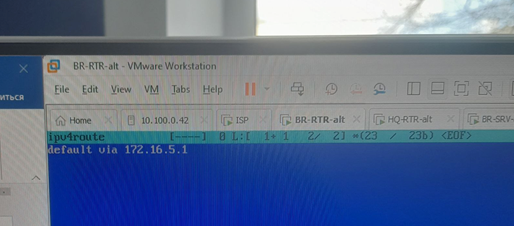
timedatectl set-timezone Asia/Novosibirsk

Присваиваем полные доменные имена устройствам согласно топологии:

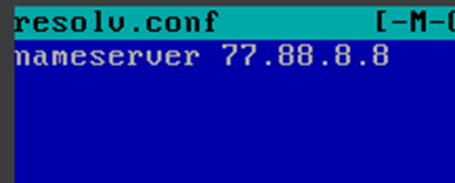
hostnamectl set-hostname br-srv.au-team.irpo && exec

Оствавляем options и только дописываем ipv4address и ipv4route

Пример ( не забыть писать default via)



Можно будет напасть dns-сервер :



**Настройка hq-rtr :**

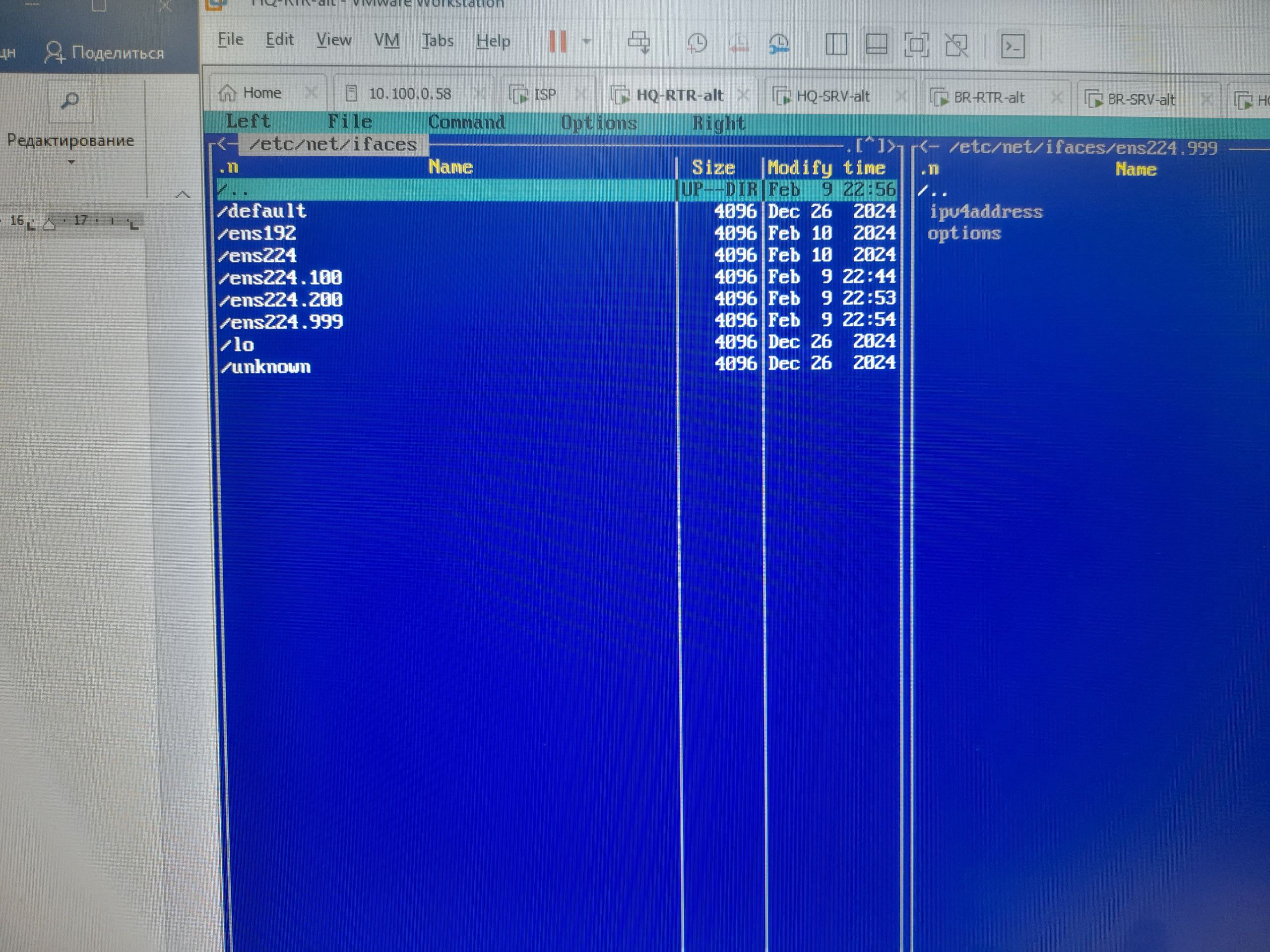
**Делаем везде одной команой** на isp надо установить tzdata командой apt-get install tzdata -y (после настройки интернета)

timedatectl set-timezone Asia/Novosibirsk

Присваиваем полные доменные имена устройствам согласно топологии:

hostnamectl set-hostname hq-rtr.au-team.irpo && exec bash

также создаем ens224 и vlan



В ens224 мы пишем только optios а в ens192 мы пишем ipv4address и ipv4route

В vlan ens192 мы оставляем только options

**Настройка VLAN**

#### Создание VLAN для офиса HQ – VLAN100

1. Создайте каталог для подинтерфейса (замените <имя\_физического\_интерфейса> на фактическое имя, например, ens224):

mkdir -p /etc/net/ifaces/224.100

1. Отредактируйте файл настроек:

nano /etc/net/ifaces/224.100/options

Пример содержимого:

TYPE=vlan

HOST=ens34

VID=100

DISABLED=no

BOOTPROTO=static

ONBOOT=yes

CONFIG\_IPV4=yes

1. Создайте файл для задания IP-адреса:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.100/ipv4address

Пример:

192.168.10.1/26

#### Создание VLAN для офиса HQ – VLAN200

1. Создайте каталог для подинтерфейса:

mkdir -p /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.200

1. Отредактируйте файл настроек:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.200/options

Пример содержимого:

TYPE=vlan

HOST=ens224

VID=200

DISABLED=no

BOOTPROTO=static

ONBOOT=yes

CONFIG\_IPV4=yes

1. Создайте файл для задания IP-адреса:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.200/ipv4address

Укажите IP-адрес в формате ip/mask.

#### Создание VLAN для управления – VLAN999

1. Создайте каталог для подинтерфейса:

mkdir -p /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.999

1. Отредактируйте файл настроек:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.999/options

Пример содержимого:

TYPE=vlan

HOST=ens34

VID=999

DISABLED=no

BOOTPROTO=static

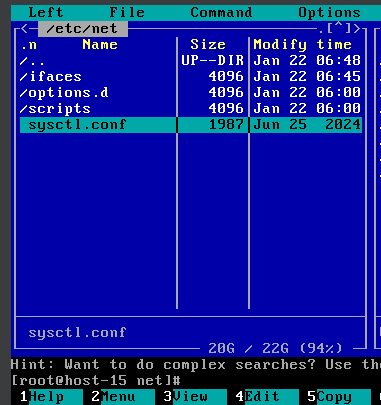
ONBOOT=yes

CONFIG\_IPV4=yes

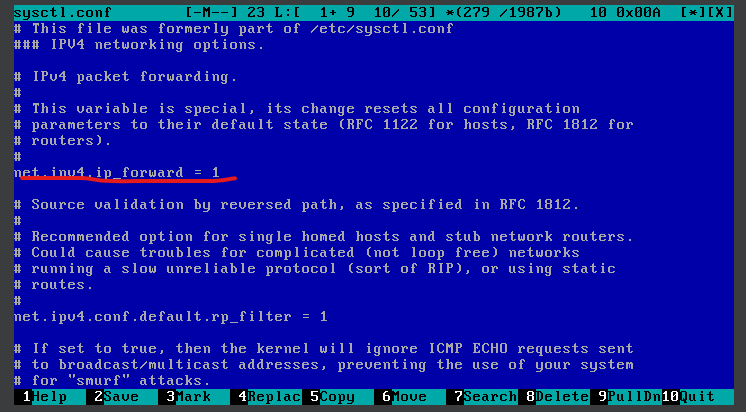
1. Создайте файл для задания IP-адреса:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.999/ipv4address

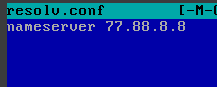
Укажите IP-адрес в формате ip/mask.



В скриншоте ниже указано, как должна выглядеть настройка IP-Forward.



DNS-клиент требуется добавить на всех машинах **кроме ISP**. В **клиенте уже ничего делать не нужно**, ведь DNS-клиент мы указали там ранее вместе с ip-адресом, маской и шлюзом. В остальных же машинах мы через **mc** заходим в конфиг по пути /etc/resolf.conf. Указываем DNS-сервер Яндекса как изображено ниже.



*systemctl restart network*

На hq-rtr

iptables -t nat -A POSTROUTING -o ens192 -s 192.168.1.0/26 -j MASQUERADE

iptables -t nat -A POSTROUTING -o ens192 -s 192.168.2.0/28-j MASQUERADE

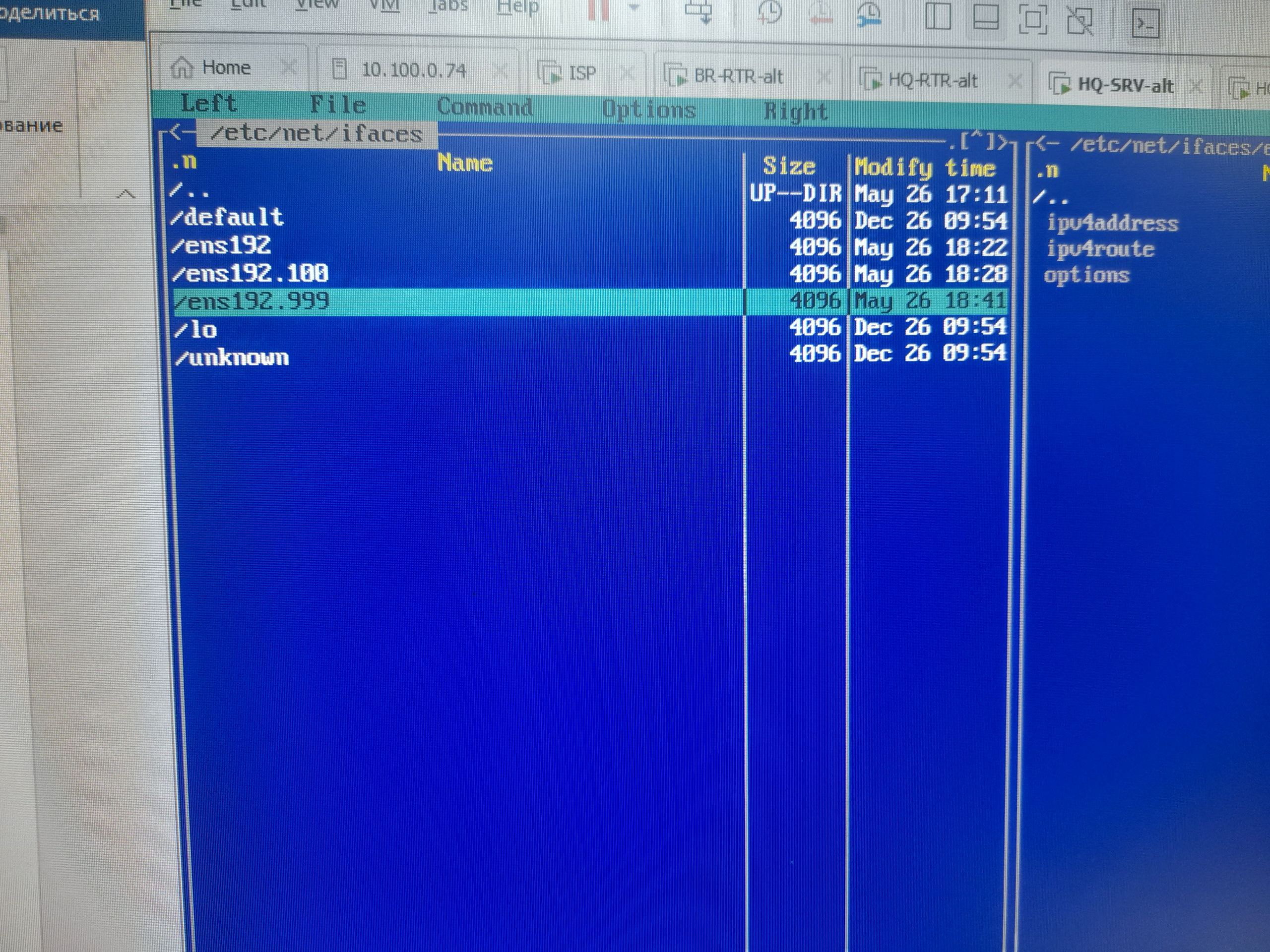
**Настройка hq-srv**

**Делаем везде одной команой** на isp надо установить tzdata командой apt-get install tzdata -y (после настройки интернета)

timedatectl set-timezone Asia/Novosibirsk

Присваиваем полные доменные имена устройствам согласно топологии:

hostnamectl set-hostname hq-srv.au-team.irpo && exec bash



**Настройка VLAN**

#### Создание VLAN для офиса HQ – VLAN100

1. Создайте каталог для подинтерфейса (замените <имя\_физического\_интерфейса> на фактическое имя, например, ens224):

mkdir -p /etc/net/ifaces/224.100

1. Отредактируйте файл настроек:

nano /etc/net/ifaces/224.100/options

Пример содержимого:

TYPE=vlan

HOST=ens34

VID=100

DISABLED=no

BOOTPROTO=static

ONBOOT=yes

CONFIG\_IPV4=yes

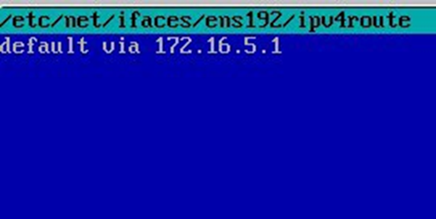
1. Создайте файл для задания IP-адреса:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.100/ipv4address

Пример:

192.168.10.1/26

Ipv4route :



#### Создание VLAN для управления – VLAN999

1. Создайте каталог для подинтерфейса:

mkdir -p /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.999

1. Отредактируйте файл настроек:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.999/options

Пример содержимого:

TYPE=vlan

HOST=ens34

VID=999

DISABLED=no

BOOTPROTO=static

ONBOOT=yes

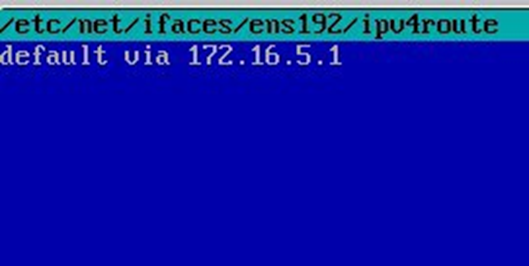
CONFIG\_IPV4=yes

1. Создайте файл для задания IP-адреса:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.999/ipv4address

Укажите IP-адрес в формате ip/mask.

Ipv4route:



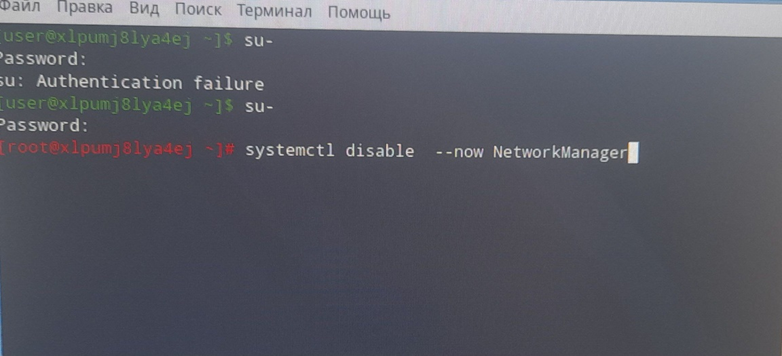
**Настройка hq-cki**

**Делаем везде одной команой** на isp надо установить tzdata командой apt-get install tzdata –y настройка через виджет

timedatectl set-timezone Asia/Novosibirsk

hostnamectl set-hostname hq-cli.au-team.irpo && exec

Прежде чем делать что то на клиента нужно:



В ens192 только options

#### Создание VLAN для офиса HQ – VLAN200

1. Создайте каталог для подинтерфейса:

mkdir -p /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.200

1. Отредактируйте файл настроек:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.200/options

Пример содержимого:

TYPE=vlan

HOST=ens224

VID=200

DISABLED=no

BOOTPROTO=static

ONBOOT=yes

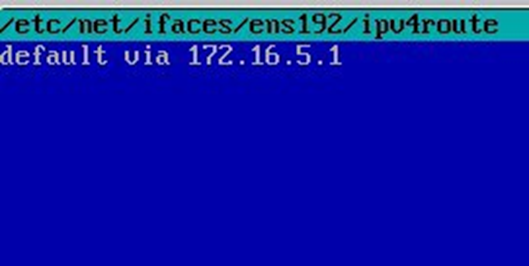
CONFIG\_IPV4=yes

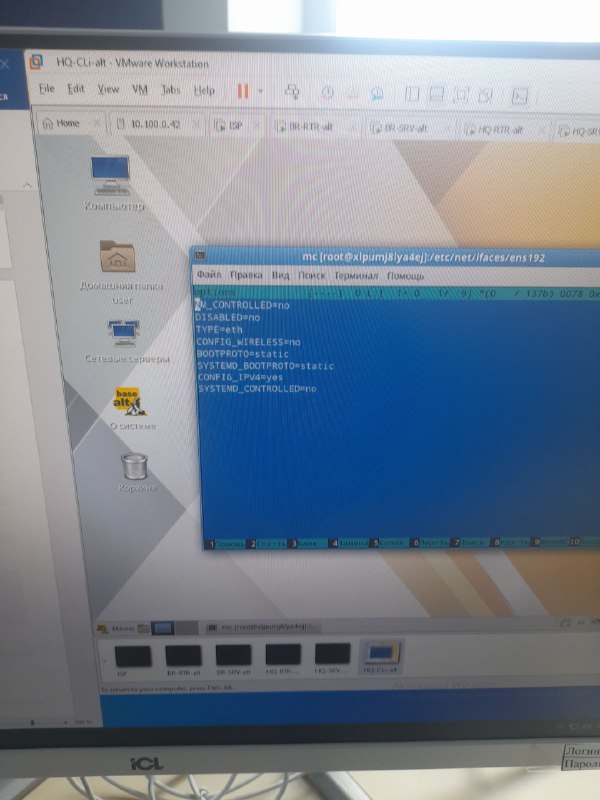
1. Создайте файл для задания IP-адреса:

nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.200/ipv4address

Укажите IP-адрес в формате ip/mask.

Ipv4route : это только на клиенте и на сервере





**Создание пользователя на роутерах и серверах**

Для сначала добавим пользователя **sshuser** на наши сервера:

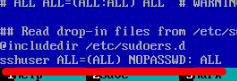
*adduser sshuser -u 1010*

Задаём пароль:

*passwd sshuser*

Мы должны будем дважды ввести пароль, который хотим поставить. Пароль в данном случае – P@ssw0rd.

Через **mc** заходим в командный файл **/etc/sudoers** и в нём нам нужно добавить следующую строчку:



Затем мы должны добавить пользователя в группу **wheel**:

*usermod -aG wheel sshuser*

Теперь проверяем, может ли наш пользователь заходить в **sudo** без доп. аутентификации. Для начала выходим из пользователя **root**:

*Logout (exit если не проходит первая команда )*

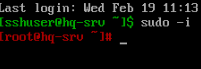
Теперь входим в новоиспеченного пользователя:

*sshuser*

*P@ssw0rd*

*sudo -i*

Лицезреть в итоге мы должны это:



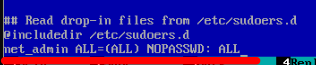
Теперь занимаемся пользователем на роутерах:

*adduser net\_admin*

*passwd net\_admin*

*P@$$word* (x2)

*mc /etc/sudoers*



*usermod -aG wheel net\_admin*

*logout*

*net\_admin*

*P@$$word*

*sudo -i*

Смотрим:

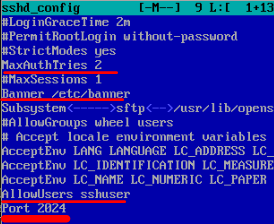


**Настройка безопасного удаленного доступа (ssh) на серверах**

Работа с удаленным доступом ведется НА СЕРВЕРАХ. Для начала заходим в **mc** и с помощью команды *touch* создаём файл **/etc/banner**, в котором печатаем следующую картину:



Теперь нам пора зайти в файл **/etc/openssh/sshd\_config**. Здесь очень важно добавить следующие строчки:



Как всегда, не забываем прожимать f2, чтобы сохранить. Перезапускаем ssh:

*systemctl restart sshd*

Идём на соответствующий нашему серверу роутер. Там, чтобы войти на сервер через удаленный доступ, вводим следующее:

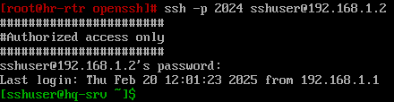
*ssh -p 2024 sshuser@192.168.1.2*

Это на HQ-RTR, на BR-RTR будет:

*ssh -p 2024 sshuser@10.16.1.2*

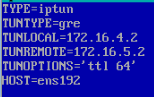
Нас спросят, хотим ли мы продолжить подключение. Пишем *yes*.

Вводим пароль, который мы ранее задали для пользователя **sshuser** и, если вы всё сделали правильно, выглядеть это будет так:



**Конфигурация ip-туннеля между роутерами (*gre)***

Все приведенные операции нужно будет осуществить на роутерах. Уже с самого начала мы заходим в **mc**. Конкретно нас интересует директория mkdir /etc/net/ifaces. Здесь мы нажимаем **f7**, чтобы создать папку gre1 и файл с именем **options**. Из директории пока никуда не уходим, ведь нужно сразу же создать еще одну папку – **ipv4address**. А вот уже теперь с помощью клавиши **f4** заглядываем внутрь **options** и пишем следующие строчки:



Обращаем внимание: в строчке **TUNLOCAL** нужно указать ip-адрес той машины, на которой вы находитесь в данный момент. В строчке **TUNREMOTE** же мы указываем ip-адрес соседа этой машины. Если мы на **HR-RTR**, то это будет адрес **BR-RTR**. На **BR-RTR** в файле **options**, как нетрудно догадаться, будет то же самое, но только строчки **TUNLOCAL** и **TUNREMOTE** поменяются айпишниками.

Сохраняем файл клавишей **f2** и выходим клавишей **f10**.

Дальше всё очень просто – идём в файл **ipv4address**, расположенный всё в той же папке **tun1** и пишем здесь айпишник начала (или конца) туннеля. Айпишник для туннеля легко можно придумать. Допустим, так:



(*HQ-RTR*)



(*BR-RTR*)

Сохраняем и выходим из **mc**. Как обычно, перезагружаем систему **Network**:

*systemctl restart network*

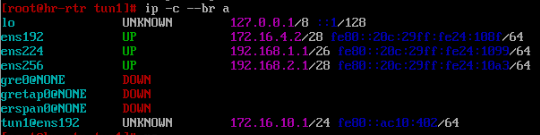
Теперь мы должны включить модуль ядра для **gre**:

*modprobe gre*

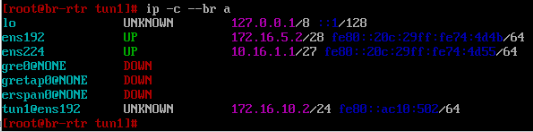
Проверяем созданный нами конец туннеля:

*ip -c --br a*

Как мы видим, конец туннеля – на месте:



(*HQ-RTR*)



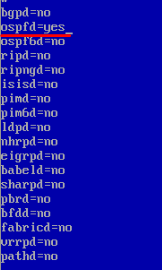
(*BR-RTR*)

**Настройка динамической маршрутизации между офисами**

По-прежнему работаем на роутерах HQ и BR. Перво-наперво нам точно нужно установить **frr** – пакет для гибкой настройки маршрутизации:

*apt-get update && apt-get install -y frr*

Посредством **mc** заходим в файл **etc/frr/daemons** и активируем службу **ospfd**. Строчка службы должна выглядеть так:

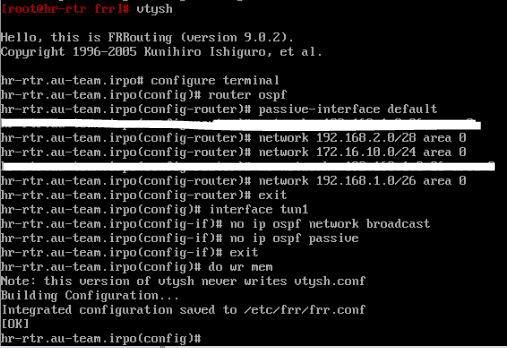


*перед как проверить перезагрузить systemctl restart frr*

Теперь нам стоит проверить, включена ли служба, с помощью специальной команды:



Дальше работаем с **frr**. Точно повторяем команды со скриншота по порядку. Работа с **frr** на скриншоте касается **HQ-RTR**:



Теперь, чтобы выйти из терминала в **frr**, вводим:

*exit*

C **BR-RTR** принцип такой же:

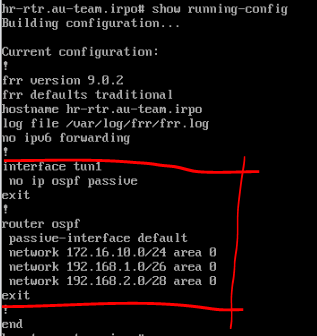


*exit*

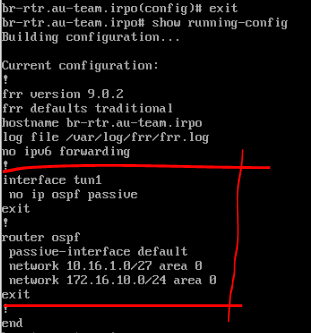
Для проверки, правильно ли всё было нами введено:

*show running-config*

Вот так это должно выглядеть на **HQ-RTR**:



Вот так это должно выглядеть на **BR-RTR**:

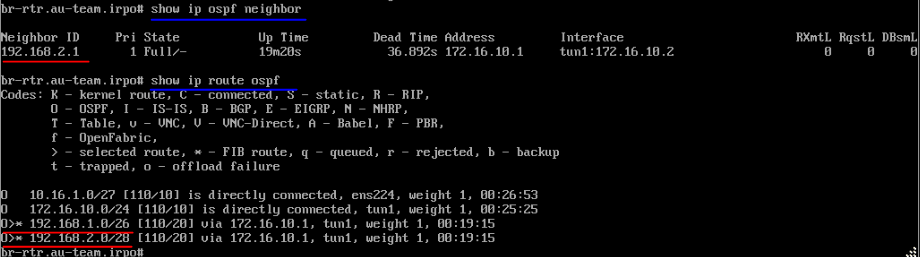


Проверить, имеется ли маршрутизация между роутерами, мы будем так.

Результат на **HQ-RTR** нас интересует такой:



Результат на **BR-RTR** нас интересует такой:



Сейчас мы должны заняться установкой парольной защиты для **frr**. Из **vtysh** мы пока не выходили, следовательно печатаем:

*configure terminal*

*interface tun1*

Активируем аутентификацию и задаём пароль:

*ip ospf authentication*

*ip ospf authentication-key PLAINPAS*

Выходим из конфигурации интерфейса, сохраняем изменение в настройках, а затем выходим и из терминала:

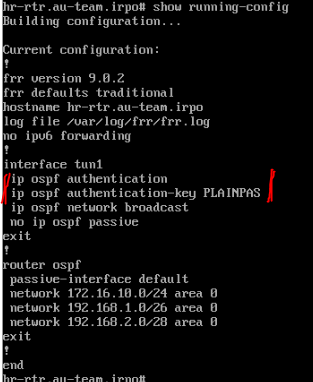
*exit*

*do wr mem*

*exit*

Как только защита протокола будет стоять на обоих роутерах, мы должны будем проверить наличие защиты:

*show running-config*



Важно: **пароль на роутерах должен стоять строго одинаковый**.

**Настройка протокола динамической конфигурации хостов (DHCP)**

Нашим dhcp-сервером будет выступать HQ-RTR. Перво-наперво установим пакеты для dhcp-сервера:

*apt-get update && apt-get install dhcp-server*

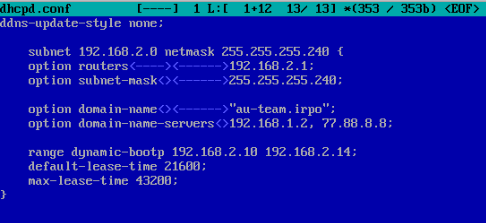
Включим автоматический запуск протокола при запуске системы:

*Systemctl enadle –now dhcpd*

Собственно запускаем протокол:

*Systemctl start dhcpd*

Теперь въезжаем в **mc** и с помощью программной команды **touch** по пути **/etc/dhcp/** создаём файл **dhcpd.conf**. Открываем файл и заполняем:



Здесь очень важно учесть следующие моменты:

-после subnet нам нужно указать подсеть HQ-CLI, а после netmask – его маску в полном формате;

-в строчке **option routers** мы указываем адрес **HQ-RTR**, смотрящий в сторону **HQ-CLI**.

-в строчке **subnet-mask** указываем такую же маску;

-DNS-суффикс по заданию – **au-team.irpo**, указываем в кавычках.

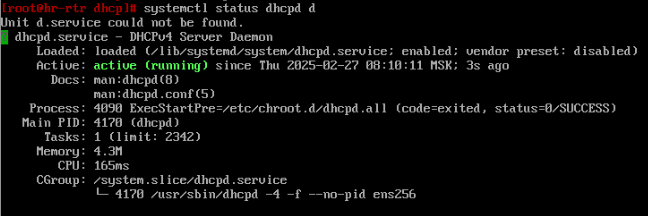
-в **option domain-name-servers** указать требуется адрес с центрального интерфейса **HQ-SRV**. А рядом – DNS-сервер яндекса (77.88.8.8);

-в строчке **range dynamic-bootp** мы указываем диапазон адресов в подсети **HQ-CLI**. Диапазон лучше сделать с 10 до 14;

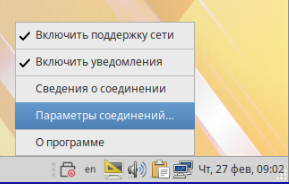
-смотрим ВНИМАТЕЛЬНО, чтобы после каждая строчка кроме самой первой кончалась точкой и запятой, иначе **dhcp** не заработает;

-лучше убрать из файла все лишние строчки.

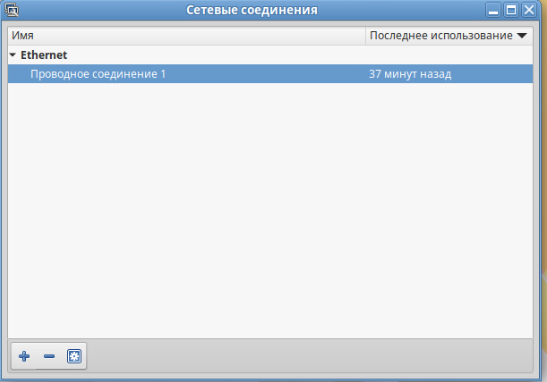
Теперь проверяем статус службы специальной командой:



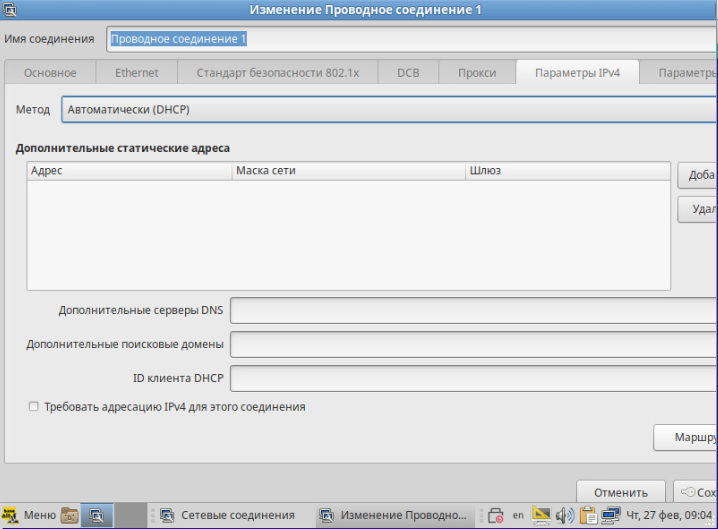
Теперь идём в машинку клиента. Здесь по соответствующей иконке кликаем правой кнопкой мыши.



Нас интересует вариант **Параметры соединений…**, кликаем на него.



Теперь кликаем дважды по **Проводное соединение 1**. Здесь нам нужно переместиться по вкладку **Параметры IPV4**. Меняем метод выхода в сеть с **Вручную** на **Автоматически (DHCP)**. Стираем адрес, маску сети, шлюз и DNS-сервер, которые мы ранее указывали.



Нажимаем на **Сохранить** и выходим. Проверить выход в интернет мы можем, зайдя в браузер и открыв сайт википедии.

*DNS сервер*

*Скачиваем*

*apt-get install -y bind bind-utils*

Для добавления в автозагрузку написать команду:

systemctl enable --now bind

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

search au-team.irpo

nameserver 127.0.0.1

nameserver 192.168.100.62

nameserver 77.88.8.8

Прописываем в /etc/bind/local.conf:

zone "au-team.irpo" {

type master;

file "au-team.irpo.db";

};

cp /etc/bind/zone/localdomain /etc/bind/zone/au-team.irpo.db

Даём права

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

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

заходи в au-team.irpo.db и исправляем под скрин снизу

$TTL 1D

@ IN SOA au-team.irpo. root.au-team.irpo. (

2024102200 ; serial

12H ; refresh

1H ; retry

1W ; expire

1H ; ncache

)

IN NS au-team.irpo.

IN A 192.168.100.62

hq-rtr IN A 192.168.100.1

br-rtr IN A 192.168.0.1

hq-srv IN A 192.168.100.62

hq-cli IN A 192.168.200.14

br-srv IN A 192.168.0.30

moodle IN CNAME hq-rtr

wiki IN CNAME hq-rtr

чтобы проверить ошибки в коде

named-checkconf -z

#### Создание и настройка обратных зон

Прописываем их в **/etc/bind/local.conf**:

zone "100.168.192.in-addr.arpa" {

type master;

file "100.168.192.in-addr.arpa";

};

zone "200.168.192.in-addr.arpa" {

type master;

file "200.168.192.in-addr.arpa";

};

копируем файлы, чтобы не писать лишнего и потом изменим настройки под себя

cp /etc/bind/zone/127.in-addr.arpa /etc/bind/zone/100.168.192.in-addr.arpa

cp /etc/bind/zone/127.in-addr.arpa /etc/bind/zone/200.168.192.in-addr.arpa

chown named. /etc/bind/zone/100.168.192.in-addr.arpa

chmod 600 /etc/bind/zone/100.168.192.in-addr.arpa

chown named. /etc/bind/zone/200.168.192.in-addr.arpa

chmod 600 /etc/bind/zone/200.168.192.in-addr.arpa

заходим в /etc/bind/zone/100.168.192.in-addr.arpa

$TTL 1D

@ IN SOA au-team.irpo. root.au-team.irpo. (

2024102200 ; serial

12H ; refresh

1H ; retry

1W ; expire

1H ; ncache

)

IN NS au-team.irpo.

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

62 IN PTR hq-srv.au-team.irpo.

заходим в /etc/bind/zone/200.168.192.in-addr.arpa

$TTL 1D

@ IN SOA au-team.irpo. root.au-team.irpo. (

2024102200 ; serial

12H ; refresh

1H ; retry

1W ; expire

1H ; ncache

)

IN NS au-team.irpo.

14 IN PTR hq-cli.au-team.irpo.

Перезапуск

systemctl restart bind