|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска | VLAN | Подсеть | Шлюз |
| ISP | ens18 | DHCP | DHCP | - | DHCP | DHCP |
| ens19 | 172.16.1.1 | /28 | - | 172.16.1.0/28 | - |
| ens20 | 172.16.1.1 | /28 | - |  | - |
| HQ-RTR | int0 (to ISP) | 172.16.1.2 | /28 | - |  | 172.16.1.1 |
| int1.100 | 192.168.1.1 | /27 | 100 |  | - |
| int1.200 | 192.168.2.1 | /28 | 200 |  | - |
| int1.999 | 192.168.3.1 | /29 | 999 |  | - |
| Tunnel.0  (IP туннель) | 172.16.100.1 | /29 | - |  | - |
| BR-RTR | int0 (to ISP) | 172.16.2.2 | /28 | - |  | 172.16.2.1 |
| int1 (to BR-SRV) | 10.10.1.1 | /28 | - |  | - |
| Tunnel.0  (IP туннель) | 172.16.100.2 | /29 | - |  | - |
| HQ-SRV | ens18 (to HQ-RTR) | 192.168.1.2  192.168.3.2 | /27  /29 | 100  300 |  | 192.168.1.1  192.168.3.1 |
| BR-SRV | ens18 (to BR-RTR) | 10.10.1.2 | /28 |  |  | 10.10.1.1 |
| HQ-CLI | ens18 (to HQ-RTR) | 192.168.2.2 | /28 | 200 |  | 192.168.2.1 |

Jornalctl -xeu

**Настройка isp**

Для начала проверим название интерфейса через команду ip a. Как узнали название интерфейса необходимо создать для него папку с помощью этой команды:

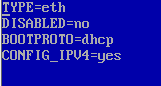
mkdir /etc/net/ifaces/ens192

Создаем конфигурационный файл для настройки подачи интернета через провайдера, используя vim:

vim /etc/net/ifaces/ens192/options

Для конфигурации необходимо нажать кнопку i.

После этого пишем данный текст:



Нажимаем Esc и пишем:

:wq

Далее можно установить Midnight Commander, необязательно, но явно облегчит работу:

apt-get update && apt-get install mc

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

После установки необходимо добавить еще два интерфейса для дальнейшей работы:

mkdir /etc/net/ifaces/ens20

mkdir /etc/net/ifaces/ens21

В них надо настроить раздачу адресов для подачи интернета в другие подсети. Чтобы это сделать надо создать в каждом интерфейсе файл ipv4address и вписать в эти файлы IP-адреса которые даны в таблице:

touch /etc/net/ifaces/ens20/ipv4address

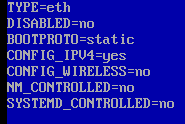
touch /etc/net/ifaces/ens21/ipv4address

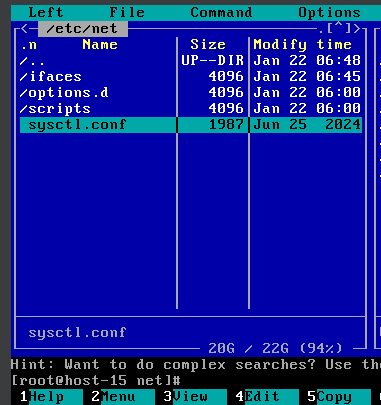
Когда вписаны IP-адреса создаем также и файлы настройки для каждого интерфейса:

touch /etc/net/ifaces/ens20/options

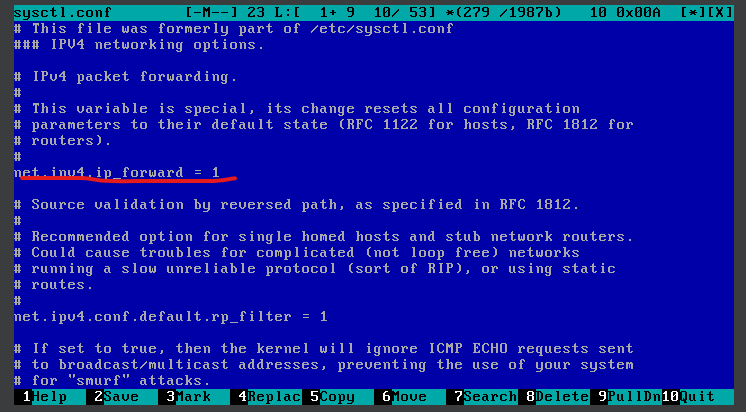
touch /etc/net/ifaces/ens21/options

В них вписываем эти строки:





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 ens19 -j MASQUERADE

Сохраним правило:

iptables-save > /etc/sysconfig/iptables

Добавим iptables в автозагрузку:

systemctl enable –now iptables

**Настройка BR-RTR**

Для начала проверим название интерфейса через команду ip a. Как узнали название интерфейса необходимо создать для него папку с помощью этой команды:

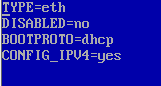
mkdir /etc/net/ifaces/ens192

Создаем конфигурационный файл для настройки подачи интернета через провайдера, используя vim:

vim /etc/net/ifaces/ens192/options

Для конфигурации необходимо нажать кнопку i.

После этого пишем данный текст:



Нажимаем Esc и пишем:

:wq

Далее можно установить Midnight Commander, необязательно, но явно облегчит работу:

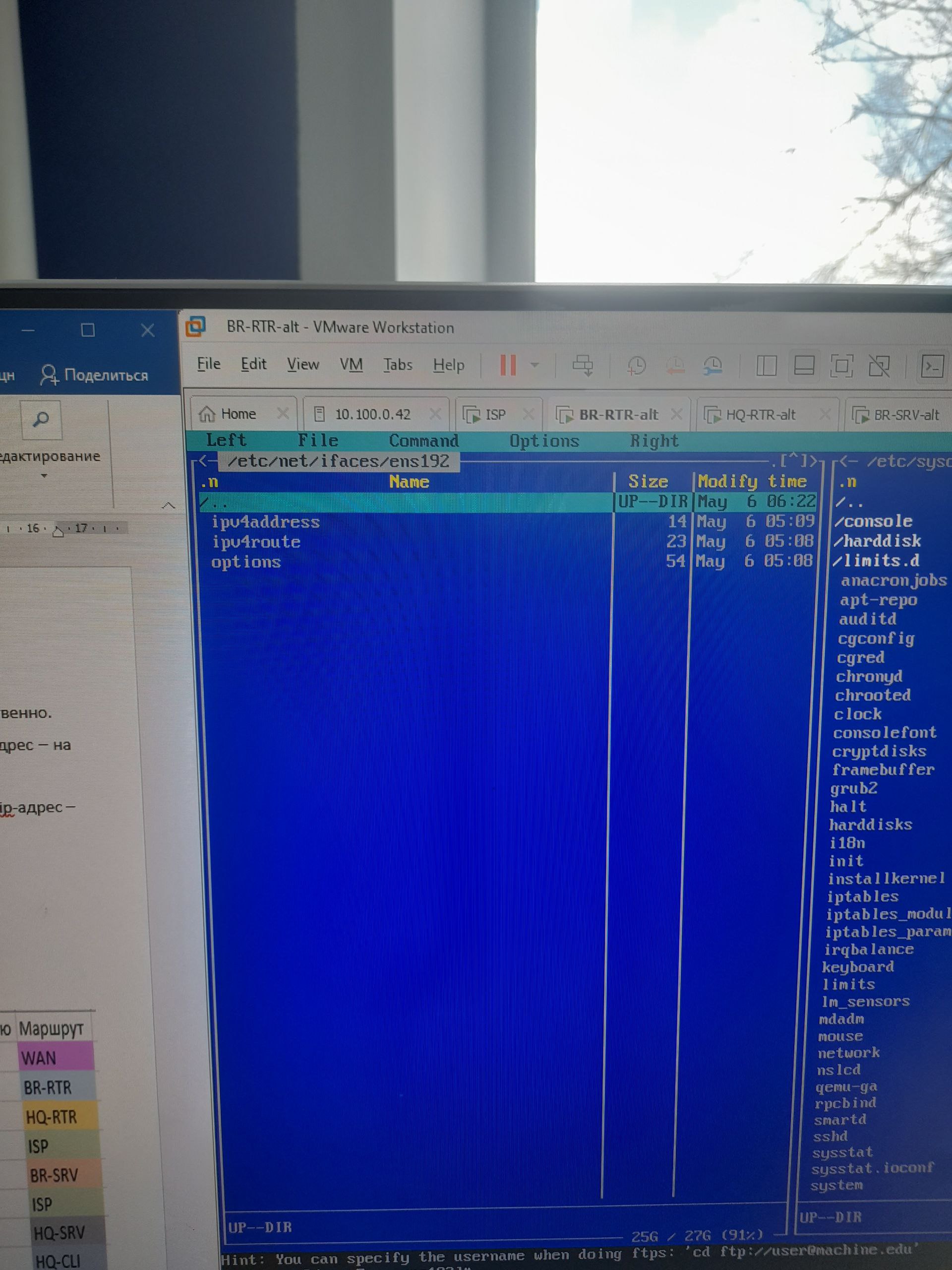
apt-get update && apt-get install mc

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

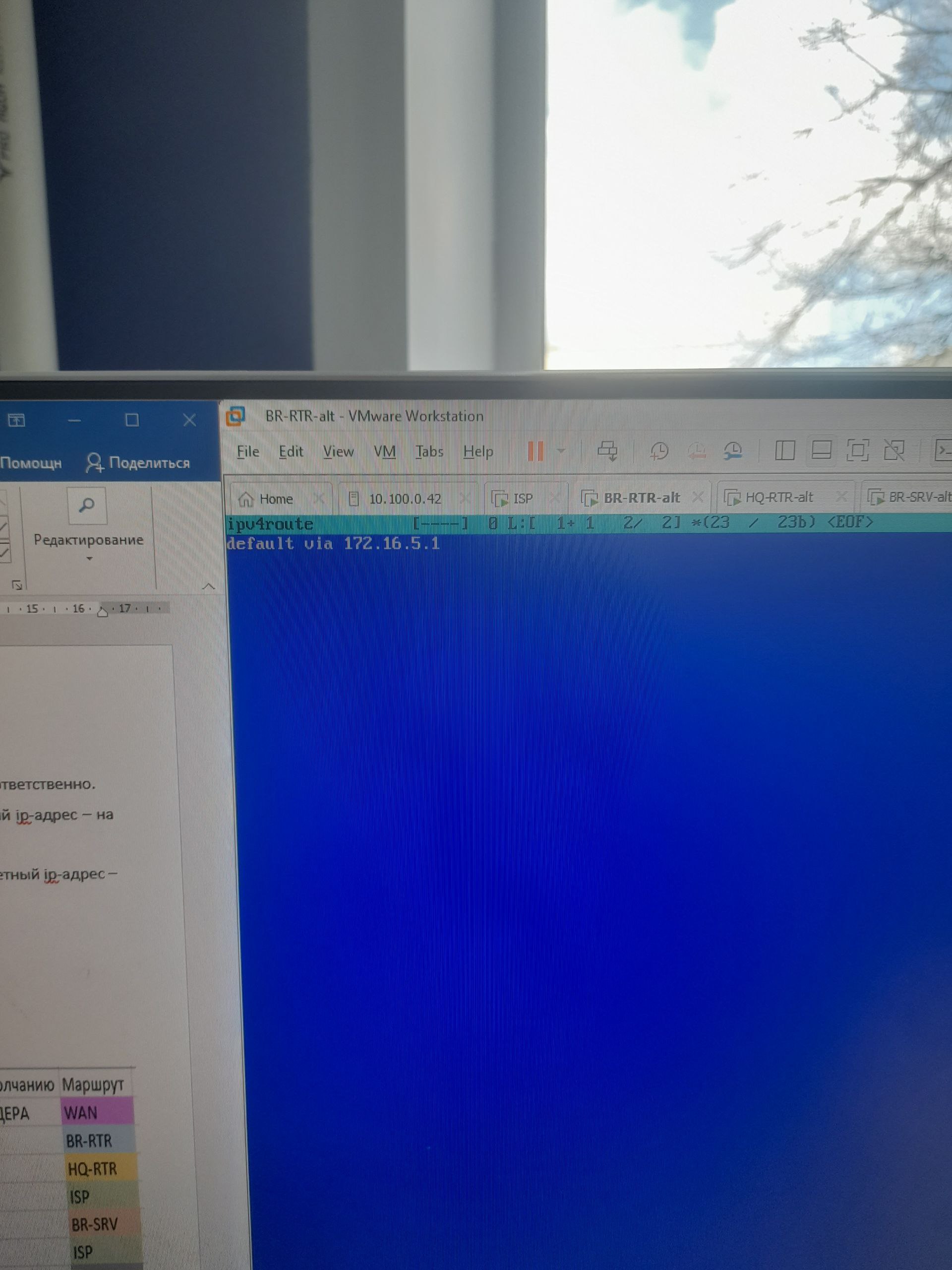
timedatectl set-timezone Asia/Novosibirsk

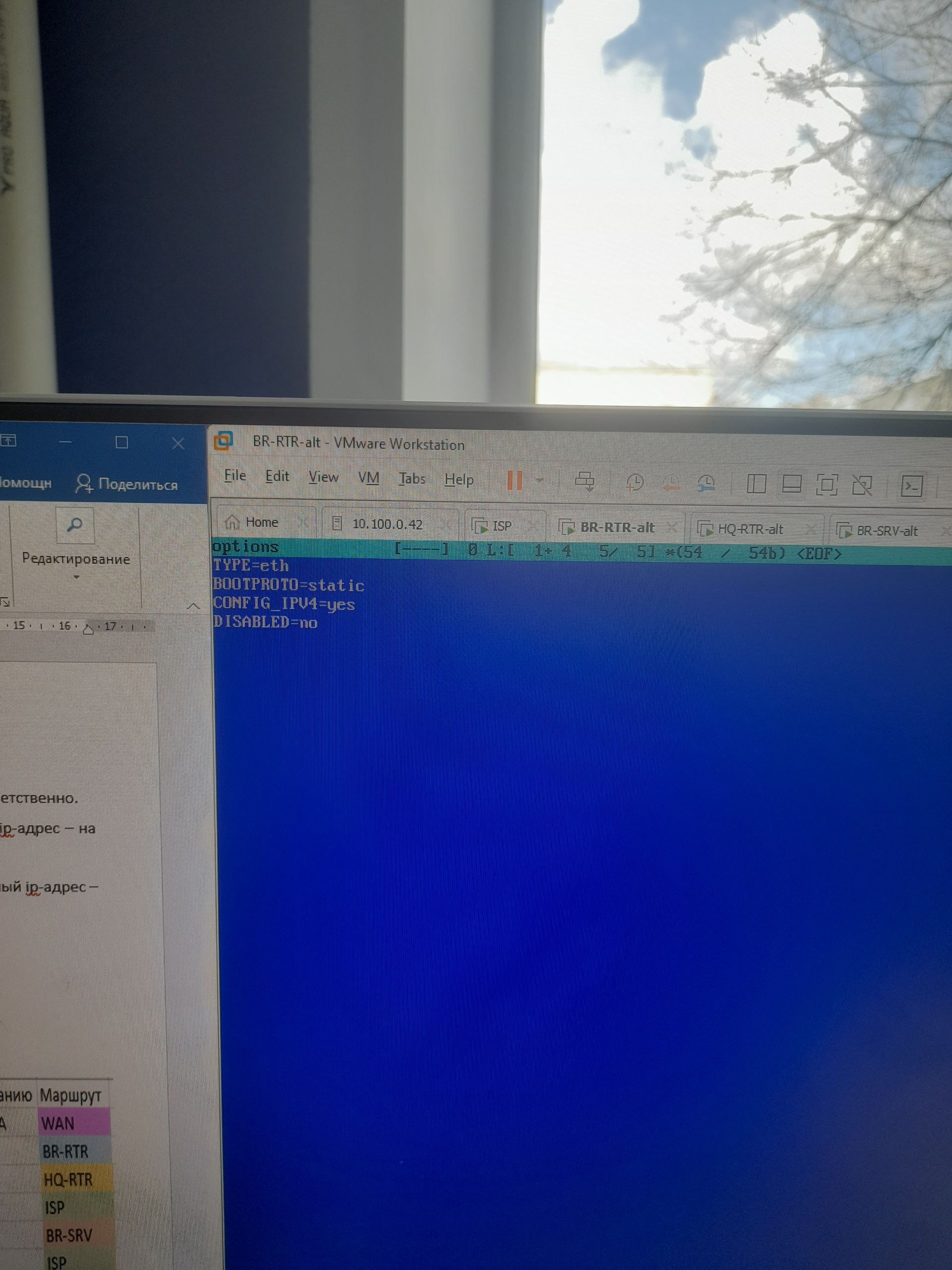
hostnamectl set-hostname br-rtr.au-team.irpo && exec bash

СОЗДАЕМ ENS20(И КОЕ ЧТО ДАБАВЛЯЕМ В ENS19):

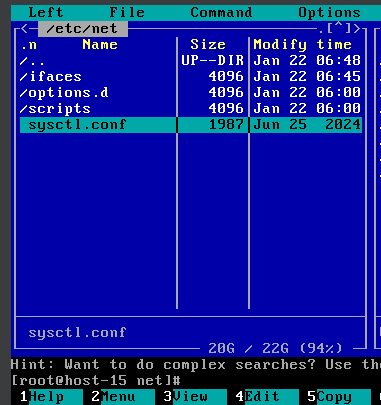


В IPV4ADDRESS ПИШИМ АДРИС

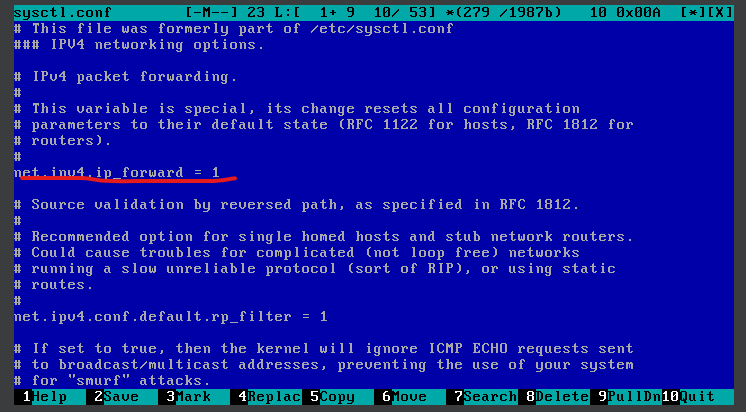


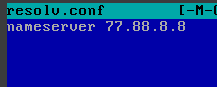


В ENS20 ПИШИЕМ ТОЖЕ САМОЕ ТОЛЬКО БЕЗ IPV4ROUTE(НУ И АЙПИ ДРУГОЙ )



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





*systemctl restart network*

Настройка NAT

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

iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE

Сохраним правило:

iptables-save > /etc/sysconfig/iptables

Добавим iptables в автозагрузку:

systemctl enable –now iptables

**Создание пользователя на роутерах**

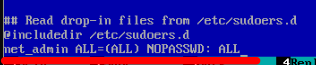
*adduser net\_admin*

*passwd net\_admin*

*P@$$word* (x2)

apt-get update && apt-get install sudo -y

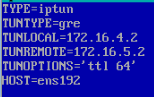
*mc /etc/sudoers*



*usermod -aG wheel net\_admin*

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

*/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****.*

**

***TUNLOCAL*** *ip-адрес той машины, на которой вы находитесь в данный момент. Это ip br-rtr*

***TUNREMOTE*** *p-адрес соседа этой машины. Это ip hq-rtr*

*Дальше всё очень просто – идём в файл ipv4address и пишем той внутреней сети*

***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:

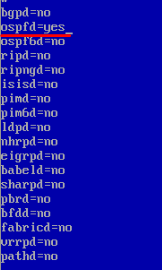
*ip -c --br a*

**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*

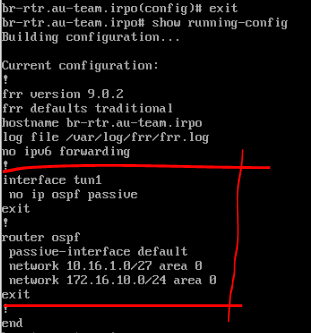
Теперь нам стоит проверить, включена ли служба, с помощью специальной команды:

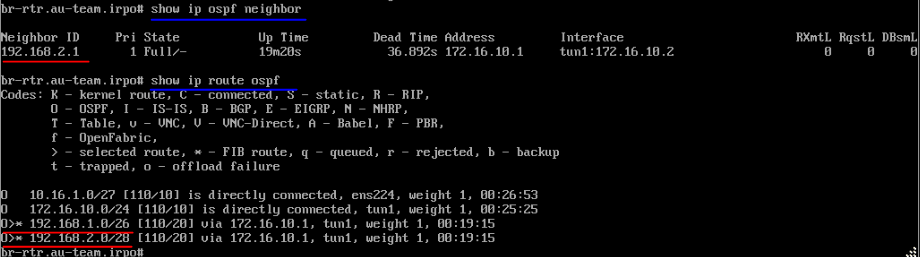
**

*exit*

Для проверки, правильно ли всё было нами введено:

*show running-config*

**

**

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:

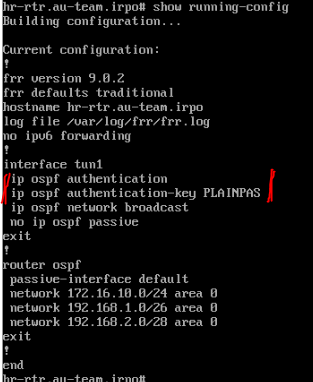
*exit*

*do wr mem*

*exit*

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

*show running-config*

**

**Настройка BR-SRV**

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

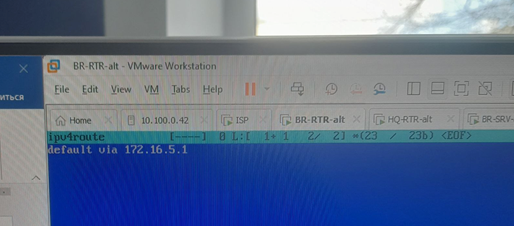
timedatectl set-timezone Asia/Novosibirsk

Присваиваем полные доменные имена устройствам согласно топологии:

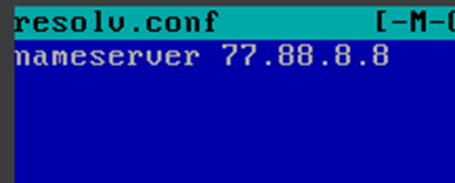
hostnamectl set-hostname br-srv.au-team.irpo && exec

Оствавляем options и только дописываем ipv4address и ipv4route

Пример ( не забыть писать default via)



Можно будет напасть dns-сервер :

**

***Создание пользователя на серверах***

*скачать apt-get update&& apt-get install sudo -y*

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

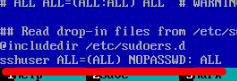
*adduser sshuser -u 1010*

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 )*

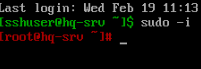
Теперь входим в новоиспеченного пользователя:

*sshuser*

*P@ssw0rd*

*sudo -i*

Лицезреть в итоге мы должны это:

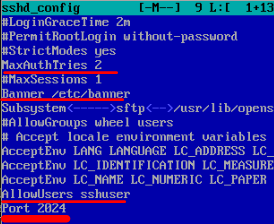
**

***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:

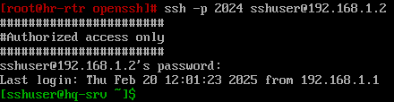
*ssh -p 2024 sshuser@192.168.1.2*

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:



***Настройка hq-rtr :***

Для начала проверим название интерфейса через команду ip a. Как узнали название интерфейса необходимо создать для него папку с помощью этой команды:

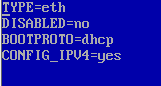
mkdir /etc/net/ifaces/ens192

Создаем конфигурационный файл для настройки подачи интернета через провайдера, используя vim:

vim /etc/net/ifaces/ens192/options

Для конфигурации необходимо нажать кнопку i.

После этого пишем данный текст:



Нажимаем Esc и пишем:

:wq

Далее можно установить Midnight Commander, необязательно, но явно облегчит работу:

apt-get update && apt-get install mc

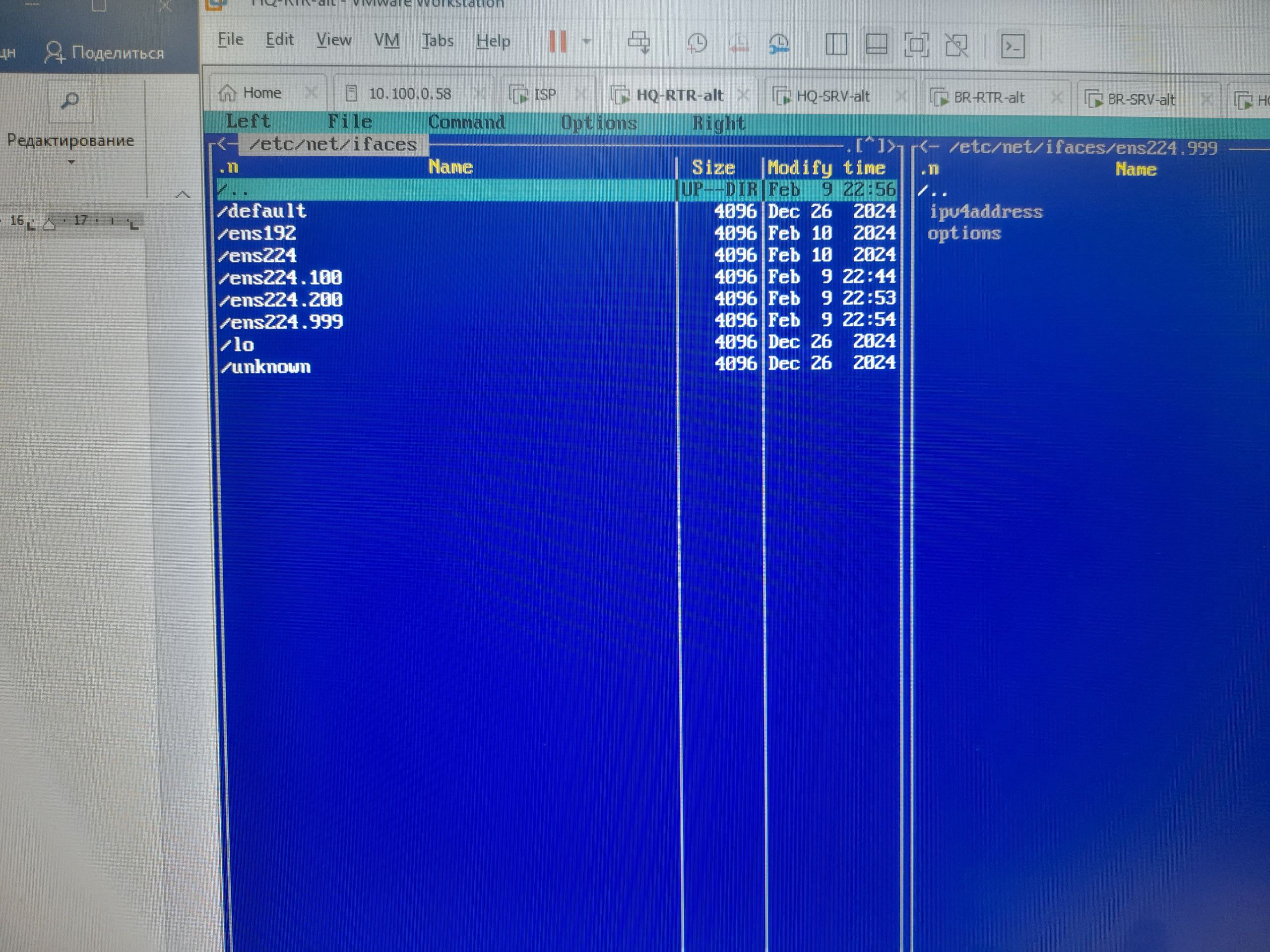
Делаем везде одной команой на isp надо установить tzdata командой apt-get install tzdata -y (после настройки интернета)

*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

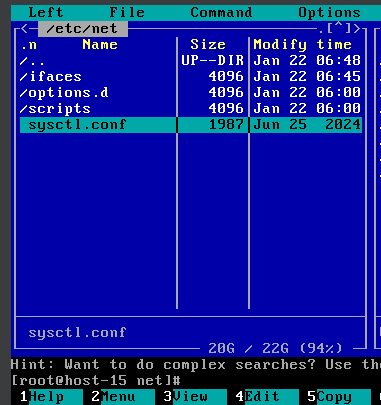
ONBOOT=yes

CONFIG\_IPV4=yes

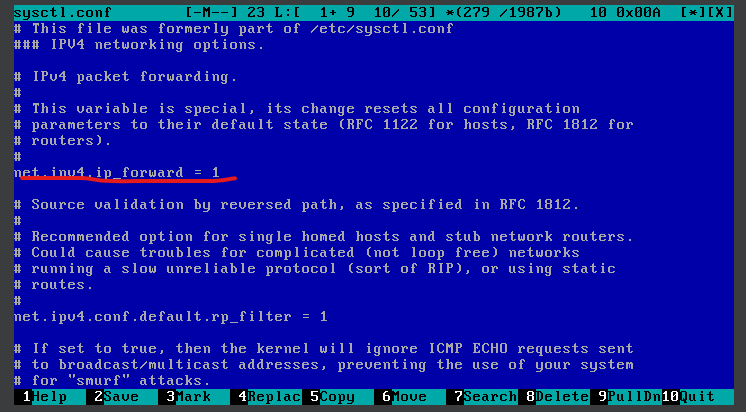
1. Создайте файл для задания IP-адреса:

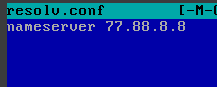
nano /etc/net/ifaces/<имя\_физического\_интерфейса>.hq.999/ipv4address

Укажите IP-адрес в формате ip/mask.



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

**



*systemctl restart network*

На hq-rtr

iptables -t nat -A POSTROUTING -o -j MASQUERADE

Сохраним правило:

iptables-save > /etc/sysconfig/iptables

Добавим iptables в автозагрузку:

systemctl enable –now iptables

**Создание пользователя на роутерах**

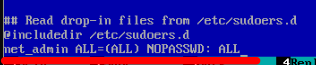
Теперь занимаемся пользователем на роутерах:

*adduser net\_admin*

*passwd net\_admin*

*P@$$word* (x2)

*mc /etc/sudoers*



*usermod -aG wheel net\_admin*

*logout*

*net\_admin*

*P@$$word*

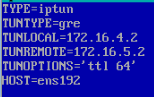
*sudo -i*

Смотрим:



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

*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****.*

**

***TUNLOCAL*** *ip-адрес той машины, на которой вы находитесь в данный момент. Это ip hq-rtr*

***TUNREMOTE*** *p-адрес соседа этой машины. Это ip br-rtr*

*Дальше всё очень просто – идём в файл ipv4address и пишем той внутреней сети*

*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:

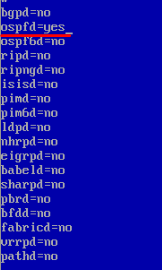
*ip -c --br a*

***Настройка динамической маршрутизации между офисами***

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:

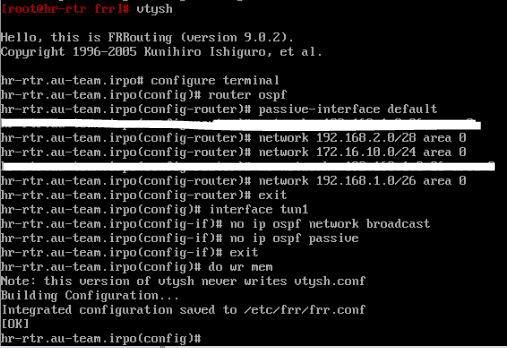


*перед как проверить перезагрузить systemctl restart frr*

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



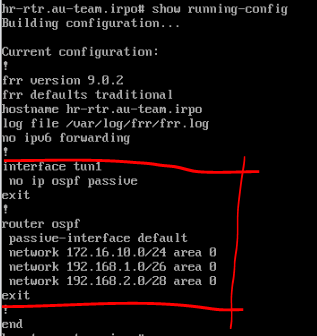
Дальше работаем с **frr**. Точно повторяем команды со скриншота по порядку. Работа с **frr** на скриншоте касается **HQ-RTR**:



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

*exit*

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

******

******

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:

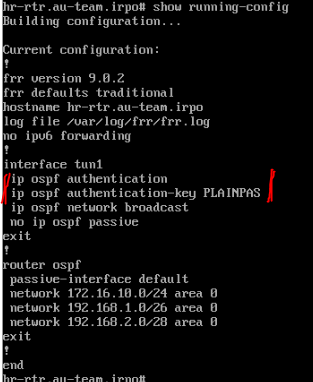
*exit*

*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*

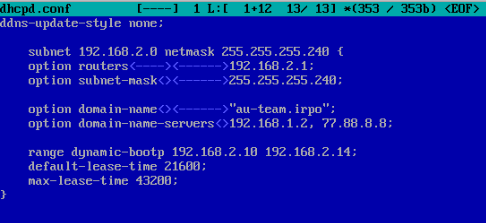
Включим автоматический запуск протокола при запуске системы:

*Systemctl enadle –now dhcpd*

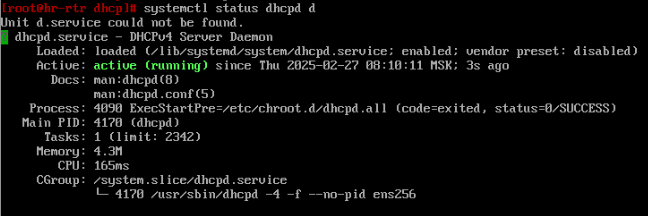
Собственно запускаем протокол:

*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:

**

Теперь проверяем статус службы специальной командой:

**

*Если вышла ошибка нужно добавить*

*/etc/sysconfig/dhcpd и добавить ens20*

*на hq-cli нужно /etc/net/ifaces/ens19.200/options поменять на dhcpd*

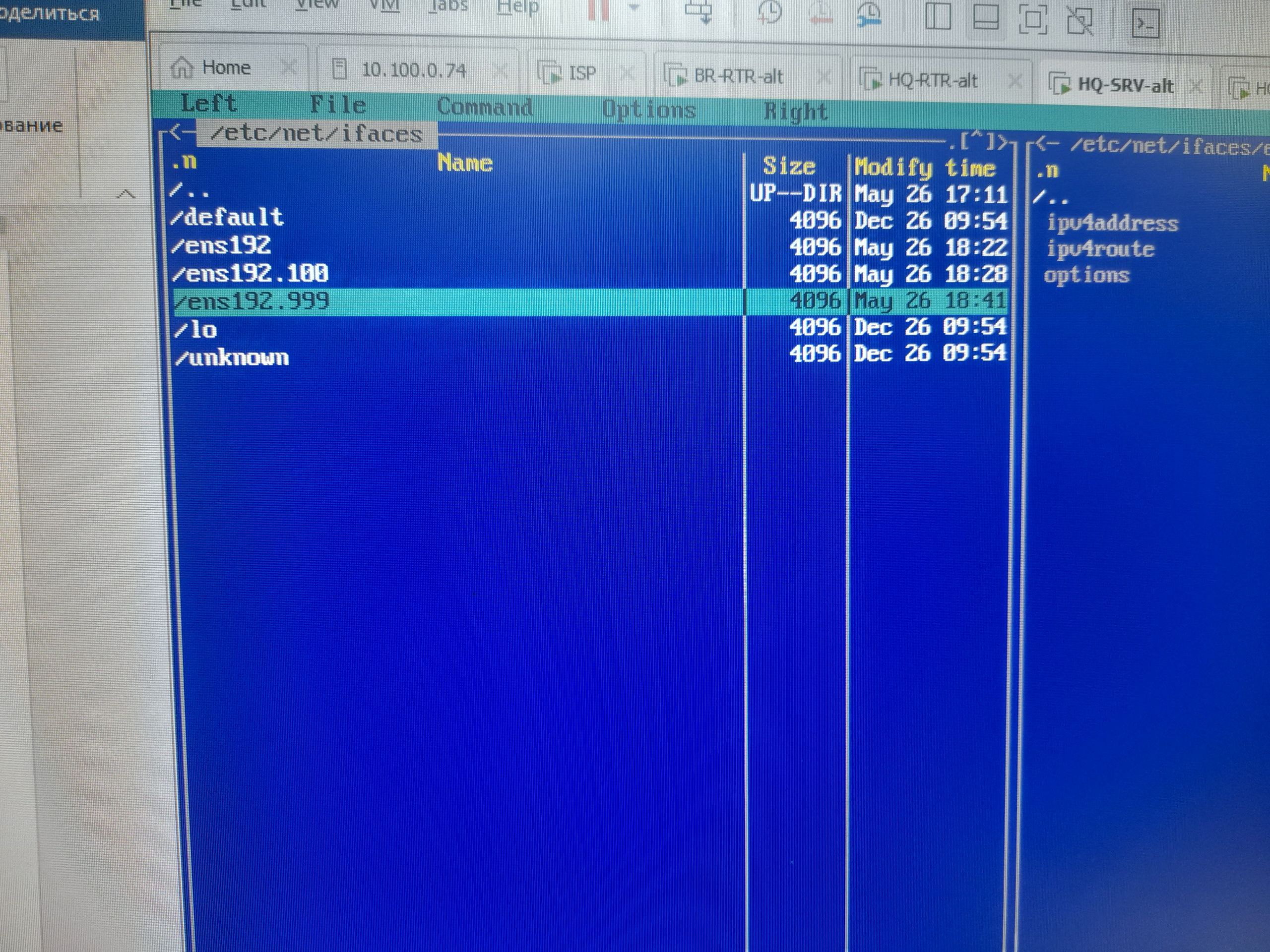
***Настройка hq-srv***

**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

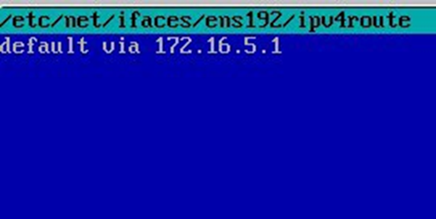
1. Создайте файл для задания IP-адреса:

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

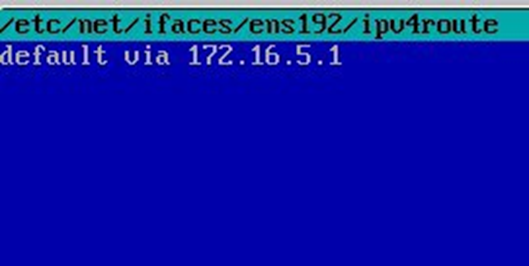
CONFIG\_IPV4=yes

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:

**

***Создание пользователя на серверах***

*скачать apt-get update&& apt-get install sudo -y*

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

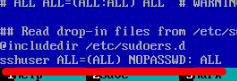
*adduser sshuser -u 1010*

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 )*

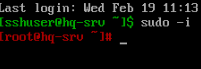
Теперь входим в новоиспеченного пользователя:

*sshuser*

*P@ssw0rd*

*sudo -i*

Лицезреть в итоге мы должны это:

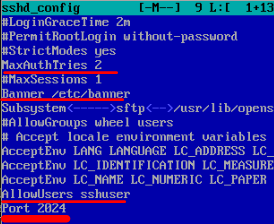
******

**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:

