

базовая
настройка
IP адресов

схемку сохран

- Это схема сети

У маршрутника BR-R 2 интерфейса:

- enp0s3
- enp0s8

HQ-R:

- enp0s3
- enp0s8
- enp0s9

ISP:

- enp0s3
- enp0s8
- enp0s9
- enp0s10

эти интерфейсы расположены закономерно, enp0s3 всегда смотрит вверх, enp0s8 всегда смотрит вниз.

Интерфейсы ISP:

enp0s3 – Смотрит в сторону интернет

enp0s8 – Смотрит в сторону HQ-R

enp0s9 – Смотрит в сторону BR-R

enp0s10 – Смотрит в сторону CLI

Интерфейсы HQ-R:

enp0s3 – Смотрит вверх

enp0s8 – Смотрит вниз

enp0s9 – Смотрит в сторону CLI (на него можно забить)

ВАЖНЫЕ КОМАНДЫ

- `systemctl restart/enable {название протокола}` – перезагрузить/включить протокол
- `systemctl status {название протокола}` – проверить состояние протокола (вкл/выкл)
- `control sudowheel enabled` - не знаю что это, но нужно прописывать при первом запуске каждого устройства (кроме CLI)

У серверов всего один интерфейс (по крайней мере который мы будем юзать) – enp0s3. Он всегда смотрит в сторону маршрутников (наверх)

Если какой то протокол не работает, либо выключен:

- systemctl restart/enable {название протокола} – перезагрузить/включить

- systemctl status {название протокола} – чекнуть его состояние

- Глава I

*При первом включении каждого устройства, всегда пишите команду
«control sudowheel enabled» - выдача рут прав*

ТАК ЖЕ НА КАЖДОМ УСТРОЙСТВЕ ДОБАВЛЯЕМ DNS:

- nano /etc/resolv.conf

nameserver 8.8.8.8

Настройка ISP:

- control sudowheel enabled
- ip -c a
- nano /etc/net/ifaces/enp0s3/options
в переменной «BOOTPROTO» меняем static на dhcp,
в переменной «SYSTEMD_BOOTPROTO» меняем static на dhcp4
- systemctl restart network
- ping 8.8.8.8 (проверяем доступность днс сервака)
- mkdir /etc/net/ifaces/enp0s8
- mkdir /etc/net/ifaces/enp0s9
- mkdir /etc/net/ifaces/enp0s10

создали значит папки для интерфейсов. В дальнейшем они нужны будут, запомните их путь.

Далее в КАЖДОЙ папке создаем файл «options»

- nano /etc/net/ifaces/enp0s8(9,10)/options

и в каждом файле «options» пишем следующие загогулины:

BOOTPROTO=static

TYPE=eth

NM_CONTROLLED=no

DISABLED=no

CONFIG_IPV4=yes

CONFIG_IPV6=yes

ДАЛЬШЕ АДРЕСАЦИЯ (ISP)! - можно не вписывать, по желанию

1 команда – айпи

2 команда - шлюз

- echo 192.168.0.165/30 > /etc/net/ifaces/enp0s8/ipv4address (1)
- echo default via 192.168.0.166 > /etc/net/ifaces/enp0s8/ipv4route(2)
- echo 192.168.0.161/30 > /etc/net/ifaces/enp0s9/ipv4address(1)
- echo default via 192.168.0.162 > /etc/net/ifaces/enp0s9/ipv4route(2)
- echo 192.168.0.249/30 > /etc/net/ifaces/enp0s10/ipv4address
- systemctl restart network

Исходя из видоса, далее хостнеймы:

- HQ-R:
hostnamectl set-hostname hq-r.hq.work;exec bash
- BR-R:
hostnamectl set-hostname br-r.branch.work;exec bash
- HQ-SRV:
hostnamectl set-hostname hq-srv.hq.work;exec bash
- BR-SRV:
hostnamectl set-hostname br-srv.branch.work;exec bash

Маршрутнеки:

На интерфейсе «**enp0s3**» по дефолту задница какая то, отсутствует строка «**CONFIG_IPV6=yes**»

- nano /etc/net/ifaces/enp0s3/options

встречать нас будут строки

BOOTPROTO=static

TYPE=eth

NM_CONTROLLED=no

DISABLED=no

CONFIG_IPV4=yes

CONFIG_IPV6=yes – (этой строки не будет наверное)

DISABLED=no

NM_CONTROLLED=no

SYSTEMD_CONTROLLED=no

Добавляем строчку «CONFIG_IPV6=yes» на ее законное место!!!!

ЭТО НЕОБХОДИМО СДЕЛАТЬ ДЛЯ ВСЕХ МАРШРУТНИКОВ (enp0s3 интерфейс)

ДЛЯ (HQ-R)!

- mkdir /etc/net/ifaces/enp0s8
- mkdir /etc/net/iface---s/enp0s9
- nano /etc/net/ifaces/enp0s(8,9)/options

и в файле «options» пишем следующие загогулины:

```
BOOTPROTO=static  
TYPE=eth  
NM_CONTROLLED=no  
DISABLED=no  
CONFIG_IPV4=yes  
CONFIG_IPV6=yes
```

ДАЛЬШЕ АДРЕСАЦИЯ (HQ-R)!

- echo 192.168.0.166/30 > /etc/net/ifaces/enp0s3/ipv4address
- echo default via 192.168.0.165 > /etc/net/ifaces/enp0s3/ipv4route

- echo 192.168.0.1/25 > /etc/net/ifaces/enp0s8/ipv4address
- echo default via 192.168.0.40 > /etc/net/ifaces/enp0s8/ipv4route

И ЕЩЕ АДРЕСАЦИЯ (BR-R)!

но сперва V

ДЛЯ (BR-R)!

- mkdir /etc/net/ifaces/enp0s8
- nano /etc/net/ifaces/enp0s8/options

и в файле «options» пишем следующие загогулины:

```
BOOTPROTO=static  
TYPE=eth  
NM_CONTROLLED=no  
DISABLED=no  
CONFIG_IPV4=yes  
CONFIG_IPV6=yes
```

- echo 192.168.0.162/30 > /etc/net/ifaces/enp0s3/ipv4address
- echo default via 192.168.0.161 > /etc/net/ifaces/enp0s3/ipv4route

- echo 192.168.0.129/27 > /etc/net/ifaces/enp0s8/ipv4address
- echo default via 192.168.0.140 > /etc/net/ifaces/enp0s8/ipv4route

А ТЕПЕРЬ НАСТРОИМ СЕРВЕРЫЫЫЫЫ

Не забываем про хостнеймы:

- HQ-SRV:
hostnamectl set-hostname hq-srv.hq.work;exec bash
- BR-SRV:
hostnamectl set-hostname br-srv.branch.work;exec bash

На интерфейсе «**enp0s3**» по дефолту задница какая то, отсутствует строка «**CONFIG_IPV6=yes**» - ОНА ЕСТЬ И НА СЕРВЕРЕ! ВОТ ЕТО ДА

- nano /etc/net/ifaces/enp0s3/options

встречать нас будут строки

```
BOOTPROTO=static
TYPE=eth
NM_CONTROLLED=no
DISABLED=no
CONFIG_IPV4=yes
CONFIG_IPV6=yes – (этой строки не будет наверное)
DISABLED=no
NM_CONTROLLED=no
SYSTEMD_CONTROLLED=no
```

Добавляем строчку «**CONFIG_IPV6=yes**» на ее законное место!!!! – **ЭТО ДЕЛАТЬ НА ОБОИХ СЕРВЕРАХ**

Маршрутизация на HQ-SRV:

- echo 192.168.0.40/25 > /etc/net/ifaces/enp0s3/ipv4address
- echo default via 192.168.0.1 > /etc/net/ifaces/enp0s3/ipv4route
- systemctl restart network

Маршрутизация на BR-SRV:

- echo 192.168.0.140/27 > /etc/net/ifaces/enp0s3/ipv4address
- echo default via 192.168.0.129 > /etc/net/ifaces/enp0s3/ipv4route
- systemctl restart network

ДАЛЕЕ ISP (nftables):

Щас мы настроим доступ в интернет.

- apt-get update
- apt-get install -y nftables

- nano /etc/nftables/isp.nft

В этом файле необходимо прописать следующее:

```
table inet my_nat {  
  
    chain my_masquerade {  
        type nat hook postrouting priority srcnat;  
        oifname "enp0s3" masquerade  
    }  
  
}
```

Дальше идем:

- nano /etc/sysconfig/nftables.conf

И туда пишем:

```
include  
include "/etc/nftables/isp.nft"
```

- systemctl enable --now nftables

Далее на маршрутиках (**HQ-R, BR-R, ISP**) необходимо включить пересылку пакетов:

- nano /etc/net/sysctl.conf

в строке «net.ipv4.ip_forward = 0» **нолик** меняем на **1**

- reboot

УСТАНОВКА FIREWALL НА ISP:

- apt-get update
- apt-get install -y firewall
- systemctl enable firewall
- firewall-cmd --permanent --zone=public --add-interface=enp0s8
- firewall-cmd --permanent --zone=public --add-interface=enp0s9
- firewall-cmd --permanent --zone=public --add-masquerade
- reboot

УСТАНОВКА NFTABLE НА (HQ-R & BR-R)

- apt-get update
- apt-get install nftables
- nft flush ruleset

- nft add table nat
- nft -- add chain nat prerouting { type nat hook prerouting priority -100 \; }
- nft -- add chain nat postrouting { type nat hook postrouting priority 100 \; }
- nft add rule nat postrouting oifname "enp0s3" masquerade
- echo "flush ruleset" >> /etc/nftables/nftables.nft
- nft list ruleset >> /etc/nftables/nftables.nft
- systemctl restart nftables

НАСТРОЙКА EIGRP

Глава 2.

Перед этим надо поставить пакет «FRR» на все маршрутники (включая ISP)

ЭТО НАДО СДЕЛАТЬ НА ВСЕХ 3х РОУТЕРАХ – установка FRR

- apt-get update
- apt-get install -y frr

теперь настройка frr

- nano /etc/frr/daemons

в ЭТОМ текстовике ищем «eigrpd=no» и no меняем на yes

- systemctl enable --now frr.service

вход в frr:

- vtysh

- ISP -

EIGRP настройка

- vtysh
- configure terminal
- router eigrp 1
- network 192.168.0.164/30
- network 192.168.0.160/30
- sh ip route eigrp
- do wr
- ex

- BR-R -

EIGRP настройка

- vtysh
- configure terminal
- router eigrp 1
- network 192.168.0.160/30
- network 192.168.0.128/27

- sh ip route eigrp
- do wr
- ex

- HQ-R -

EIGRP настройка

- vtysh
- configure terminal
- router eigrp 1
- network 192.168.0.164/30
- network 192.168.0.0/25
- sh ip route eigrp
- do wr
- ex

- ВАЖНО -

Перед проверкой EIGRP, проверьте **nftables**

- systemctl status nftables.service
- **sh ip route eigrp** – посмотреть что получилось в еигрп

УСТАНОВКА DHCP Сервера –

HQ-R

- apt-get -y install dhcp-server
- nano /etc/sysconfig/dhcpd

Открывается конфиг, там в следующем параметре указываем enp0s8

- DHCPDARGS=enp0s8

Потом чето копируем и редактируем

- cp /etc/dhcp/dhcpd.conf.sample /etc/dhcp/dhcpd.conf.sample
/etc/dhcp/dchpd.conf
- nano /etc/dhcp/dhcpd.conf

```
idns-update-style none;

subnet 192.168.0.0 netmask 255.255.255.128 {
    option routers          192.168.0.1;
    option subnet-mask      255.255.255.128;

    option domain-name-servers 8.8.8.8;

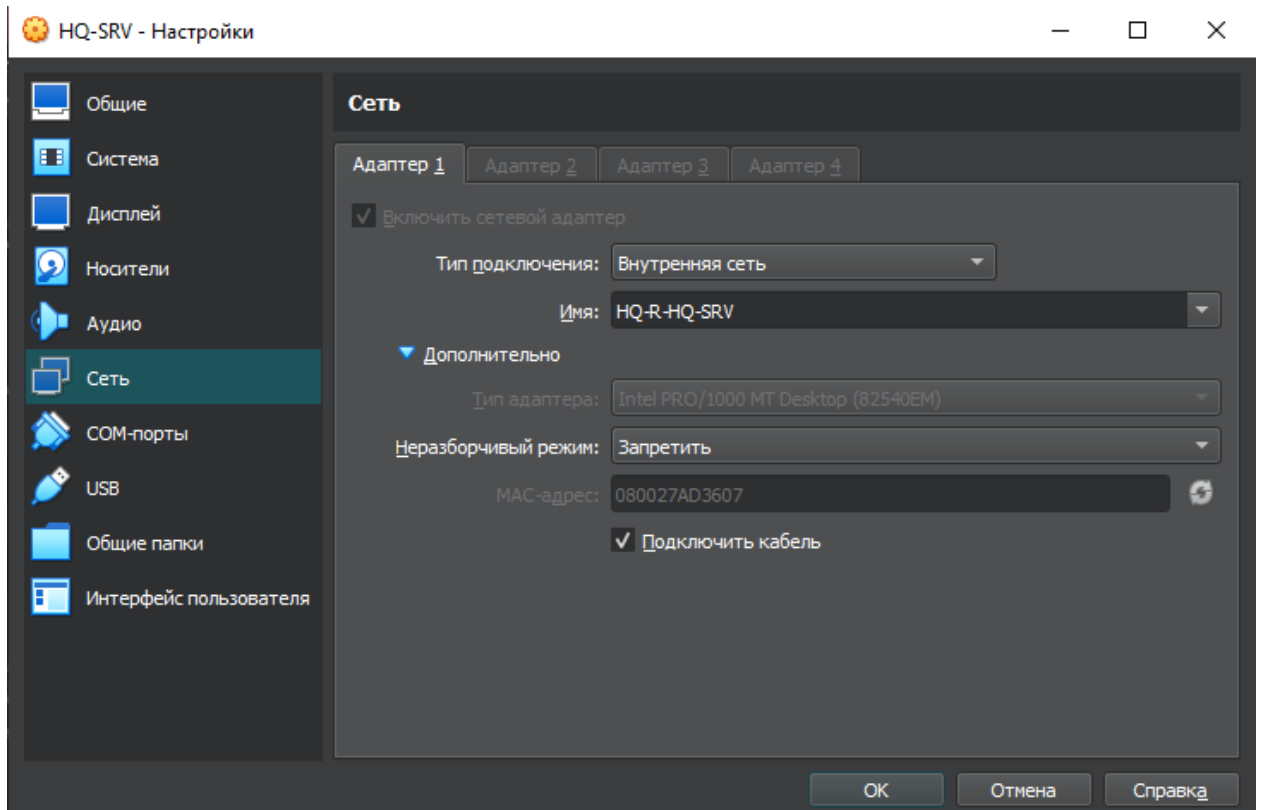
    range dynamic-bootp 192.168.0.2 192.168.0.126;
    default-lease-time 21600;
    max-lease-time 43200;
}

host HQ-SRV
{
    hardware ethernet 08:00:27:e3:cf:9a;
    fixed-address 192.168.0.48;
}

[root@hq-r ~]#
[root@hq-r ~]# systemctl restart dhcpd
[root@hq-r ~]# systemctl restart dhcpd
```

- + Здесь просто меняем маску (на 255.255.255.128). красные квадраты.
- + 3 строчки про домен просто сносим и пишем то что в зеленом квадрате.
- + в голубом квадрате меняем адрес на тот который на скрине.
- + желтый квадрат – просто все подчистую перепишите. **НО**

Не отсылка на
Укроену →



Необходимо открыть настройки HQ-SRV и зайти на 1 адаптер, нажать на дополнительно и посмотреть MAC-Адрес. Он может быть у всех разный.

- И В РОЗОВОМ КВАДРАТЕ ПИШИТЕ МАК АДРЕС СВОЕГО АДАПТЕРА!

Дальше просто ребут dhcpd:

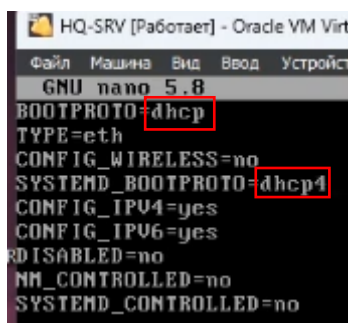
- `systemctl restart dhcpd`

После этой команды чего нето будет, поэтому просто пишите это:

- `chkconfig dhcpd on`
- `service dhcpd start`

HQ-SRV

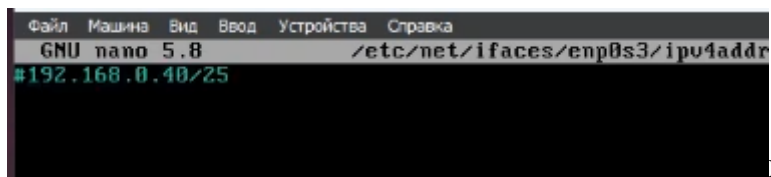
- `nano /etc/net/ifaces/enp0s3/options`



тут будет статика, но меняем на DHCP

И так как мы меняем здесь статику на автоматику, то нужно закомментировать адрес на интерфейсе

- `nano /etc/net/ifaces/enp0s3/ipv4address`



```
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 5.8  /etc/net/ifaces/enp0s3/ipv4addr
#192.168.0.40/25
```

ну тут просто # добавляем

И ребутиим сеть

- `systemctl restart network`

Конфигурация пользователя (на примере одной машины)

HQ-SRV

Настройте локальные учётные записи на всех устройствах в соответствии с таблицей.

Учётная запись	Пароль	Примечание
Admin	P@ssw0rd	CLI, HQ-SRV, HQ-R
Branch admin	P@ssw0rd	BR-SRV, BR-R
Network admin	P@ssw0rd	HQ-R, BR-R, HQ-SRV

Вот это нам надо наверн

На устройстве HQ-SRV:

- useradd admin
- passwd admin
- {пароль}
- {повторить пароль}
- useradd network_admin
- passwd network_admin
- {пароль}
- {повторить пароль}

На HQ-R вводим команду ниже (измеряем пропускную способность)

- apt-get -y install iperf3

И нам потребуется ISP в роли сервера сие деяний

Настройка firewall для iperf3 (ISP)

- **firewall-end --permanent --add port-5201/tcp**

так-же необходимо добавить интерфейсы в паблик на ISP-командой:

- **firewall-cmd --permanent --zone=public --add-interface=enp0s8**
- **firewall-cmd --permanent --zone=public --add-interface=enp0s9**

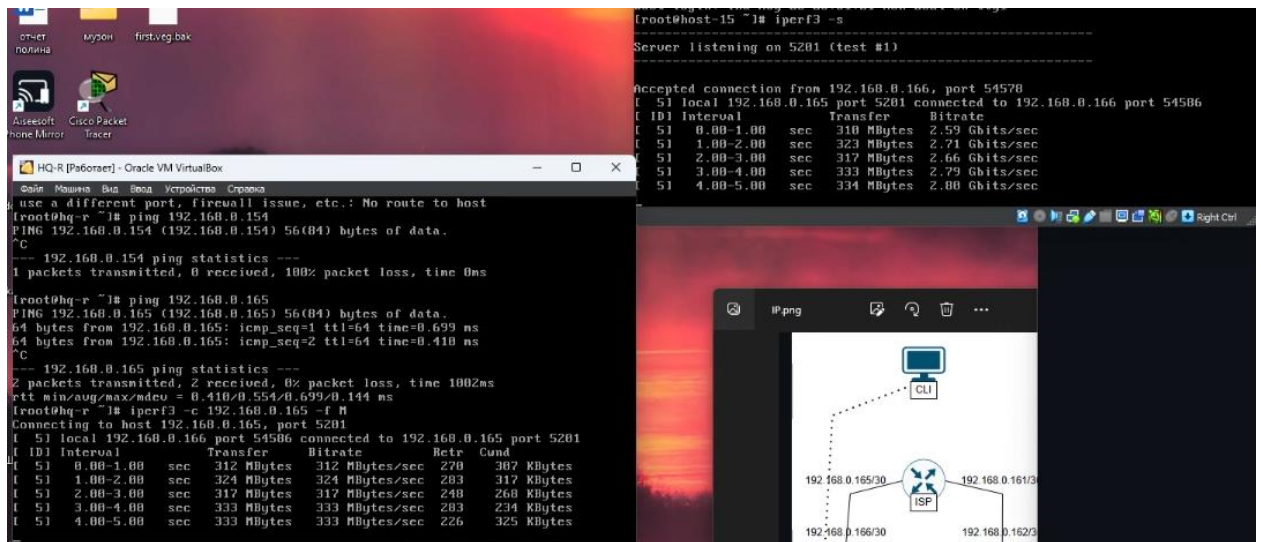
а дальше тупа ребут (ISP)

- reboot

МОЛОДЦЫ! Настроили iperf3. Теперь можно заценить как это работает:

На (ISP):

- iperf3 -s



И вот такая картена у нас будет

НАСТРОЙКА БЭКАП

ISP – сервер

55413/tcp

55414/tcp

55415/tcp

55423/tcp

понадобится

HQ & BR R – клиенты (маршрутники)

Щас мы настраиваем ISP

Сперва установим бэкап утилиту

- apt-get install -y urbackup-server

Добавляем его в автозагрузку

- systemctl enable --now urbackup-server

Создаем директорию для хранения копий на сервере

- mkdir /mnt/backups

Даем права роутерам и утилите на папку /mnt/backups

- `chown -R urbackup:urbackup /mnt/backups`

Права на папку всем группам юзеров

- `chmod 777 /mnt/backups`

И теперь порты ебашим

- `firewall-cmd --permanent --add-port=55413/tcp`
- `firewall-cmd --permanent --add-port=55414/tcp`
- `firewall-cmd --permanent --add-port=55415/tcp`
- `firewall-cmd --permanent --add-port=35623/tcp`
- `firewall-cmd --permanent --add-port=35623/udp`

HQ & BR – R

Установка бекап клиента на роутеры

- `apt-get install urbackup-client`
- `systemctl enable --now urbackup-client`

ЗАПУСКАЕМ **CLI (ВИРТУАЛКА)** (сперва enter при первом запуске, а при загрузке жмаем английскую E)

```
setparams 'ALT Workstation 10,2'

savedefault
load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='hd0,msdos2'
if [ x$feature_platform_search_hint = xy ]: then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos2\
--hint-efi=hd0,msdos2 --hint-baremetal=ahci0,msdos2 cfe61890-87c5-4a64\
-9e7c-1dc42a238f0a
else
  search --no-floppy --fs-uuid --set=root cfe61890-87c5-4a64-9e7\
c-1dc42a238f0a
fi
linux      /boot/vmlinuz-un-def root=UUID=cfe61890-87c5-4a64-9\
e7c-1dc42a238f0a ro resume=/dev/disk/by-uuid/e64bab1f-bb78-412d-b240-4b\
898eb9ea78 panic=30 quiet loglevel=3 splash init=/bin/bash_
initrd     /boot/initrd-un-def.img
```

Поддерживается несколько Emacs-подобных команд редактирования на экране. Есть списки дополнений по TAB. Нажмите Ctrl-x или F10 для загрузки, Ctrl-c или F2 для получения командной строки или ESC для отмены изменений и возврата в меню GRUB.

Выделенного красного текста после того как вы зажмали E – НЕ БУДЕТ! Его надо дописать.

- После splash пишем «init=/bin/bash»

И дальше просто ctrl+x

Потом загрузится консоль, туда пишем:

- mount / -o rw,remount

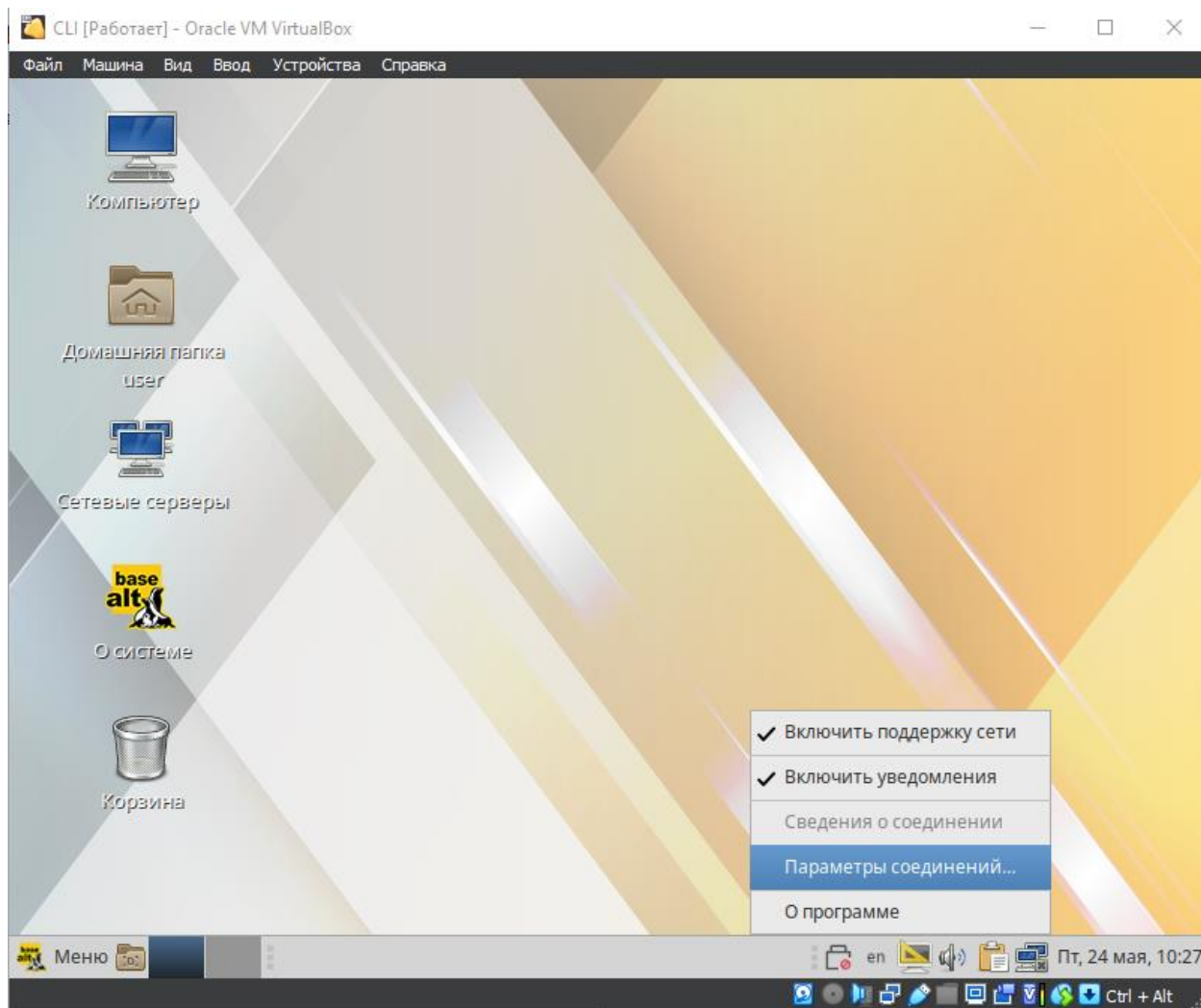
Далее меняем пароль. Первая команда для root, вторая для пользователя

- passwd
- {пароль}
- passwd user
- {пароль}

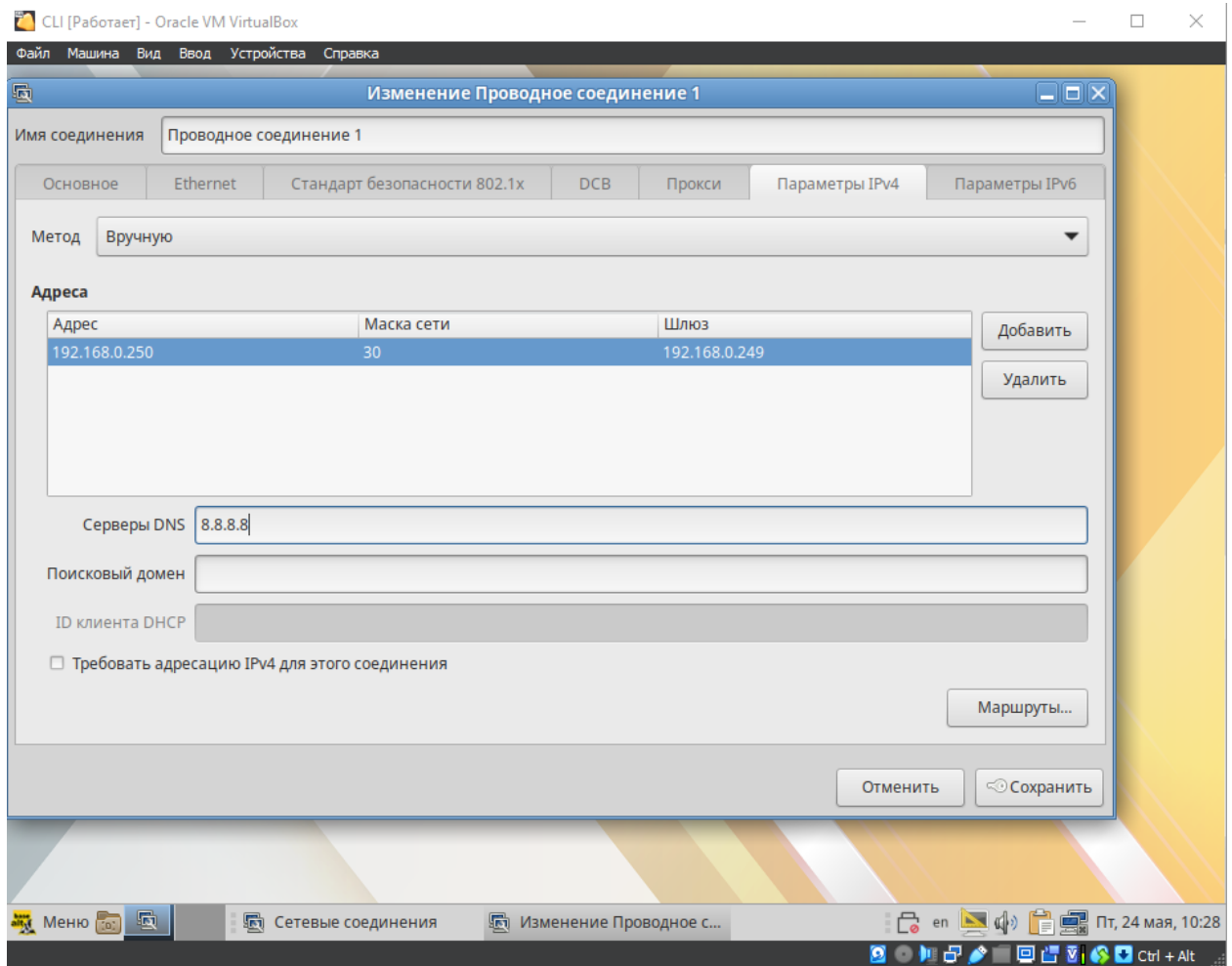
Потом выключаем и включаем виртуалку, букву E не жмать, там уже вводите пароль от пользователя.

НАСТРОЙКА ДОСТУПА CLI К ISP

Тычем на интернат(ПКМ) и выбираем его



Настройка первого адаптера:



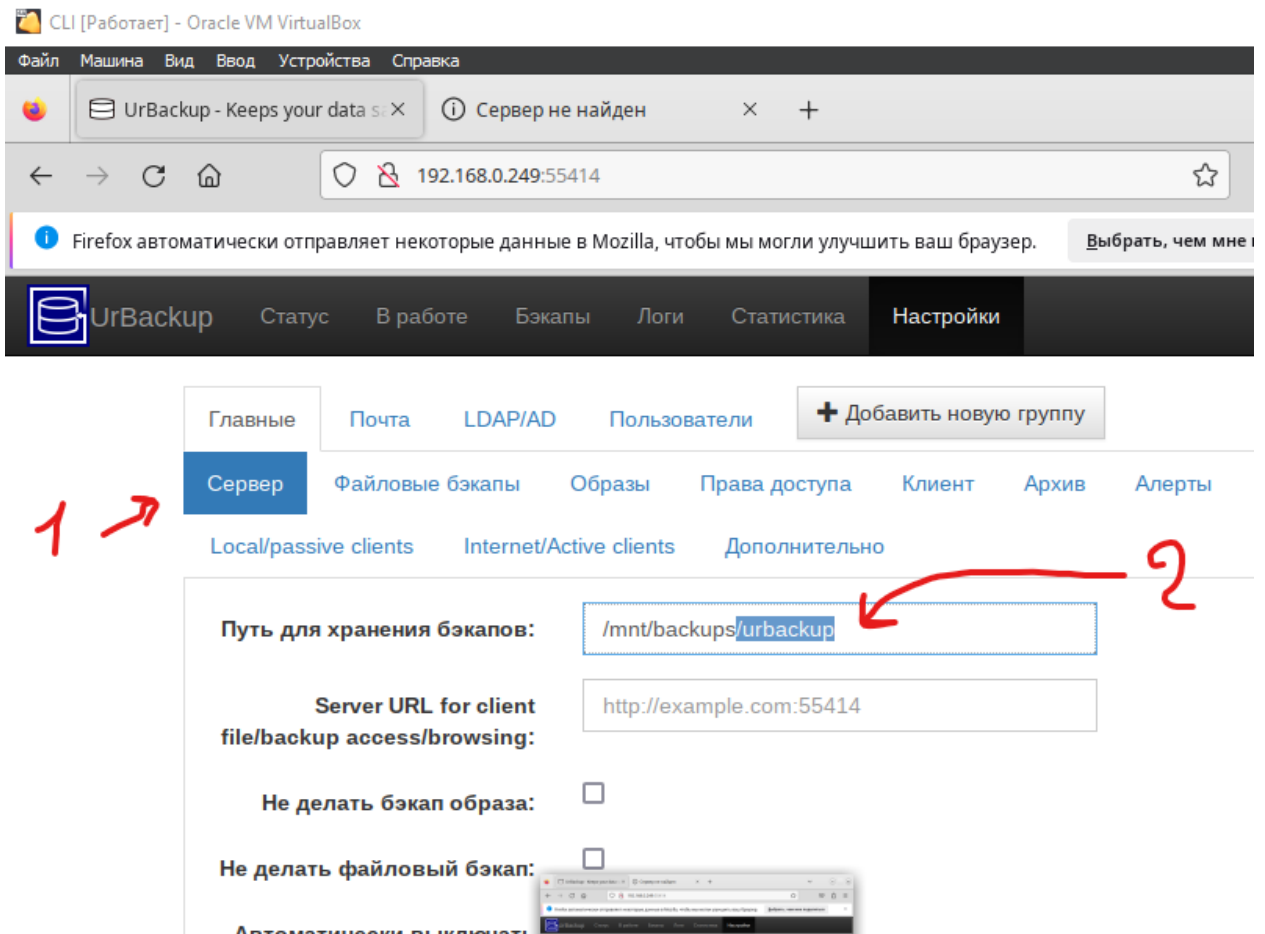
Вроде всё.

После того как настроили и установили **urbackup-server**

Перезапустите ISP (-reboot)

И переходите по адресу 192.168.0.249:55414

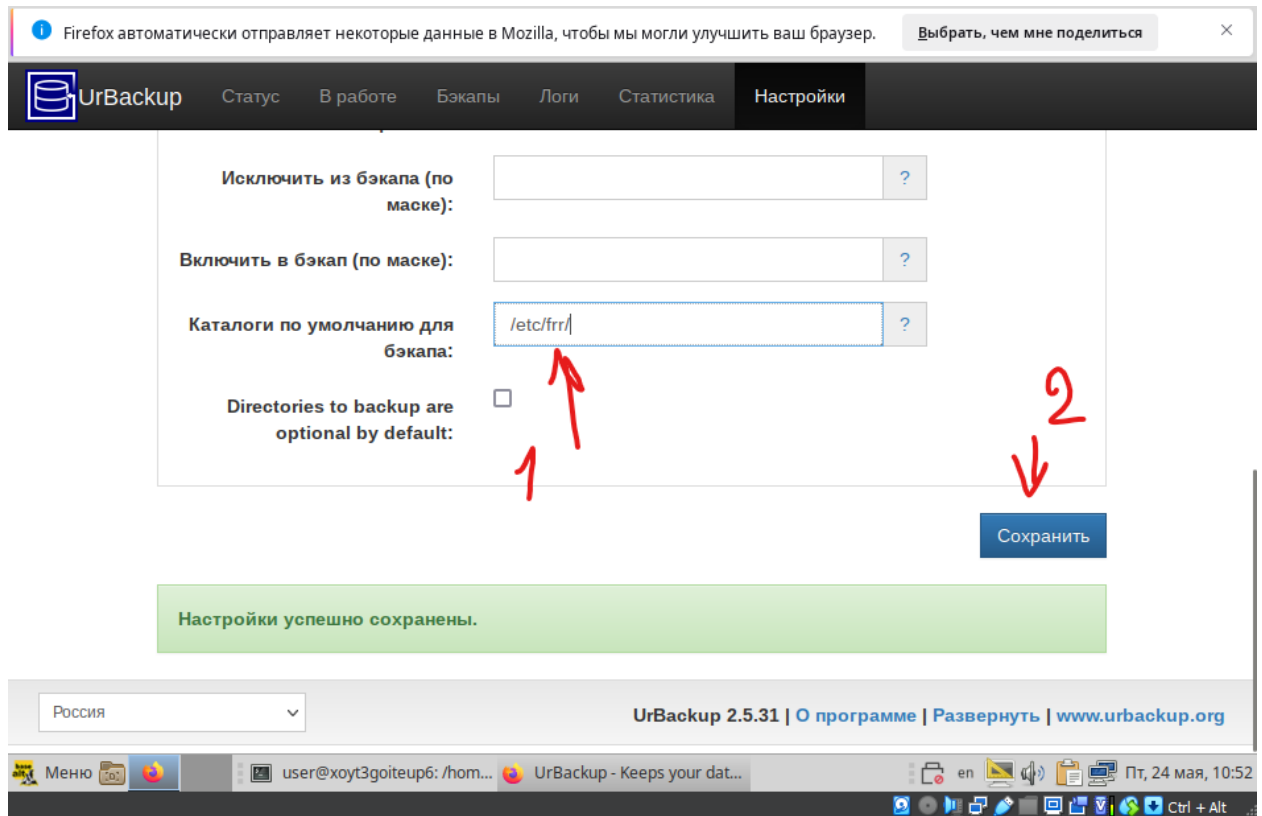
ОБЯЗАТЕЛЬНО ЭТОТ ПОРТ



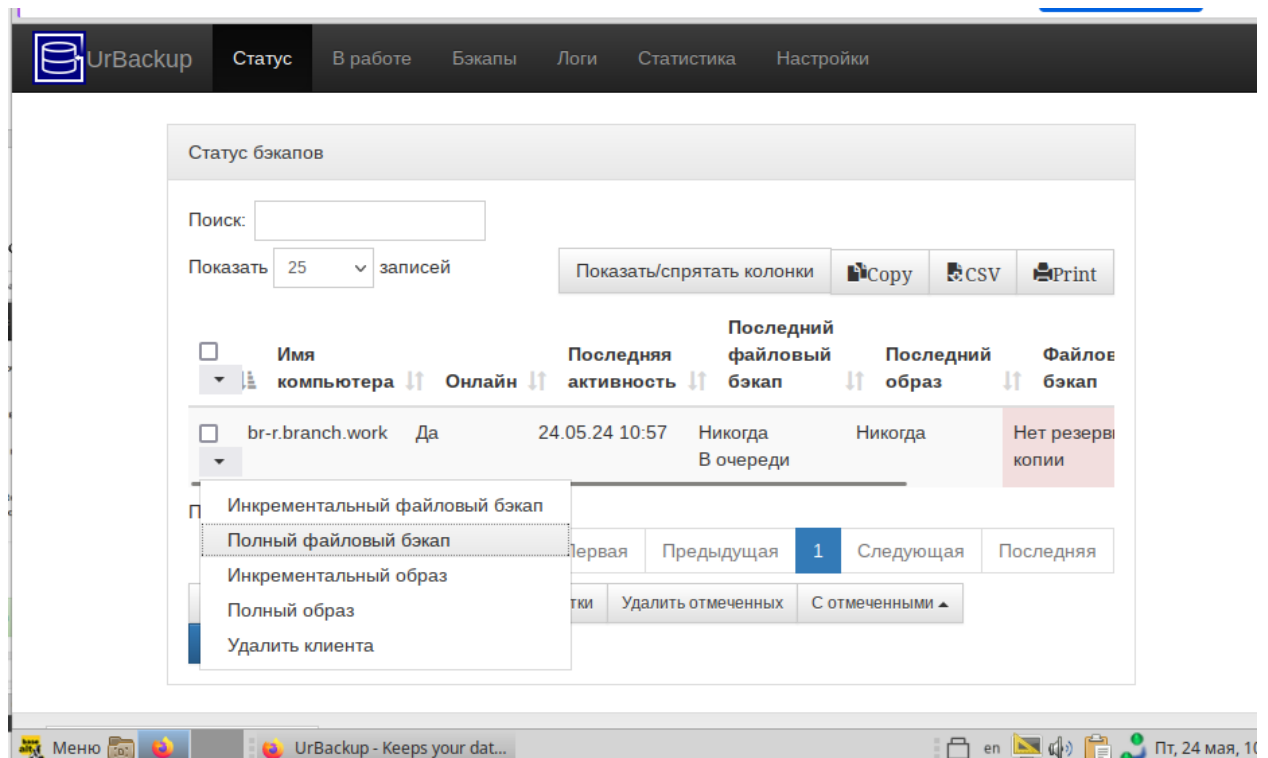
Перешли по адресу, заходим в раздел «сервер», меняем путь сохранения бэков, стирая «/urbackup» оставляя все остальное

И СОХРАНЯЕМ!

В разделе «Файловые Бэкапы» пишем это путь (/etc/frr)



Ну и все ебекапимся блин нафиг



В работе

Имя компьютера	Действие	Подробности	Прогресс	Расчетное время выполнения	Скорость
br-r.branch.work	Полный файловый бэкап	-	<div>0%</div> <div>0 bytes / 4.36 KB</div>	-	-

Еще может быть шняга такая, что в разделе «статус» ток один роутер, а может их не быть вообще. Для этого надо на маршрутники накатить urbackup-client, либо его включить/перезагрузить, либо перезагрузить вообще сам маршрутник. Команды необходимые расписал ранее

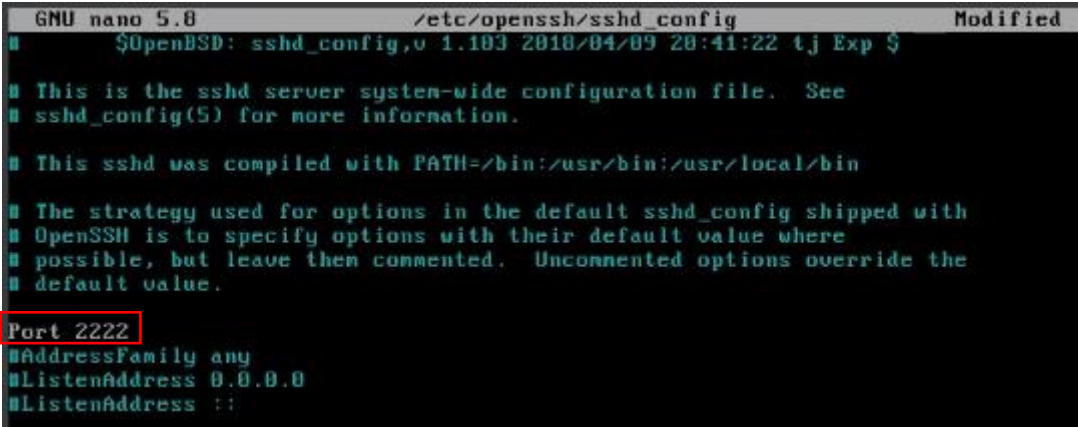
НАСТРОЙКА SSH на HQ-SRV

Настраивать будем на сервере HQ-SRV, порт 2222 (четыре двойки)

- apt-get update
- apt-get install -y openssh-server
- systemctl enable --now sshd

короче обновили пакеты, накатили ссх и врубили его.

- nano /etc/openssh/sshd_config



```
GNU nano 5.0 /etc/openssh/sshd_config Modified
$OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/bin:/usr/bin:/usr/local/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

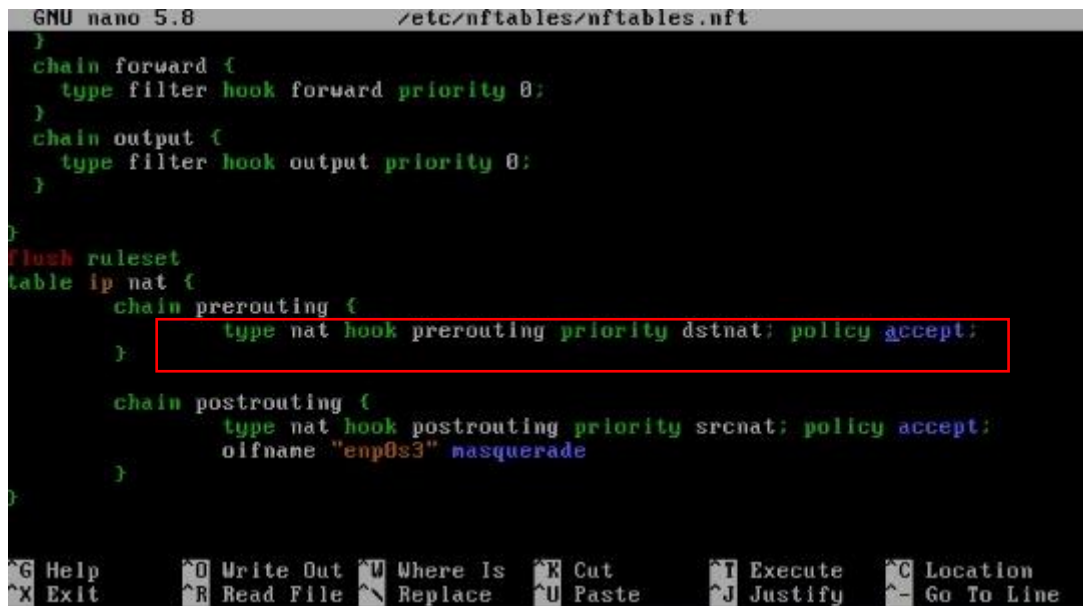
Здесь короче будет порт 22 и он будет закомментирован. Убираем хештег и добавляем еще 2 двойки

А потом прост перезагружаем ссх

- systemctl restart sshd.service

Дальше настроим маршрутник HQ-R

- nano /etc/nftables/nftables.nft



```
GNU nano 5.8 /etc/nftables/nftables.nft
}
chain forward {
    type filter hook forward priority 0;
}
chain output {
    type filter hook output priority 0;
}
}
flush ruleset
table ip nat {
    chain prerouting {
        type nat hook prerouting priority dstnat; policy accept;
    }

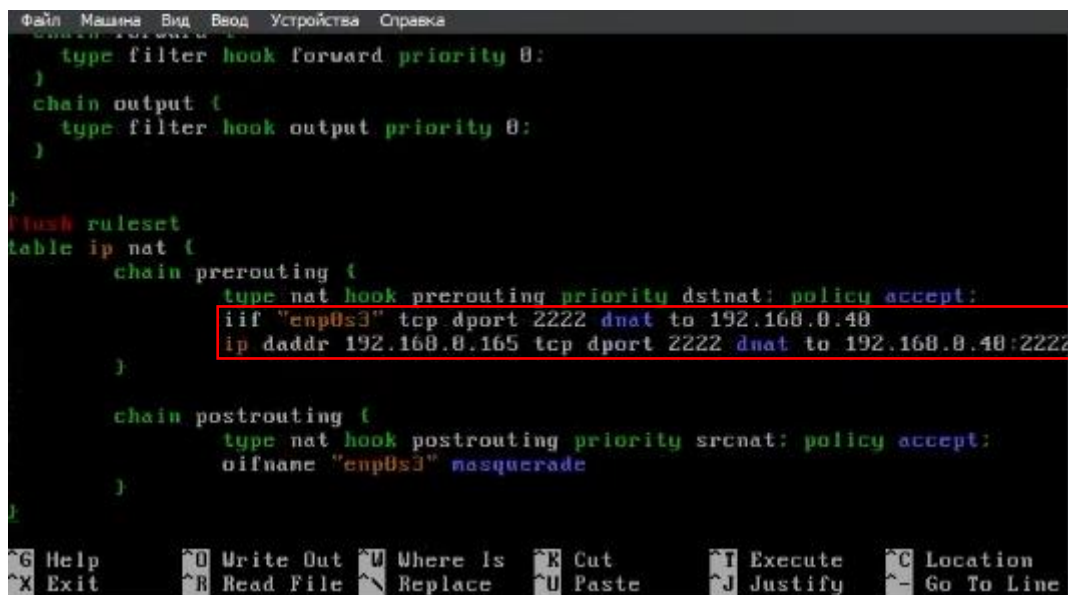
    chain postrouting {
        type nat hook postrouting priority srcnat; policy accept;
        oifname "enp0s3" masquerade
    }
}
}

^G Help      ^O Write Out ^U Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File ^\ Replace    ^U Paste       ^J Justify    ^_ Go To Line
```

При входе будет такая картина, но нам необходимо добавить еще строчки:

if "enp0s3" tcp dport 2222 dnat to 192.168.0.40

ip daddr 192.168.0.165 tcp dport 2222 dnat to 192.168.0.40:2222



```
Файл  Машинка Вид  Ввод  Устройства  Справка
chain forward {
    type filter hook forward priority 0;
}
chain output {
    type filter hook output priority 0;
}
}
flush ruleset
table ip nat {
    chain prerouting {
        type nat hook prerouting priority dstnat; policy accept;
        iif "enp0s3" tcp dport 2222 dnat to 192.168.0.40
        ip daddr 192.168.0.165 tcp dport 2222 dnat to 192.168.0.40:2222
    }

    chain postrouting {
        type nat hook postrouting priority srcnat; policy accept;
        oifname "enp0s3" masquerade
    }
}
}

^G Help      ^O Write Out ^U Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File ^\ Replace    ^U Paste       ^J Justify    ^_ Go To Line
```

Вот сюда добавляем, у чела iif написано, но я не уверен что это правильно

Дальше пишем команду

- reboot

и с маршрутника BR-R пробуем подключиться к HQ-R:

- ssh admin@192.168.0.166 -p 2222

а пароль вроде toor