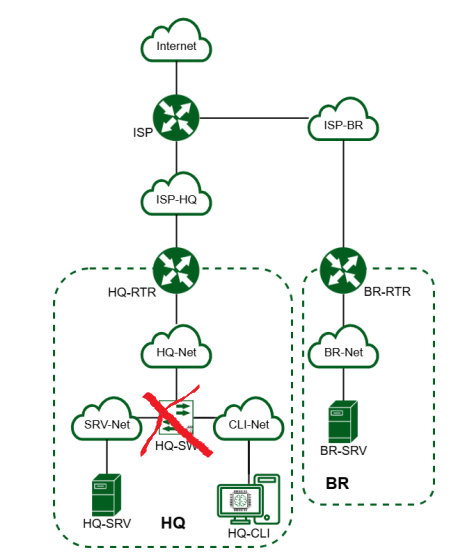
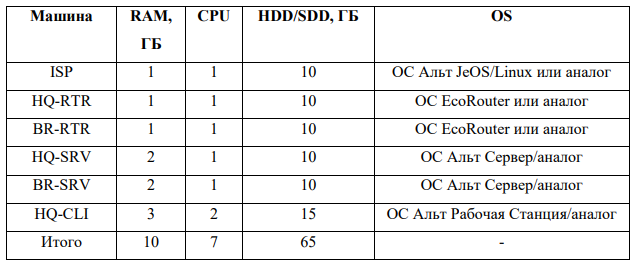
Гайд





|  |  |  |  |
| --- | --- | --- | --- |
| Устройства | Адаптер/интерфейс | Соединение | IP-адреса |
| ISP | 1-enp0s3 | NAT |  |
| 2-enp0s8 | BR-RTR-ISP | 172.16.5.1/28 |
| 3-enp0s9 | HQ-RTR-ISP | 172.16.4.1/28 |
| BR-RTR | 1-enp0s3 | NAT |  |
| 2-enp0s8 | BR-RTR-ISP | 172.16.5.2/28 |
| 3-enp0s9 | BR-RTR-BR-SRV | 192.168.3.1/27 |
| BR-SRV | 1-enp0s3 | NAT |  |
| 2-enp0s8 | BR-RTR-BR-SRV | 192.168.3.2/27 |
| HQ-RTR | 3-enp0s9 | NAT |  |
| 2-enp0s8 | HQ-RTR-ISP | 172.16.4.2/28 |
| 3-enp0s9 | HQ-RTR-HQ-SRV | 192.168.1.1/26 |
| 4-enp0s10 | HQ-RTR-CLI | 192.168.4.1/24 |
| HQ-SRV | 1-enp0s3 | NAT |  |
| 2-enp0s8 | HQ-RTR-HQ-SRV | 192.168.1.2/26 |
| HQ-CLI | 1-enp0s3 | NAT |  |
| 2-enp0s8 | HQ-RTR-HQ-CLI(DHCP) | 192.168.4.10/24 |

Настройки которые нужно провести(без свича и vlan)

 **Произведите базовую настройку устройств**:

* Настройте имена устройств согласно топологии, используя полное доменное имя.
* Настройте IPv4 на всех устройствах.
* Используйте IP-адреса из приватного диапазона согласно RFC1918.
* Сведения об адресах занесите в отчёт.

 **Настройка ISP**:

* Настройте адресацию на интерфейсах:
  + Интерфейс, подключенный к провайдеру, получает адрес по DHCP.
  + Интерфейсы для HQ-RTR и BR-RTR используют сети 172.16.4.0/28 и 172.16.5.0/28 соответственно.
* Настройте маршруты по умолчанию там, где это необходимо.
* Реализуйте динамическую NAT для доступа к Интернету на маршрутизаторе ISP.

 **Создание локальных учетных записей**:

* Создайте пользователя sshuser на HQ-SRV и BR-SRV с:
  + Паролем P@ssw0rd.
  + UID 1010.
  + Правами без запроса пароля.
* Создайте пользователя net\_admin на HQ-RTR и BR-RTR с:
  + Паролем P@$$word.
  + Максимальными привилегиями Alt Linux.

 **Настройка безопасного удалённого доступа**:

* Разрешите доступ по порту 2024.
* Ограничьте попытки входа до двух.
* Настройте баннер: «Authorized access only».
* Позвольте подключения только пользователю sshuser.

 **Конфигурация IP-туннеля между HQ и BR**:

* Выберите технологию GRE или IP-in-IP.
* Включите сведения о туннеле в отчёт.

 **Обеспечение динамической маршрутизации**:

* Используйте link-state протокол (например, OSPF или IS-IS).
* Включите протокол только на интерфейсах IP-туннеля.
* Обеспечьте парольную защиту маршрутизационного протокола.
* Обменивайтесь маршрутами только между HQ-RTR и BR-RTR.

 **Настройка динамической NAT**:

* Реализуйте трансляцию адресов для всех устройств обоих офисов, чтобы обеспечить доступ к Интернету.

 **Настройка DHCP**:

* Организуйте DHCP на HQ-RTR для офиса HQ:
  + Исключите из выдачи адрес маршрутизатора.
  + Укажите адрес сервера HQ-SRV как DNS-сервер.
  + Установите шлюз по умолчанию как HQ-RTR.
  + Добавьте DNS-суффикс au-team.irpo.

 **Настройка DNS**:

* Настройте HQ-SRV как DNS-сервер для офисов HQ и BR.
* Обеспечьте разрешение имён согласно таблице 2.
* Укажите общедоступный DNS-сервер в качестве пересылочного.

 **Настройка часового пояса**:

* Синхронизируйте все устройства с часовым поясом экзамена.

ЧЁ ГДЕ ЕСТЬ

1. [Ситуативные команды](#Ситуативные_команды)
2. [Создание машин](#Создание_машин)

1. [Модуль 1](#Модуль_1)
2. [Настройте имена устройств согласно топологии](#Настройте_имена_устройств_согласно)
3. [Настройка ISP](#Настройка_ISP)
4. [Реализуйте NAT](#Реализуйте_динамическую_NAT)
5. [Создание пользователя](#созданий_пользователя)
6. [Настройка SSH](#Настройка_безопасного_удалённого_доступа)
7. [Конфигурация IP-туннеля между HQ и BR](#GRE)
8. [Обеспечение динамической маршрутизации](#OSPF)
9. [Настройка DHCP](#DHCP)

1. [Настройка DNS](#DNS)

1. [Настройка часового пояса](#ten2)
2. [Ansible](#ansible2)
3. [Trable shutting](#Trable_shutting)

Ситуативные команды

apt-get update- для обновления пакетов

systemctl restart network (тут любой сервис, лучше после перезагрузки машины(если будет) то много сервисов перезагрузить

systemctl restart network NetworkManager system-resolved

systemctl restart dhcpcd- служба отвечает за автоматическое получение IP-адреса и других сетевых параметров от DHCP-сервера.

shutdown -r now-перезагрузка системы

[apt-get install nano NetworkManager-tui](#nmtui)- команда для установки nmtui(после установки следует перезагрузить сеть(systemctl start NetworkManager)

[нажми, что бы вернуться к модулю 1](#nmtui2)(на установку nmtui)

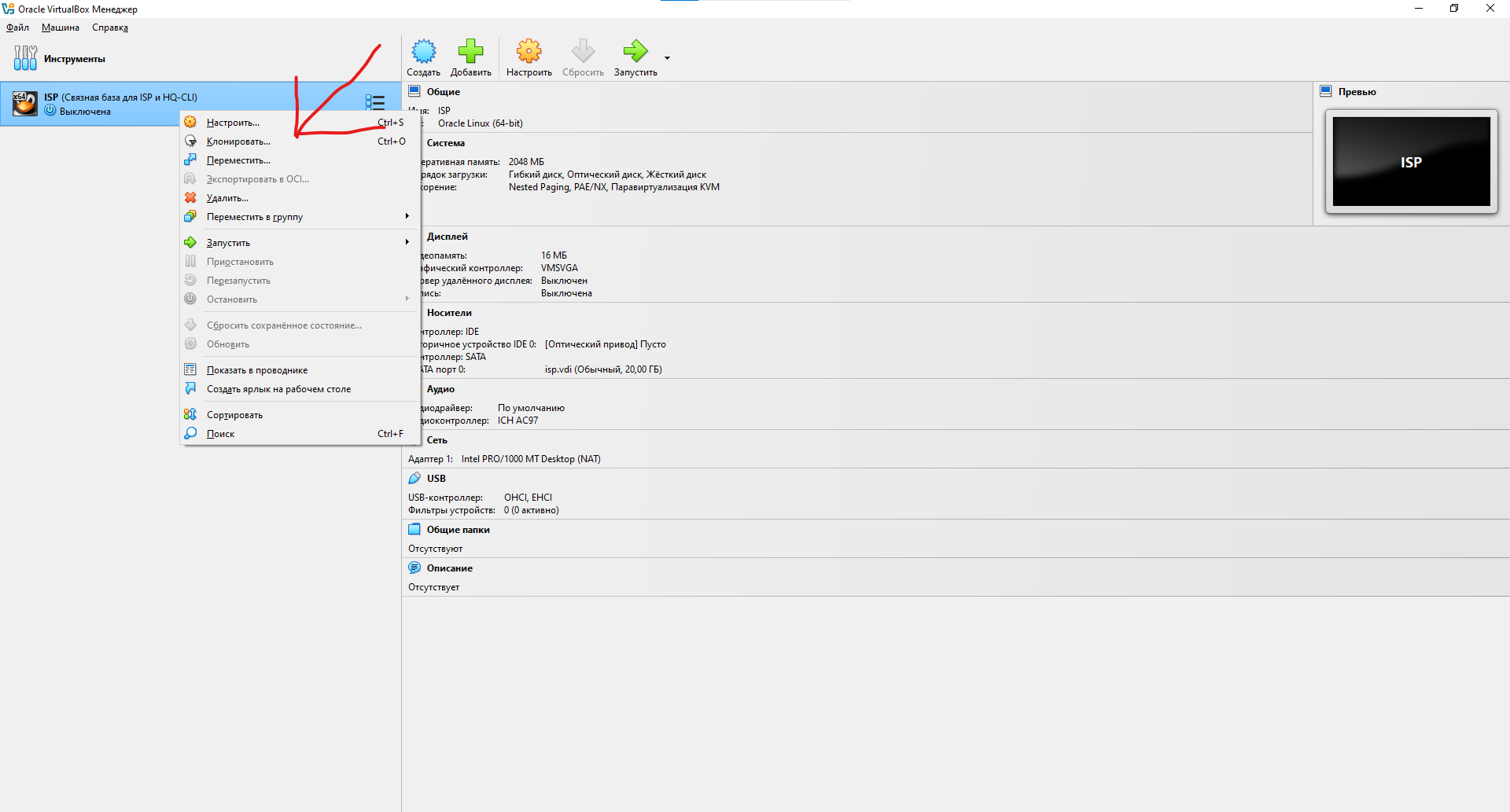
ip addr del 192.168.15.55/24 dev eth1 – удаление ip

ip link set enp(указывается какой интерфейс) up – включение int

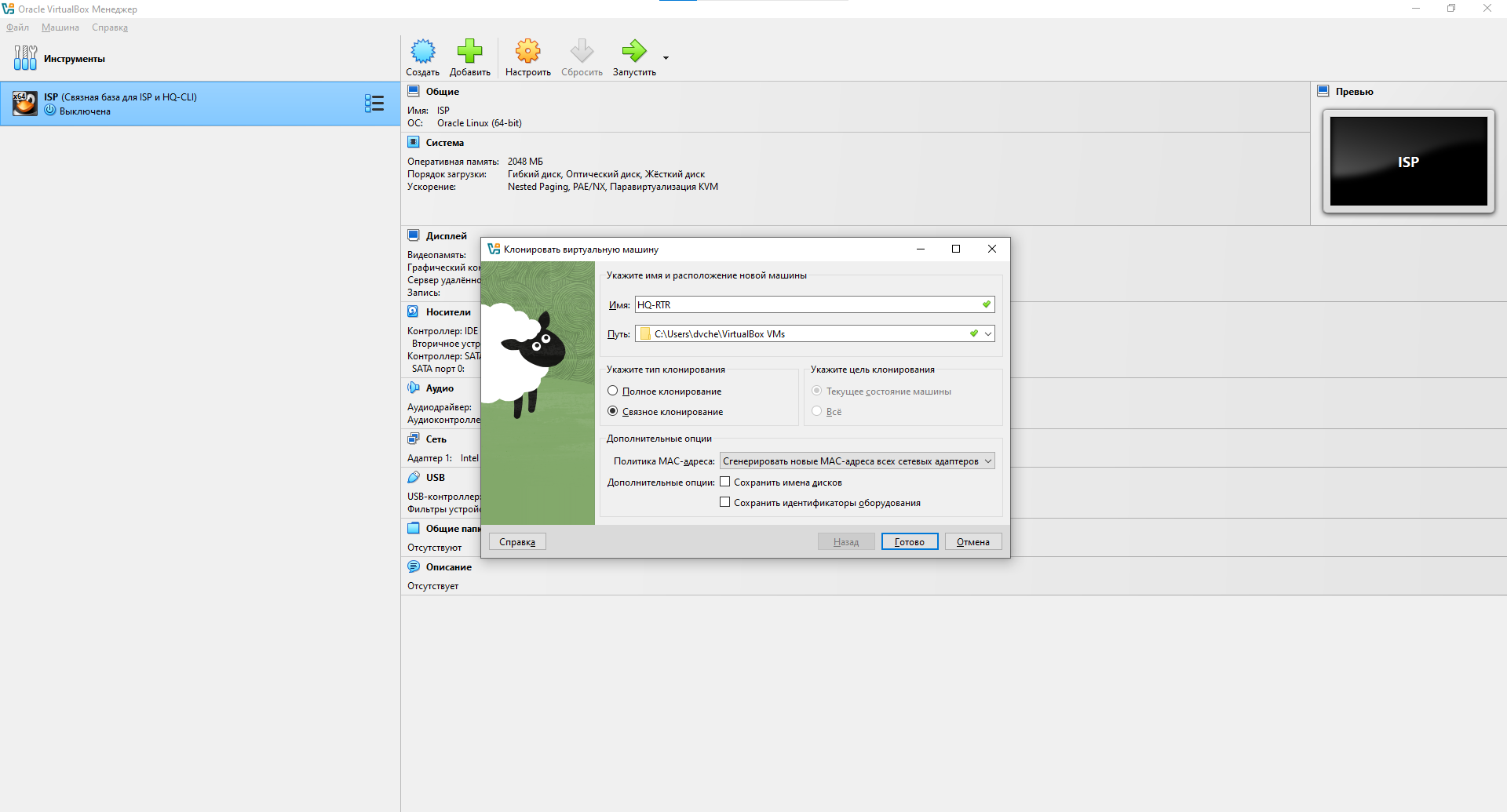
apt-get install nano – устанавливает nano

Создание машин

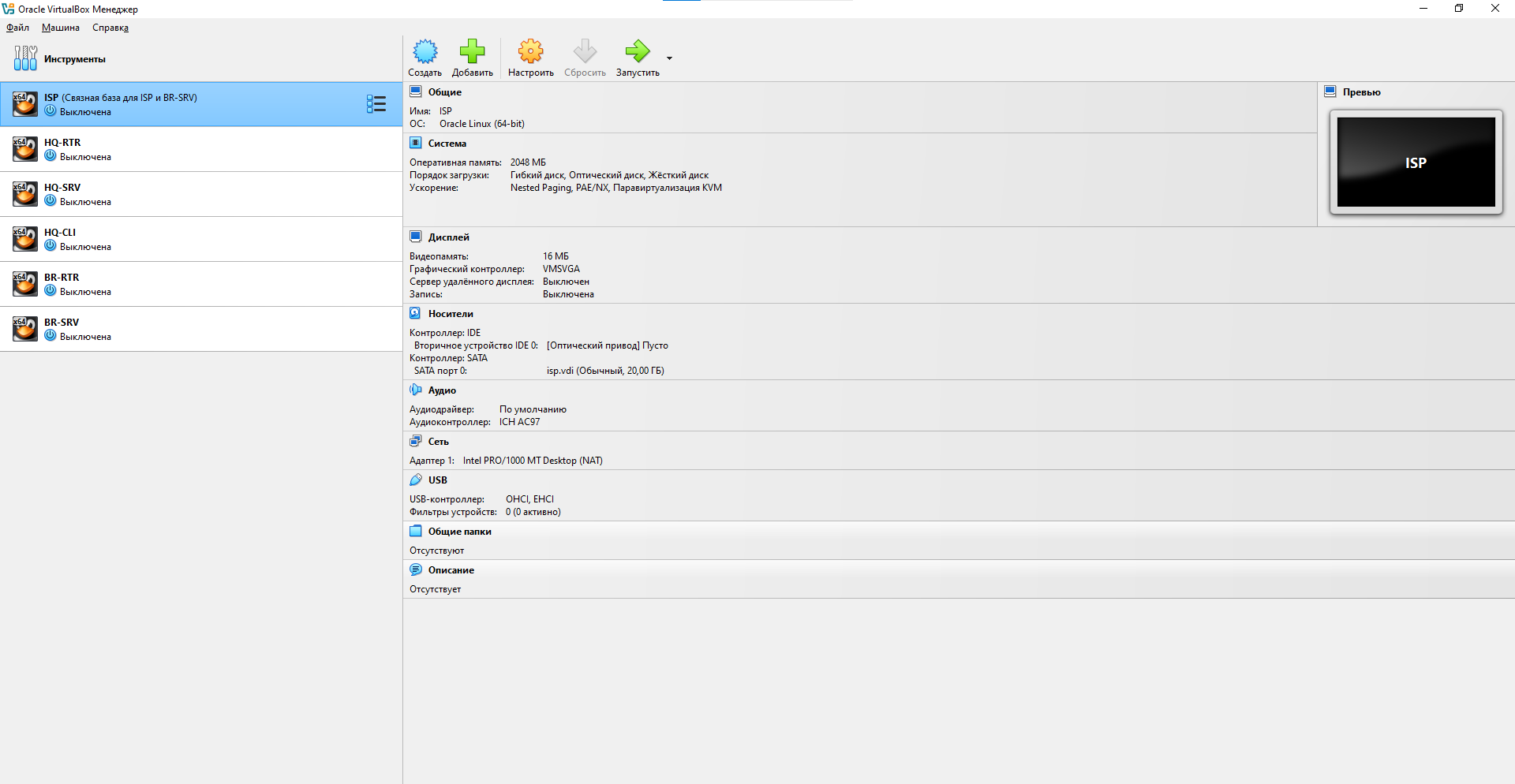
Мы создали роутер ISP(то есть уже можно зайти в систему), теперь нужно создать остальные связав с ISP с помощью клонирования



Далее переименовываем новую машину, выбираем связное клонирование и пункт- сгенерировать новые MAC-адреса(этот пункт один, его тыкаем, никакие галочки не ставим)

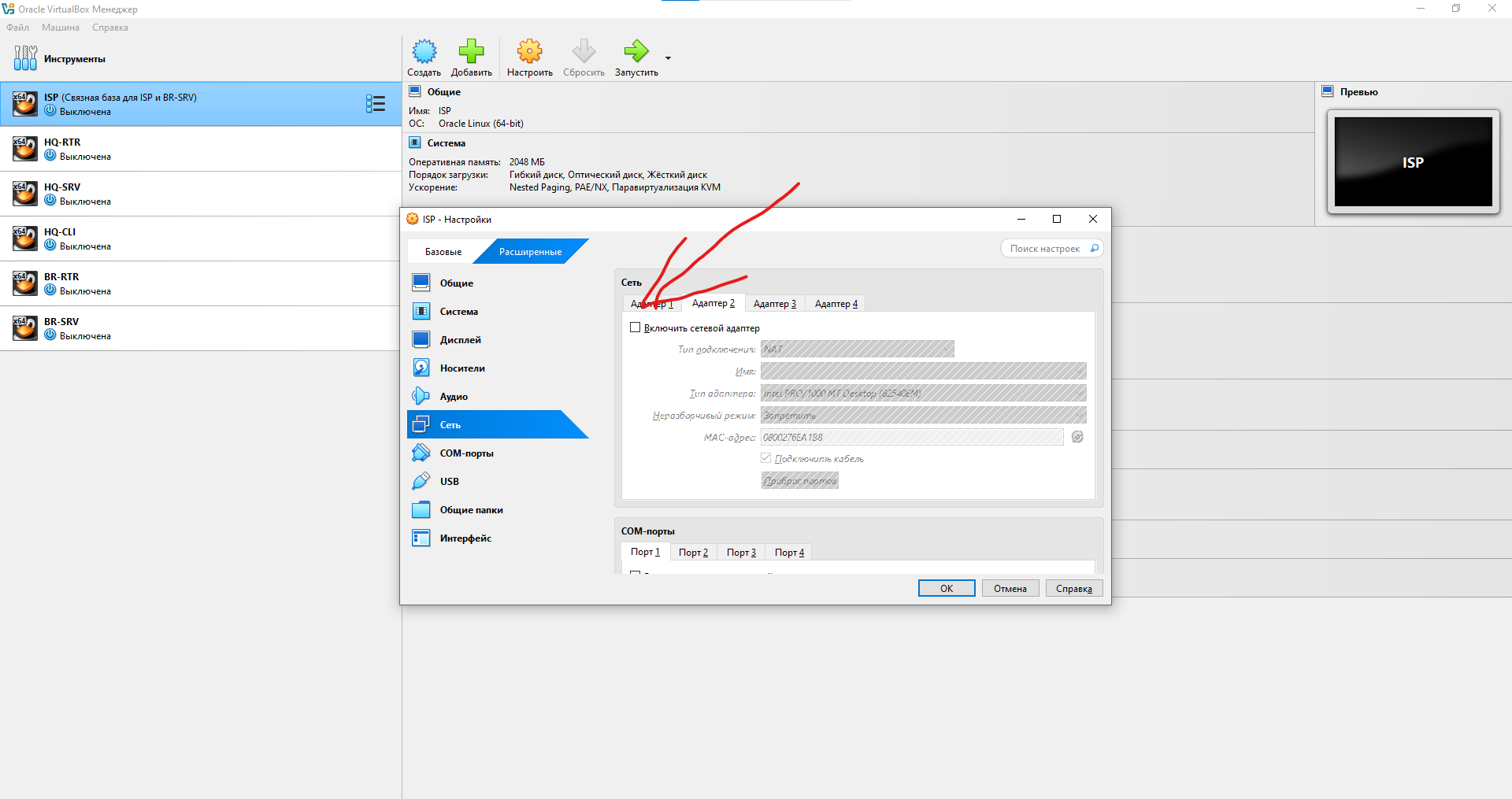


Проводим так с остальными машинами, и в итоге получаем такую картину

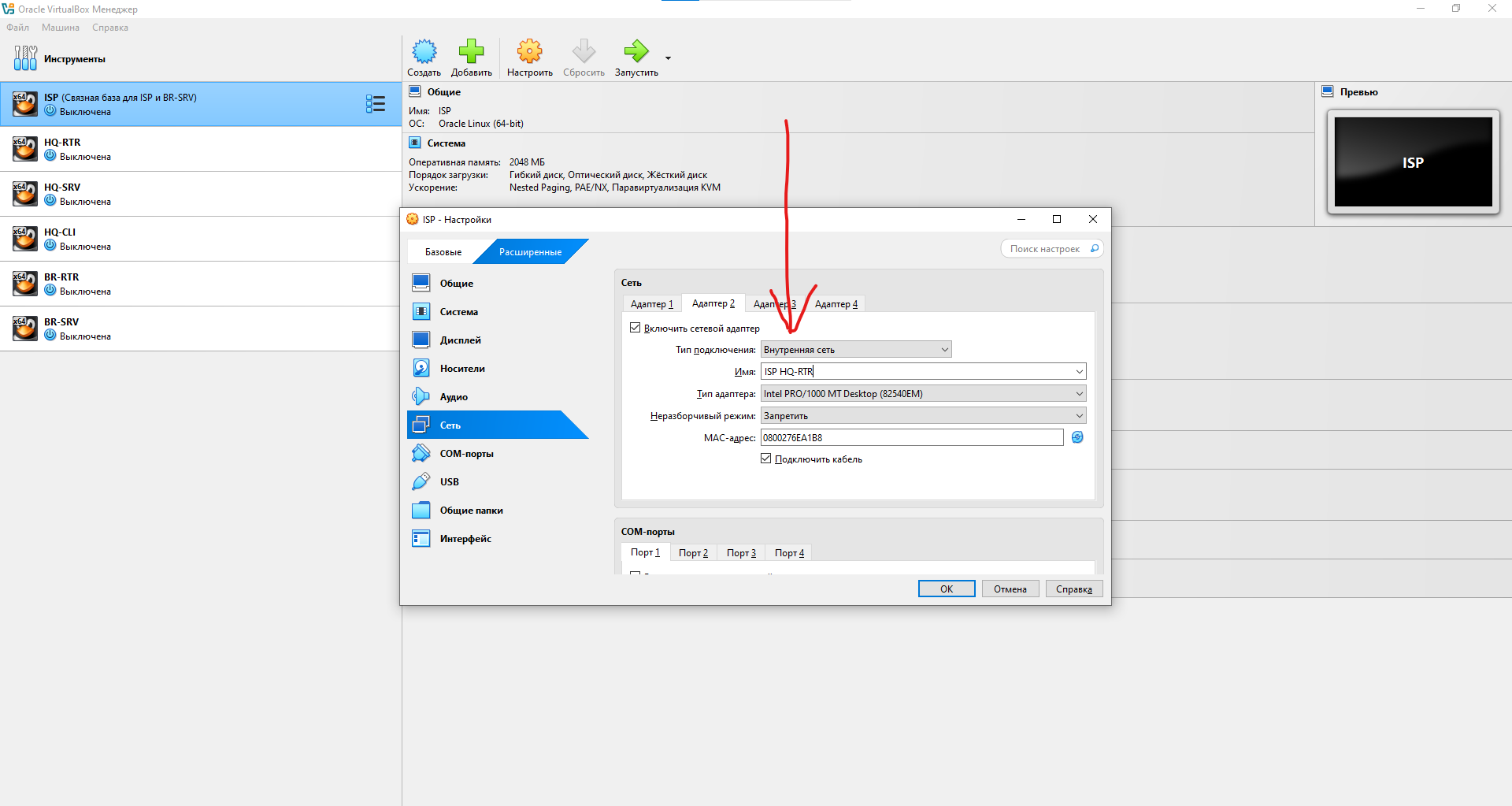


Настройка видимости других роутеров

На роутере ISP открываем настроить => сеть => адаптер 2 => включить и выбрать внутреннюю сеть

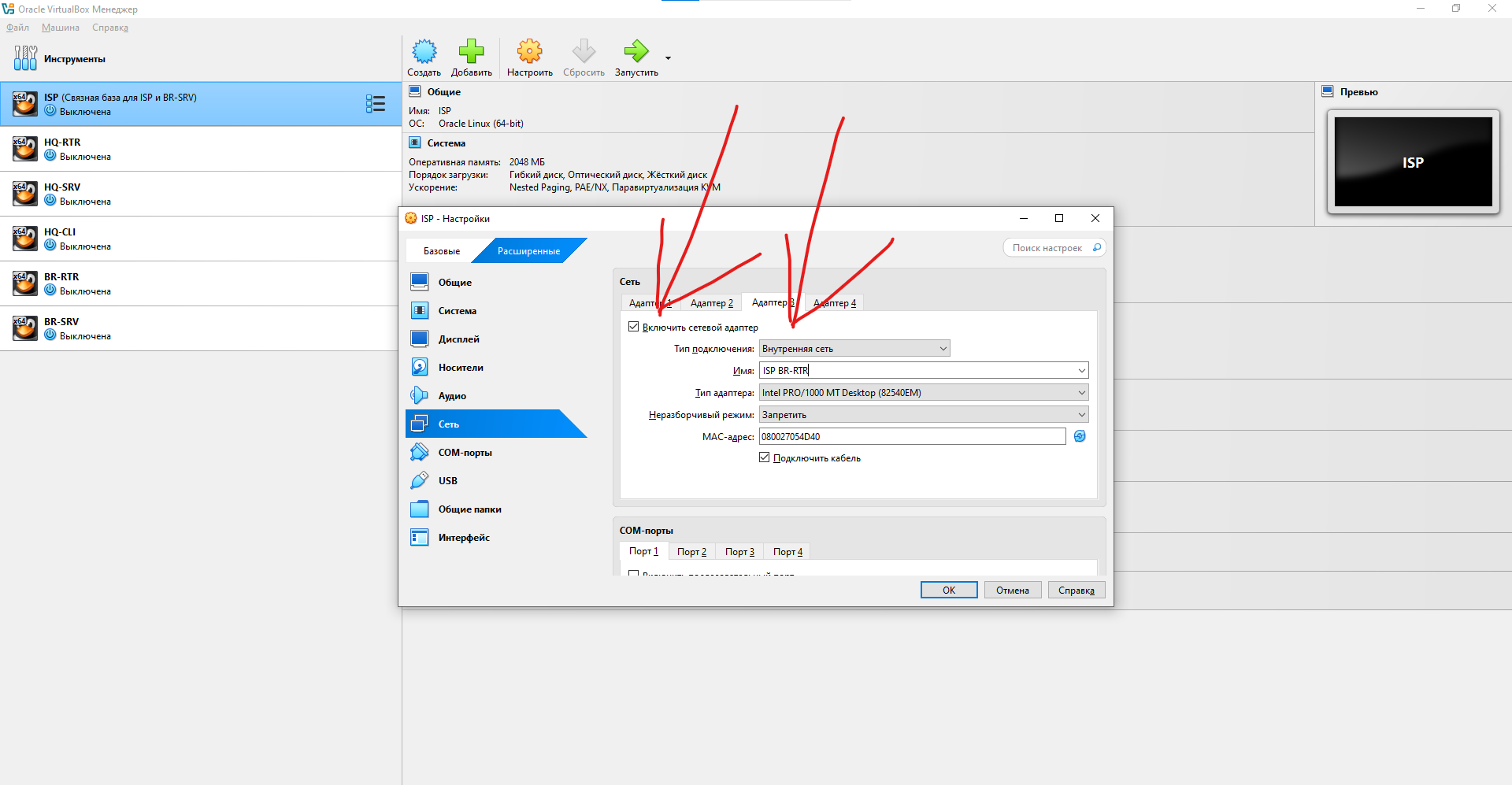


Пишем имя этого адаптера у меня ISP HQ-RTR

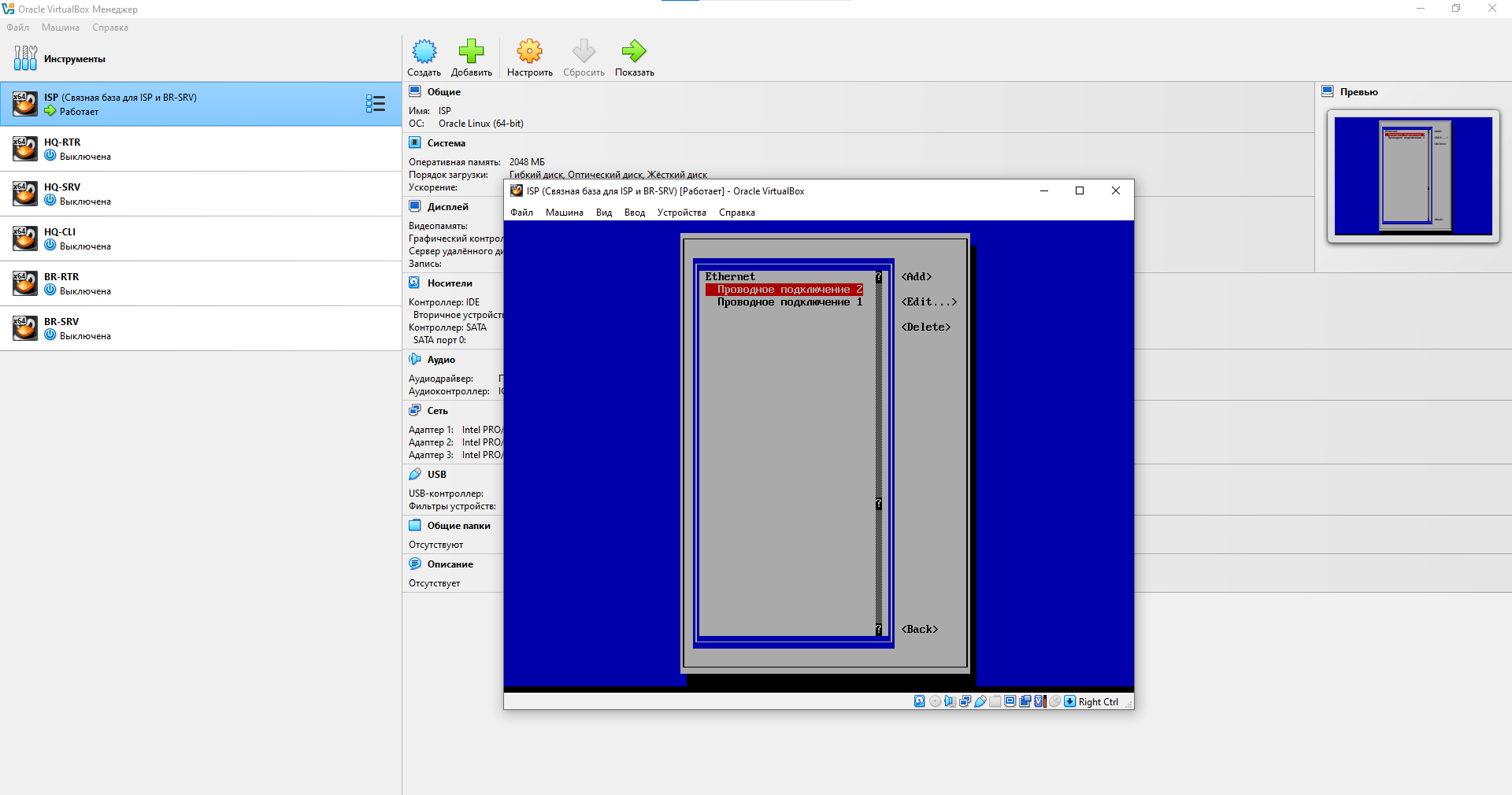


Проделываем тоже самое уже для другого роутера выбирая адаптер 3

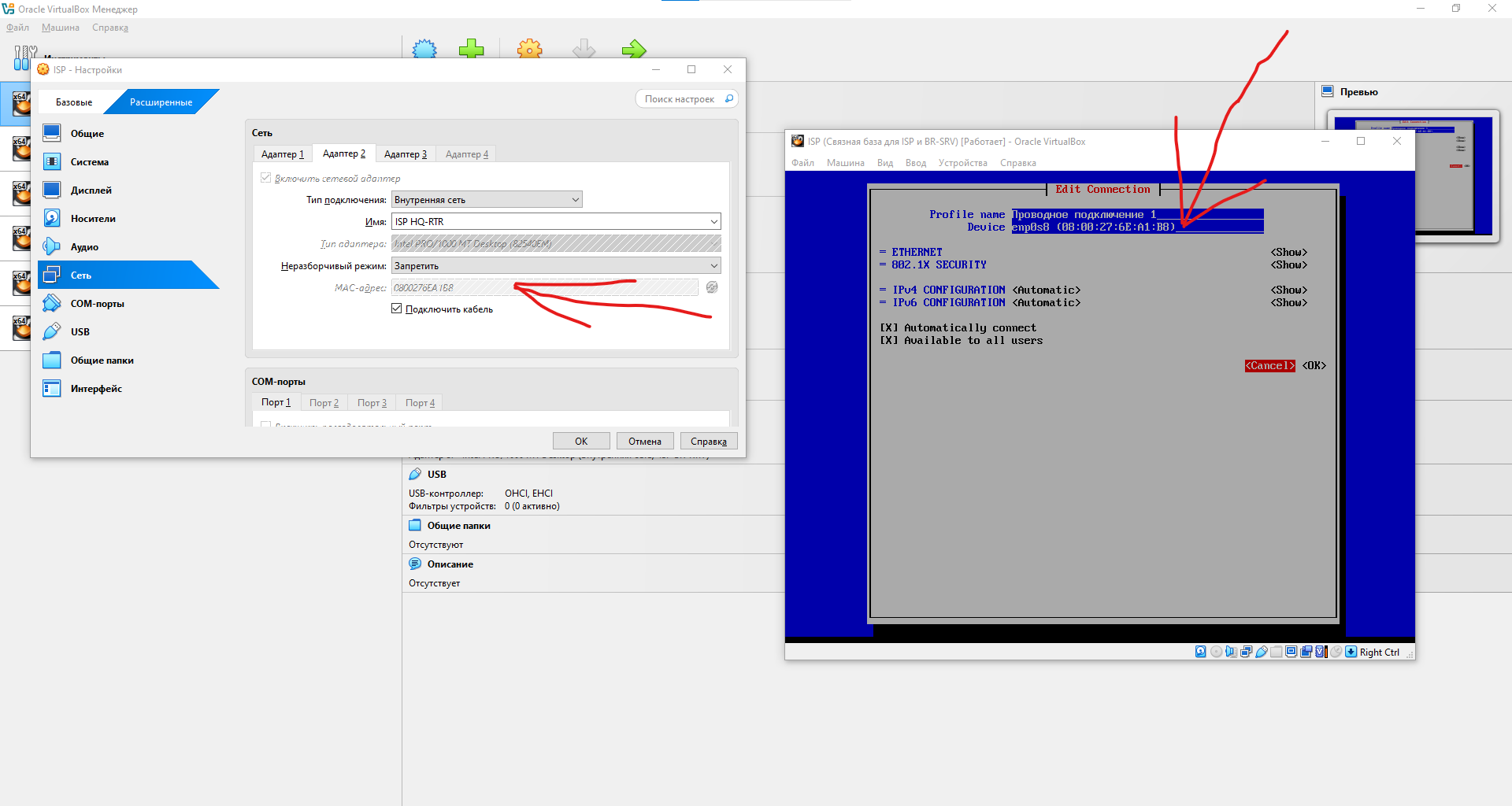
У меня имя ISP BR-RTR



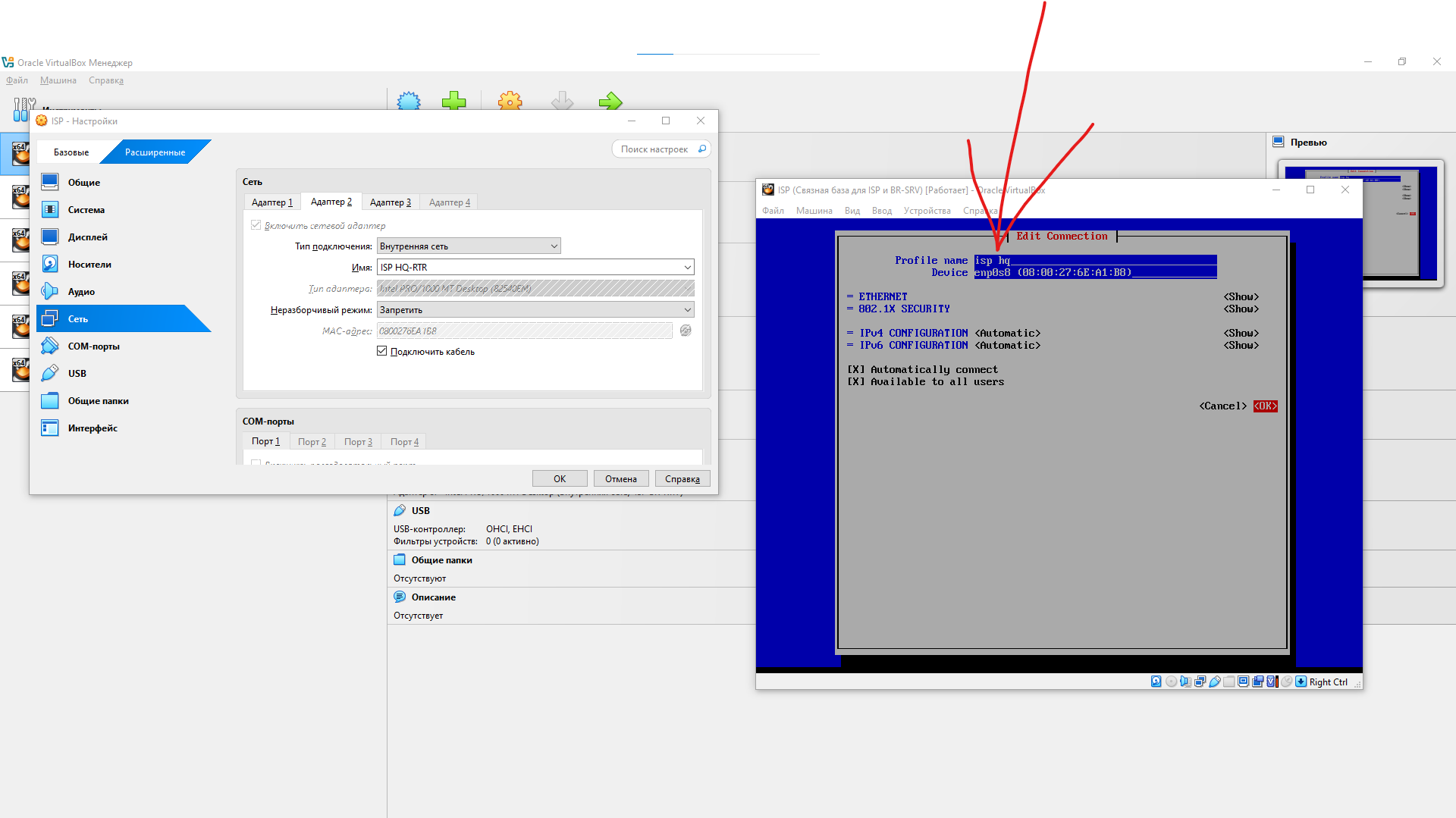
Как видим, у нас добавились и видны эти адаптеры, НО как понять какой из них к какому роутеру



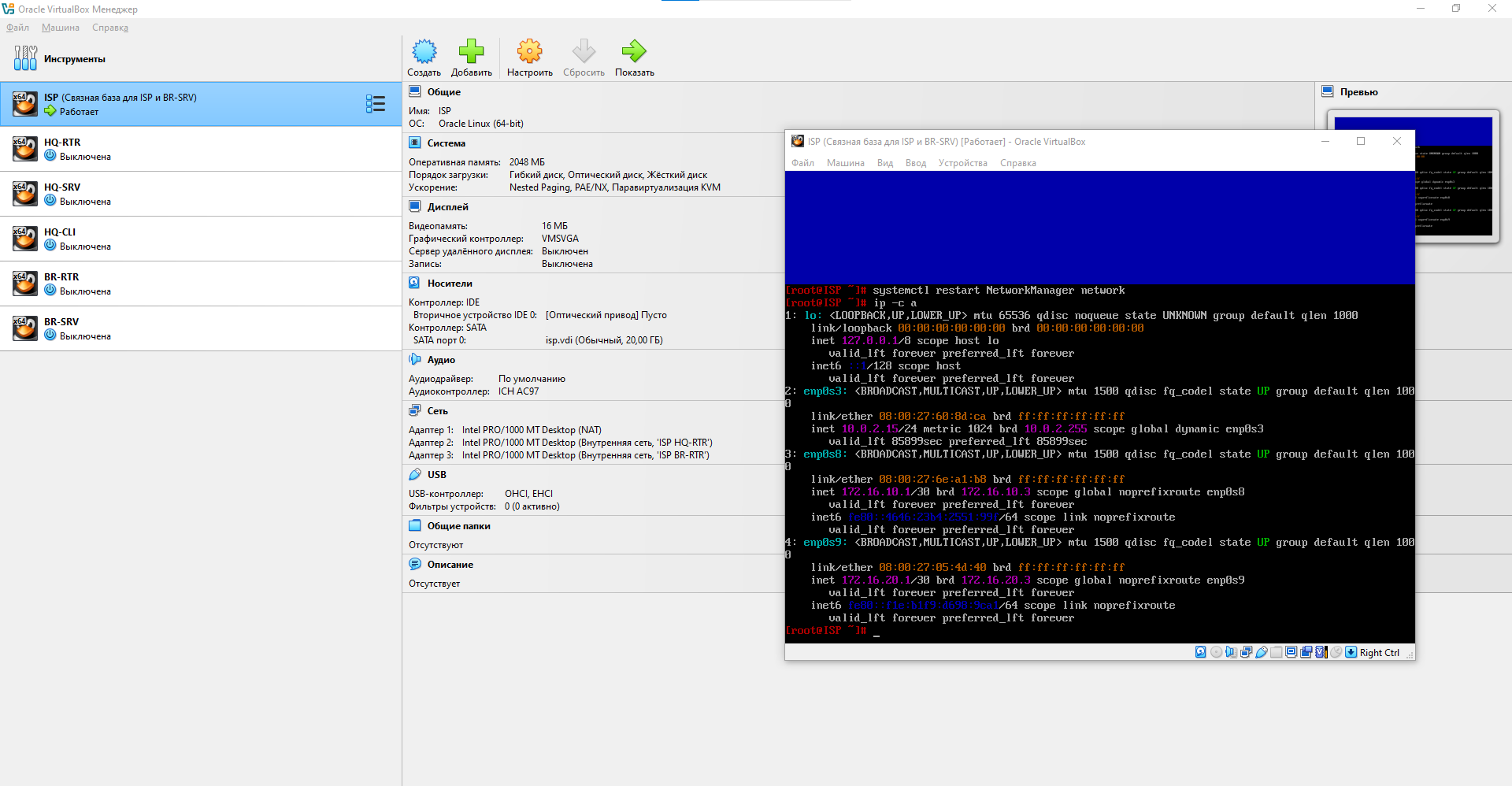
Открываем настроить => сеть => адаптер 2(для начала) и сверяем mac-адрес тут с тем который видим настройках (через [nmtui](#install_nmtui))



И видим что они одинаковы это наш адаптер для роутера HQ, для удобства переименуем -проводное соединение 1 в isp hq



Тоже самое делаем и для другого роутера, сверяем, хотя методом исключения и так понятно, что оставшийся верный

После задаем адреса и перезагружаем настройки systemctl restart NetworkManager 

Перейдем к роутеру HQ-RTR

Делаем все также с добавлением адаптеров НО имя выбираем которое писали для нужно рт

То на рт HQ-RTR выбираем имя из списка ISP HQ-RTR

И также потом сверяем mac-адреса



**Модуль 1**

[**ЧЁ**](#ЧЁ)

**Настройте имена устройств согласно топологии.**

Что ж, тут и так понятно, что нужно, если знаешь команду, то все норм, если нет, смотри ниже

hostnamectl set-hostname isp;exec bash



На всех устройствах необходимо сконфигурировать IPv4

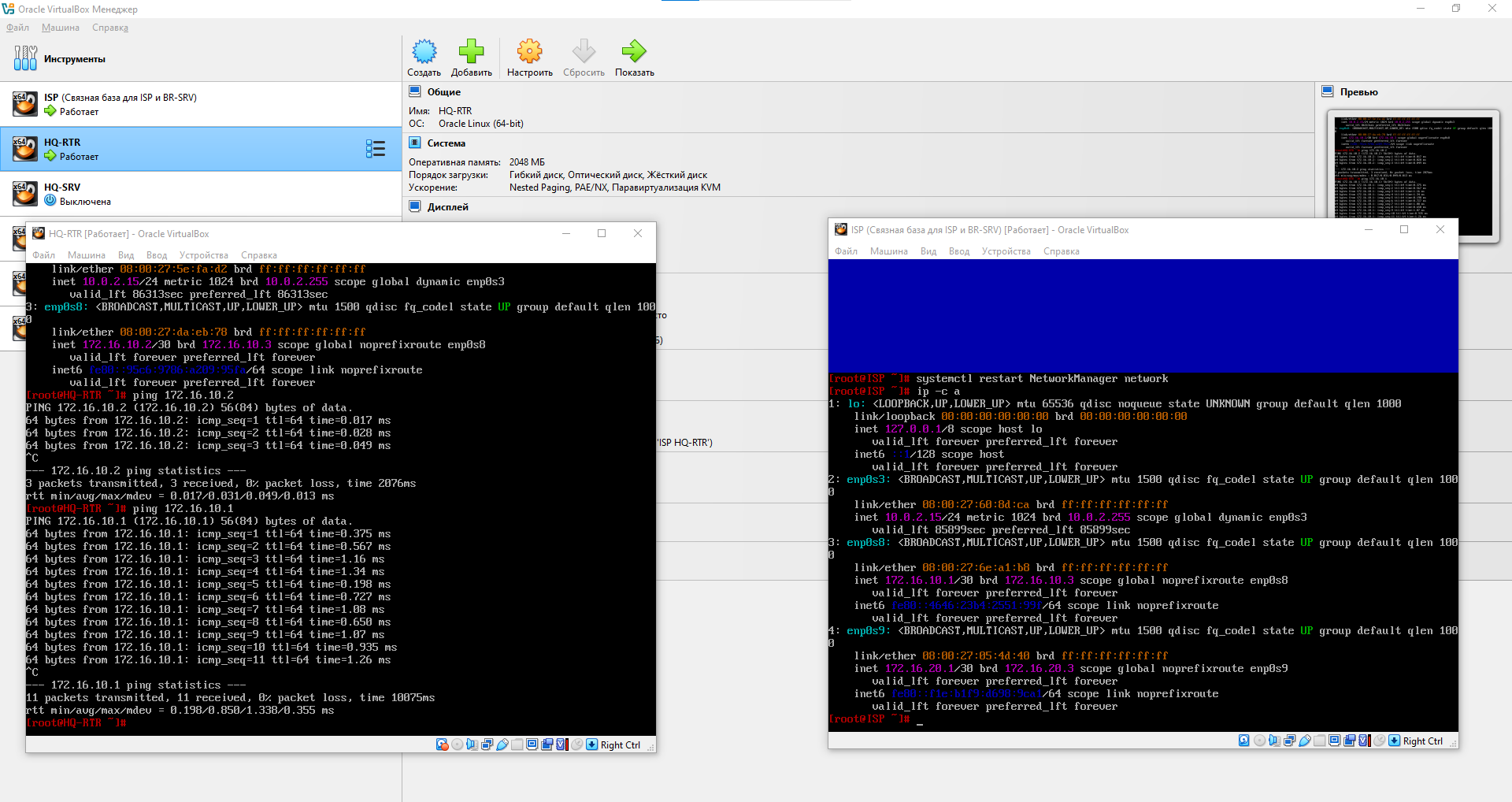
IP-адрес должен быть из приватного диапазона

Для начала установите [nmtui](#install_nmtui)

Эти диапазоны определены в RFC 1918 и включают:

1. **10.0.0.0 - 10.255.255.255** (10.0.0.0/8)
2. **172.16.0.0 - 172.31.255.255** (172.16.0.0/12)
3. **192.168.0.0 - 192.168.255.255** (192.168.0.0/16)

Сделано в выше указанных настройках



Вот результат, рт ISP и HQ-RTR между ними есть ping

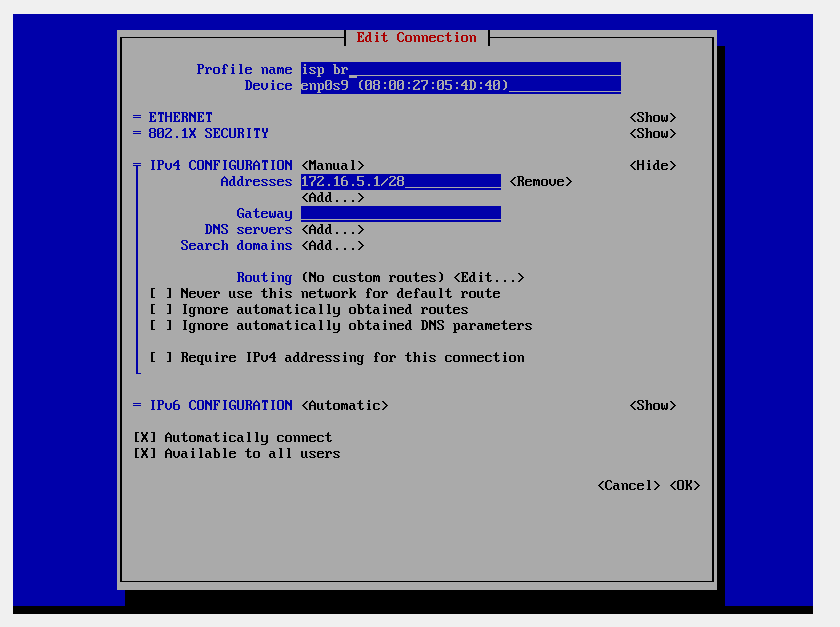
**Сведения об адресах занесите в отчёт, в качестве примера используйте Таблицу 3**

**2****. Настройка ISP ● Настройте адресацию на интерфейсах:**

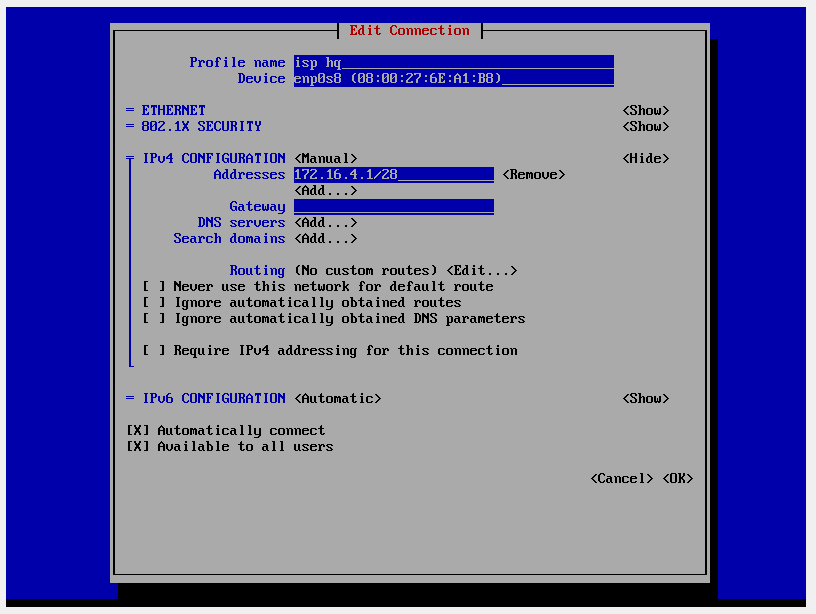
[**ЧЁ**](#ЧЁ)

1. Интерфейс, подключенный к провайдеру, получает адрес по DHCP.
2. Интерфейсы для HQ-RTR и BR-RTR используют сети 172.16.4.0/28 и 172.16.5.0/28 соответственно.
3. Настройте маршруты по умолчанию там, где это необходимо.
4. Реализуйте динамическую NAT для доступа к Интернету на маршрутизаторе ISP.

Адресация в строну BR



Адресация в строну HQ



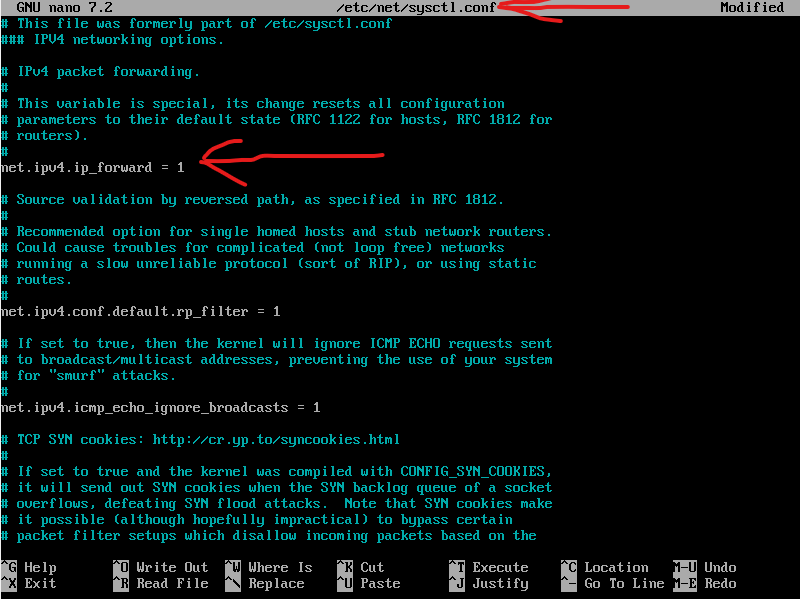
1. Реализуйте динамическую NAT для доступа к Интернету через маршрутизатор ISP.

[**ЧЁ**](#ЧЁ)

Чтобы реализовать это, нужно включить forwarding а именно, пишем команду:

nano /etc/net/sysctl.conf

В файле находим строчку net.ipv4.ip\_forward=0 и заменяем 0 на 1



**Настройка NAT с использованием iptables**

Настройка NAT (MASQUERADE)

Это делается на ISP

iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

enp0s3 интерфейс направленный в сторону провайдера

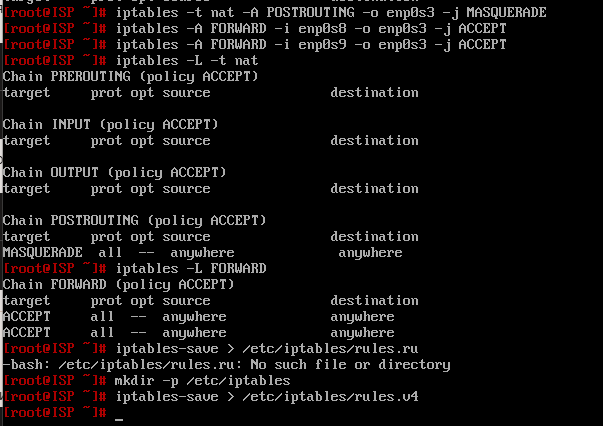
Разрешение пересылки трафика

iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT

iptables -A FORWARD -i enp0s9 -o enp0s3 -j ACCEPT

Сохранение iptables

iptables-save > /etc/iptables.rules



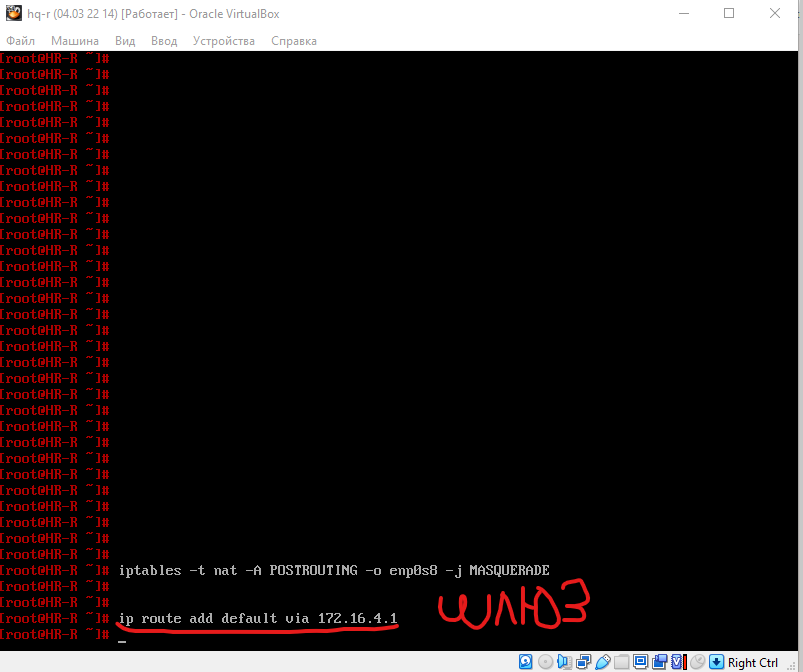
Теперь настройка NAT на HQ-R

iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE

enp0s8 интерфейс направленный в сторону ISP

Добавляем маршрут по умолчанию (через ISP)

ip route add default via 172.16.4.1



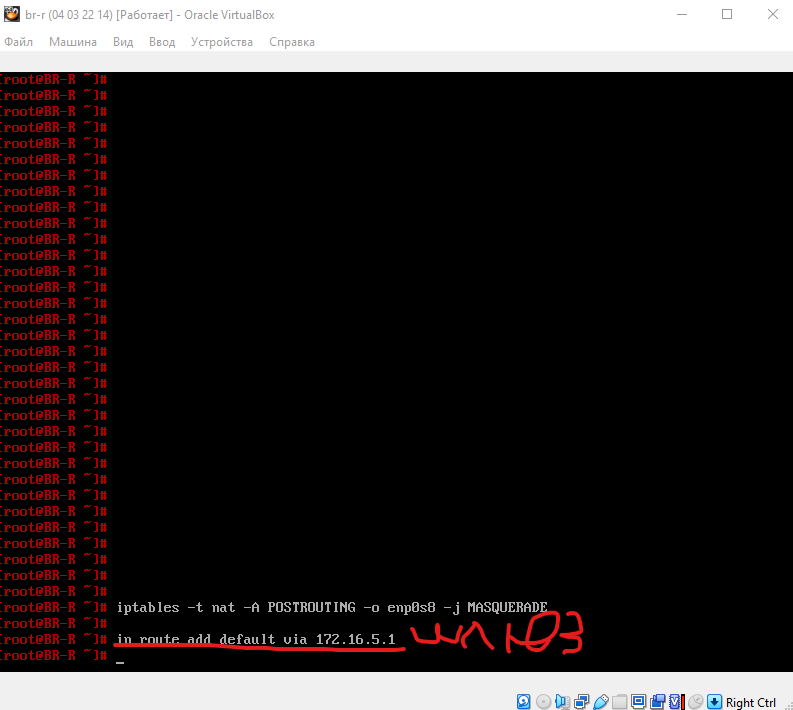
Дальше идет настройка NAT на BR-R

iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE

enp0s8 интерфейс направленный в сторону ISP

Добавление маршрута по умолчанию (через ISP)

ip route add default via 172.16.5.1



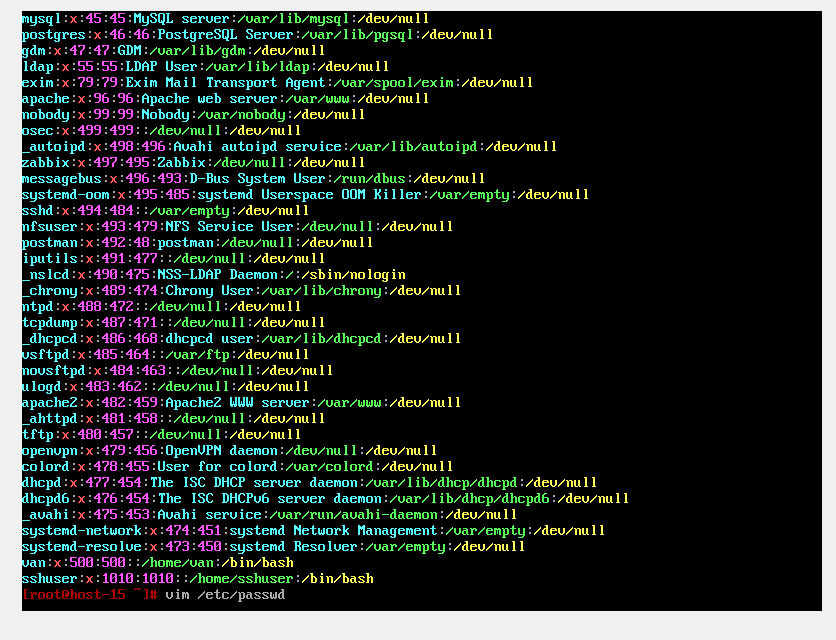
 **Создание локальных учетных записей**:

* Создайте пользователя sshuser на HQ-SRV и BR-SRV с:
  + Паролем P@ssw0rd.
  + UID 1010.
  + Правами без запроса пароля.
* Создайте пользователя net\_admin на HQ-RTR и BR-RTR с:
  + Паролем P@$$word.
  + Максимальными привилегиями для EcoRouter или на Linux.
* Создайте пользователя sshuser на HQ-SRV и BR-SRV с:
  + Паролем P@ssw0rd.
  + UID 1010.
  + Правами без запроса пароля.

Пишем команду для создания пользователя (на HQ-SRV BR-SRV и только):[**ЧЁ**](#ЧЁ)

useradd -u 1010 -m sshuser

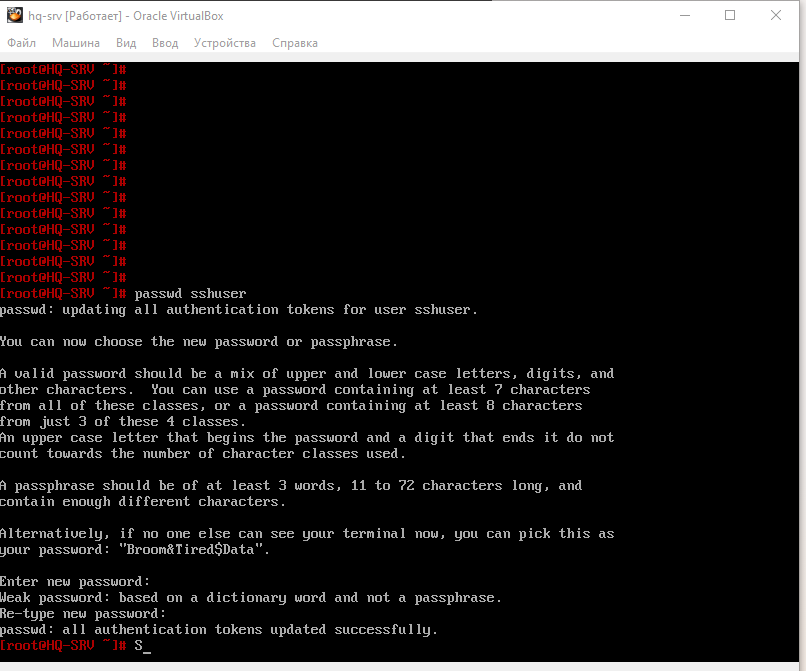




Проверили что пользователь создан (nano /etc/passwd)(последняя строчка)

Следующий шаг, это создание пароля для пользователя

Используем команду passwd(отвечает за создание пароля) sshuser(имя пользователя которому нужно создать пароль)



**Настройка прав без ввода пароля для (sudo)**

ls -l /etc/sudoers –проверка прав на файл



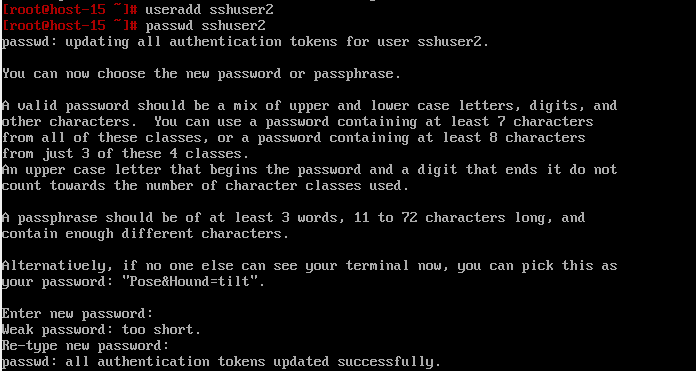
Если видим такую картину, значит, что файл можно только читать, но не редактировать.

Что бы файл можно было изменить, изменим права



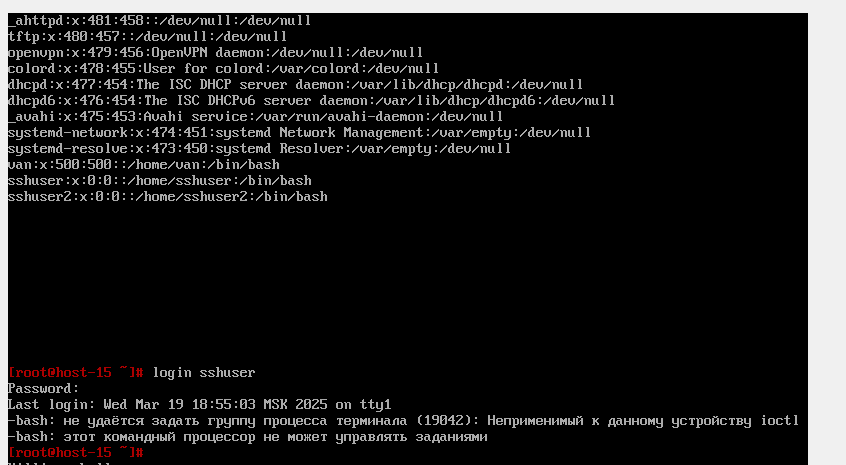
Теперь этот файл может редактировать кто угодно

Вводим команду nano /etc/sudoers, и в самом конце файла вписываем строку- sshuser ALL=(ALL) NOPASSWD: ALL, выходим и сохраняем



Луше не добавлять никаких дополнительный тегов к этой команде если нужен просто пользователь. ВМЕСТО SSHUSER2 м.б любой юзер

Что бы отредактировать права пользователя и дать фулл доступ без пароля ему везде сделайте следующие вещи:

* 1. Пишем команду visudo и нажимаем page down
  2. 

Редактируем вот так и получаем заветный фулл доступ

ВНИМАНИЕ:

1. **В справке по команде apt-get** есть фраза: «This APT has Super Cow Powers» (рус. «В APT есть коровья СУПЕРСИЛА»).
2. **Раскрыть «секрет» этой фразы** можно, если набрать команду apt-get moo — в терминале появится изображение коровы.
3. **В команде aptitude**, по описанию, нет «коровьей суперсилы», о чём также указано в справке. Однако, если набирать команду aptitude -v moo и так далее, добавляя каждый раз по одной букве «v», можно увидеть нечто интересное.

* Создайте пользователя net\_admin на HQ-RTR и BR-RTR с:
  + Паролем P@$$word.
  + Максимальными привилегиями для EcoRouter или на Linux.

Создаем пользователя, используя команду(на HQ-R и BR-R):

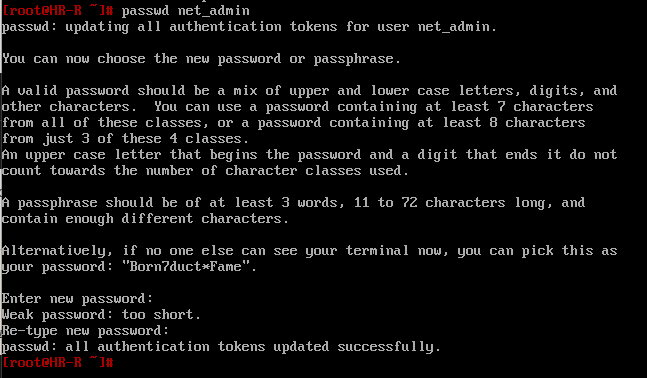
useradd -m -s /bin/bash net\_admin

-m: создаёт домашний каталог для пользователя.

-s /bin/bash: назначает Bash как оболочку.



Задаем пароль пользователю через – passwd net\_admin



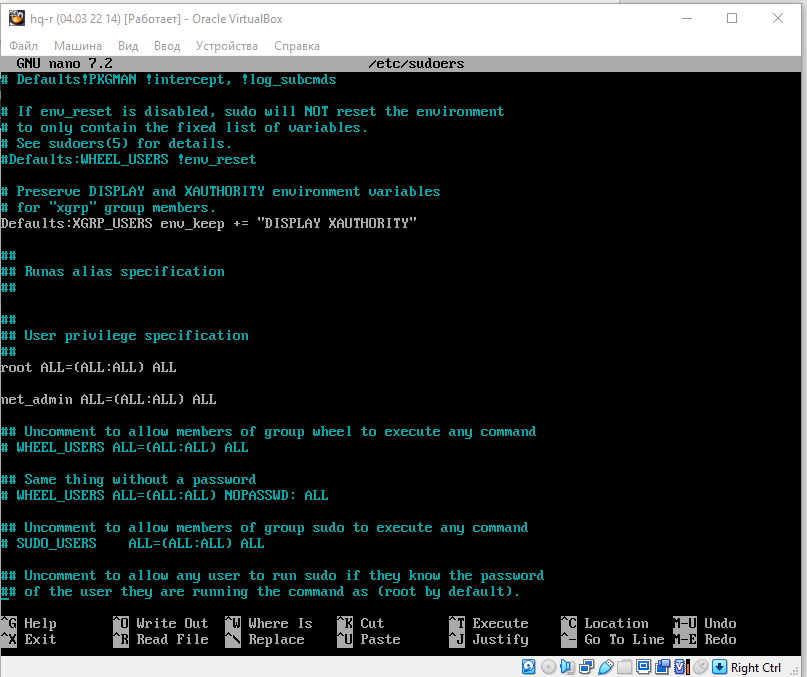
Теперь нужно дать права

usermod -aG wheel net\_admin

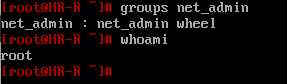
Проверяем сработало ли

Для этого используем команду groups имя пользователя

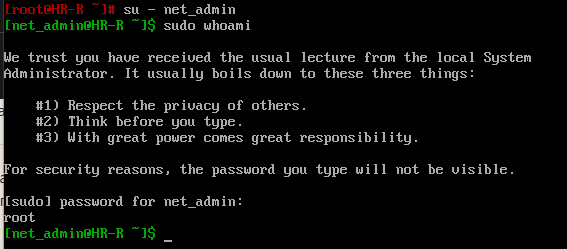




После ввода команд groups и wheel, видно что пользователь имеет права админа



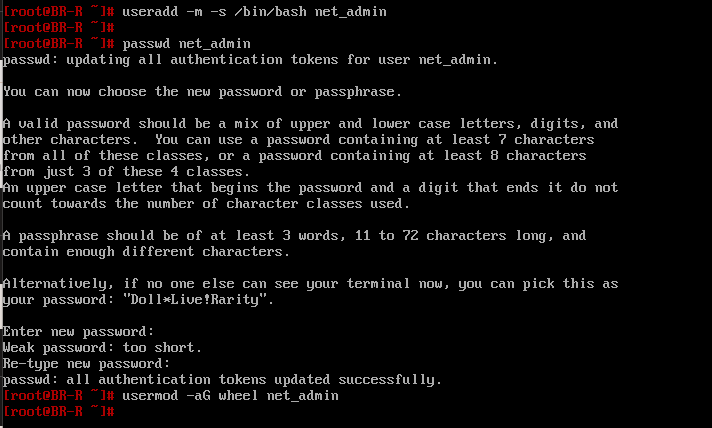
И для контрольной проверки войдем в пользователя

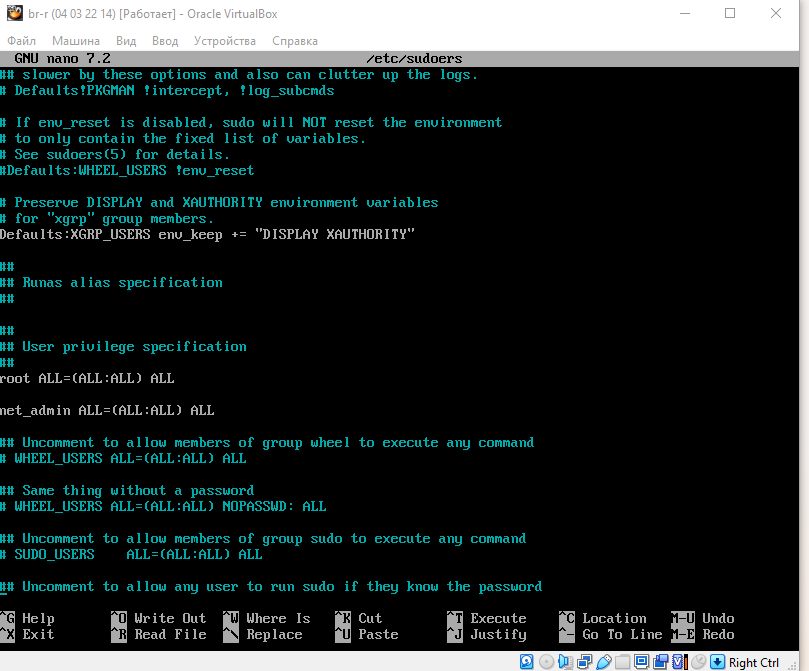
su – net\_admin

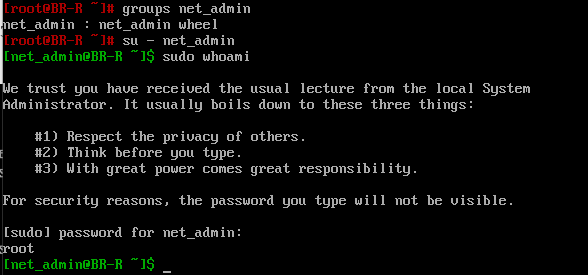
На HQ-R все ок, теперь переходим на BR-R(идентично)

BR-R

Точно также создаем пользователя и задаем пароль -P@ssw0rd





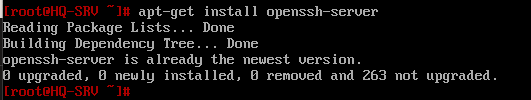


 **Настройка безопасного удалённого доступа** (на HQ-SRV и BR-SRV)

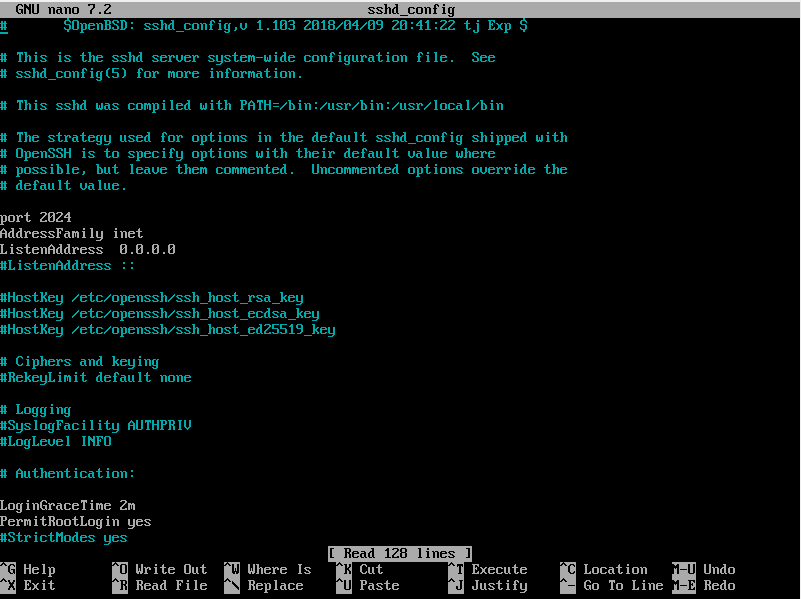
[**ЧЁ**](#ЧЁ)

* Разрешите доступ по порту 2024.
* Ограничьте попытки входа до двух.
* Настройте баннер: «Authorized access only».
* Позвольте подключения только пользователю sshuser.

Устанавливаем ssh если нет



Открываем конфиг по пути /etc/openssh/sshd\_config



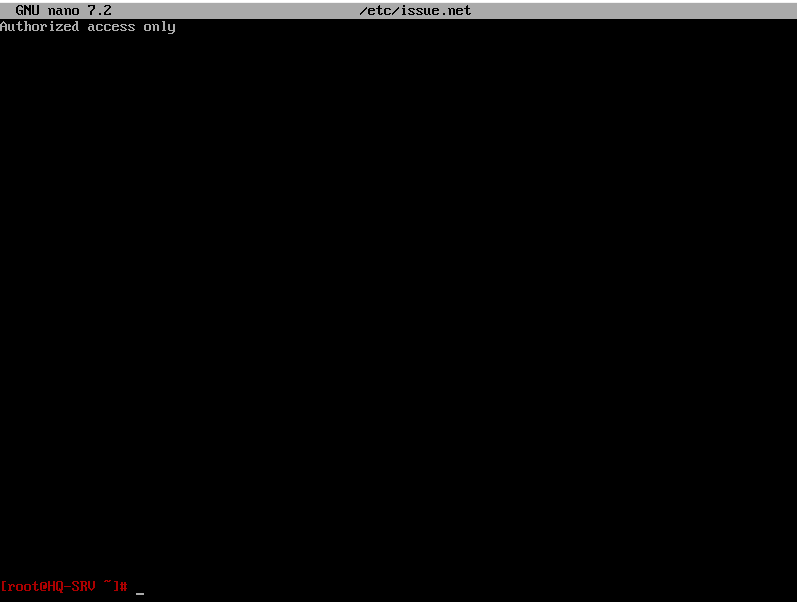
Добавляем строчку с файлом для баннера Banner /etc/issue.net



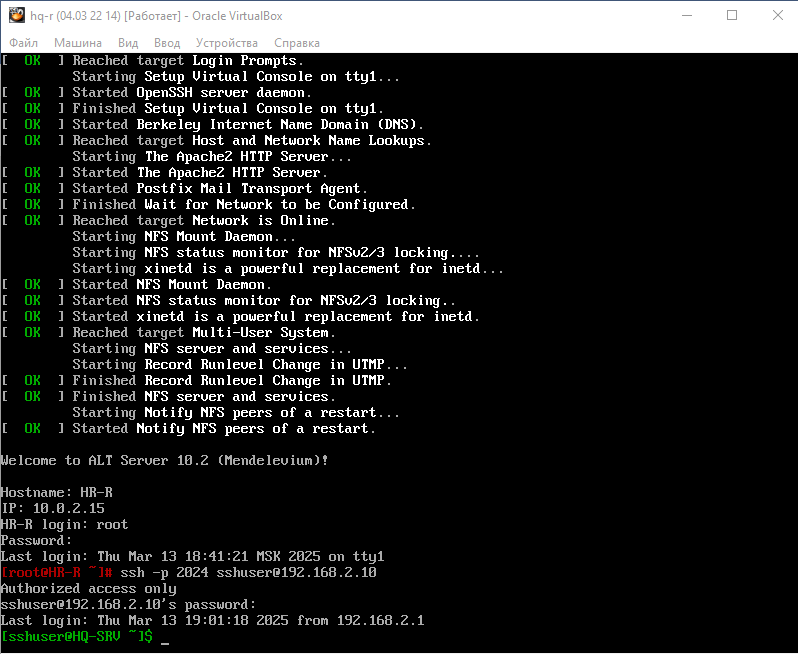
После изменений, перезагружаем ssh(команда systemctl restart sshd)

Дальше следует создать файл для настройки баннера

nano /etc/issue.net

И добавляем текст - Authorized access only

Проверяем подключение



**Конфигурация IP-туннеля между HQ и BR**:

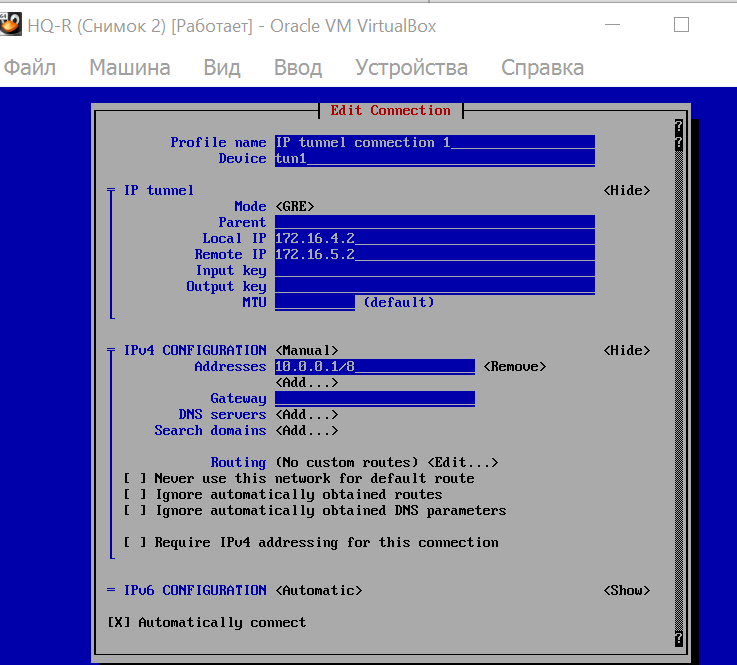
[**ЧЁ**](#ЧЁ)

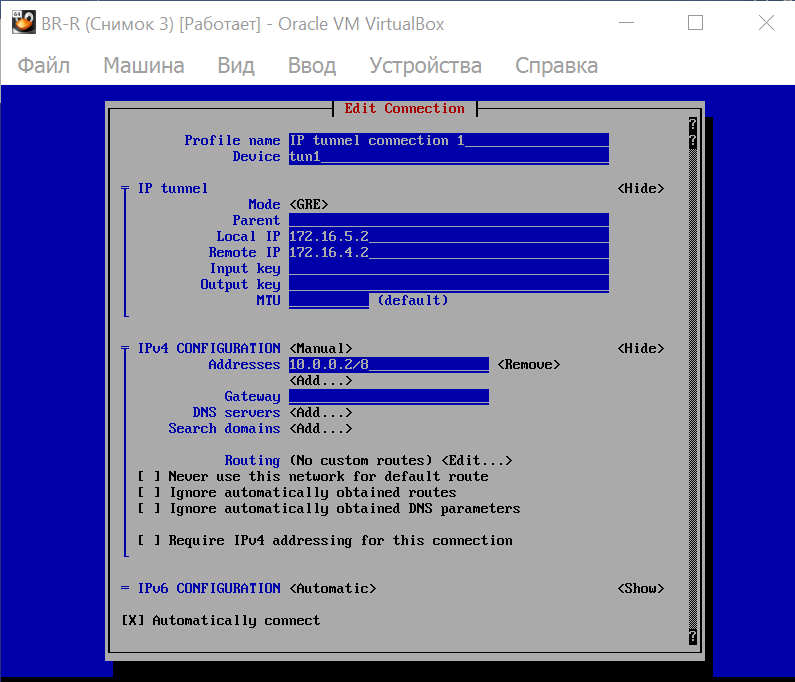
* Выберите технологию GRE или IP-in-IP.

Устанавливаем протокол для тунелирования apt-get install iproute2

На HQ-R и на BR-R

Создаем туннель:





* Включите сведения о туннеле в отчёт.

ip tunnel show

netstat –rn

**Обеспечение динамической маршрутизации**:

[**ЧЁ**](#ЧЁ)

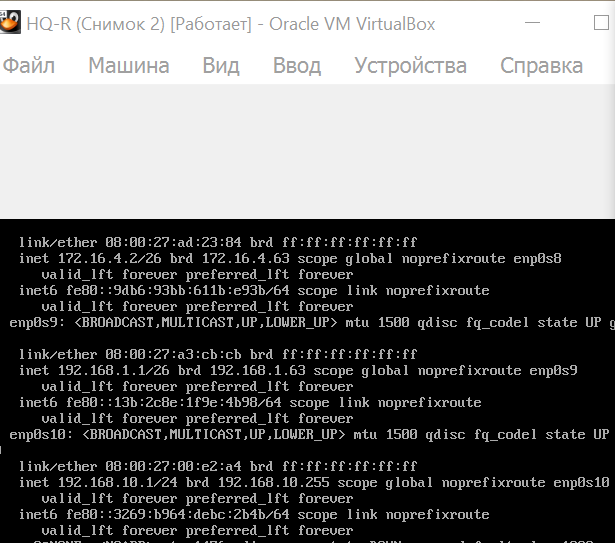
* Используйте link-state протокол (например, OSPF или IS-IS).
* Включите протокол только на интерфейсах IP-туннеля.
* Обеспечьте парольную защиту маршрутизационного протокола.
* Обменивайтесь маршрутами только между HQ-RTR и BR-RTR.

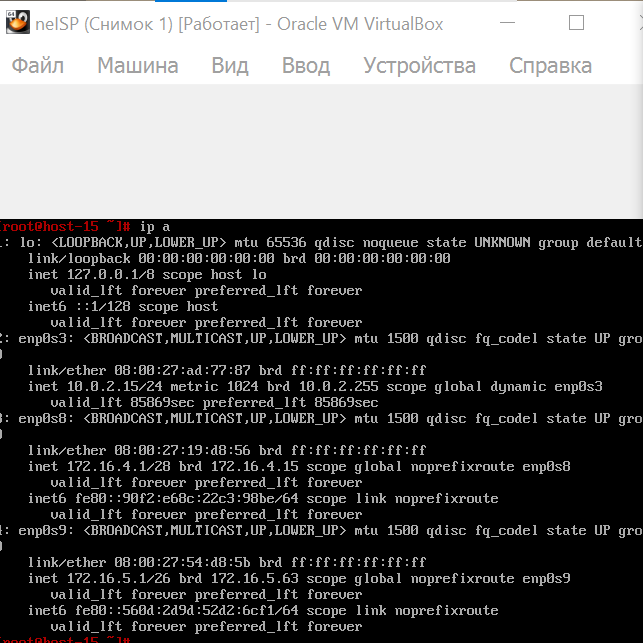
Устанавливаем frr(на HQ-R и BR-R)

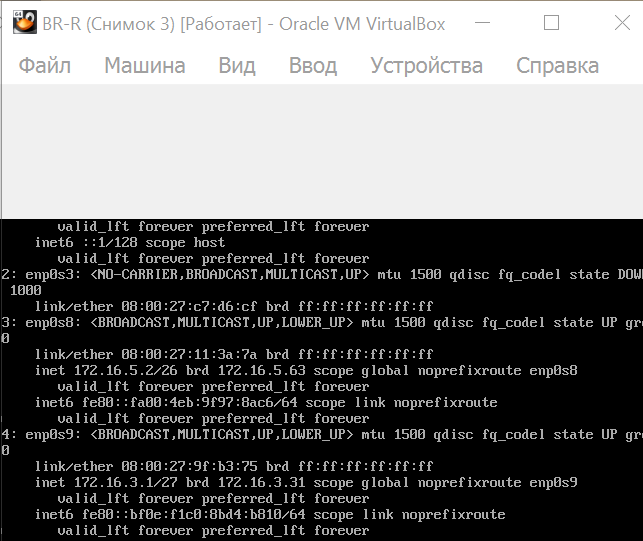
**OSPF**

**1)**Настроить связь между роутерами

**Примерно следующий вид**

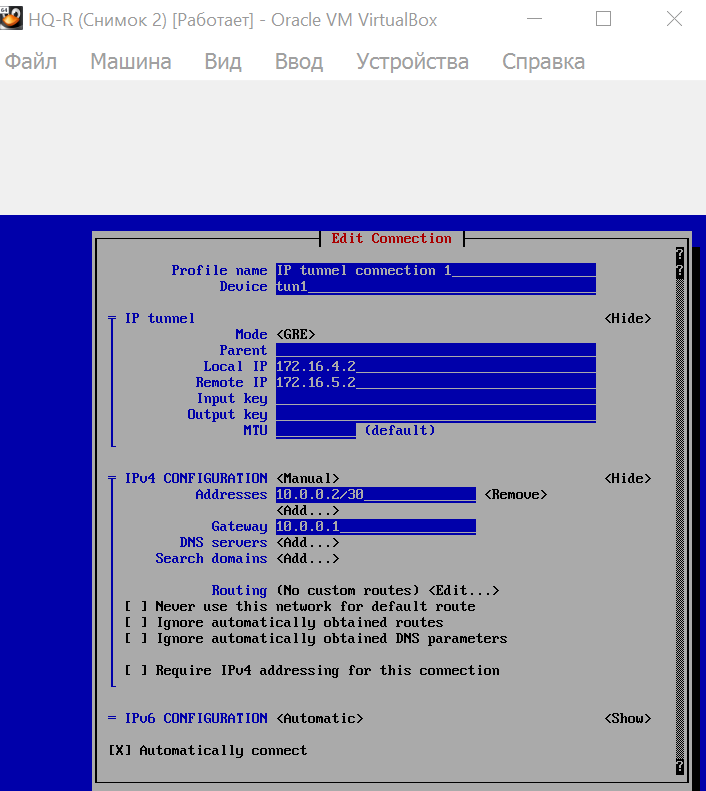
****

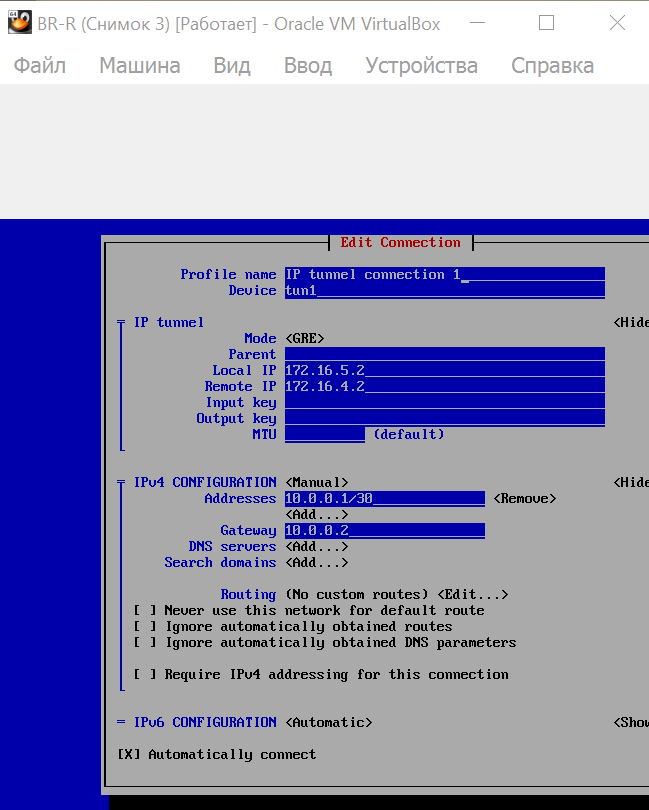
****

****

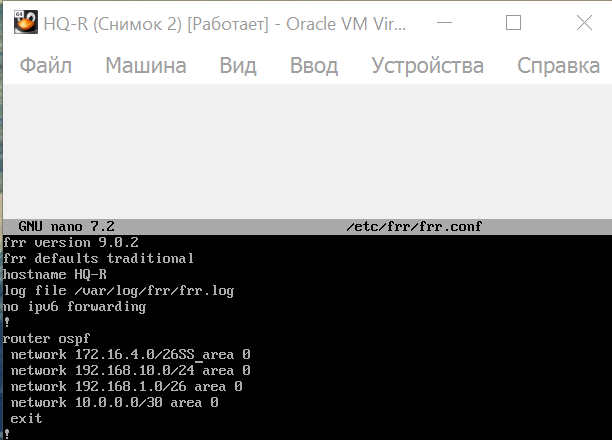
2)отключаем интерфейс NAT, иначе VB заартачится и будет пытаться связаться через него

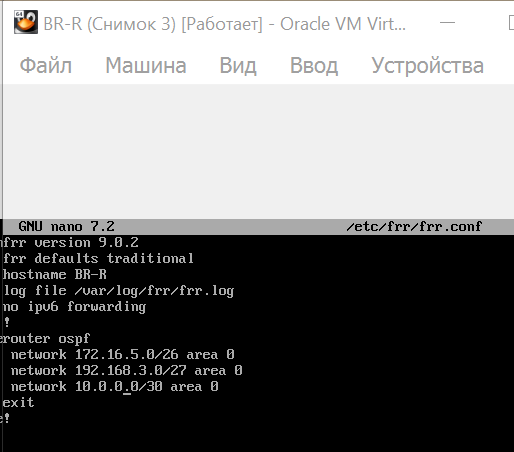
3)строим туннель между BR-R и HQ-R





Теперь долбанём рестарт systemctl restart NetworkManager network и теперь эти двое связаны на прямую.

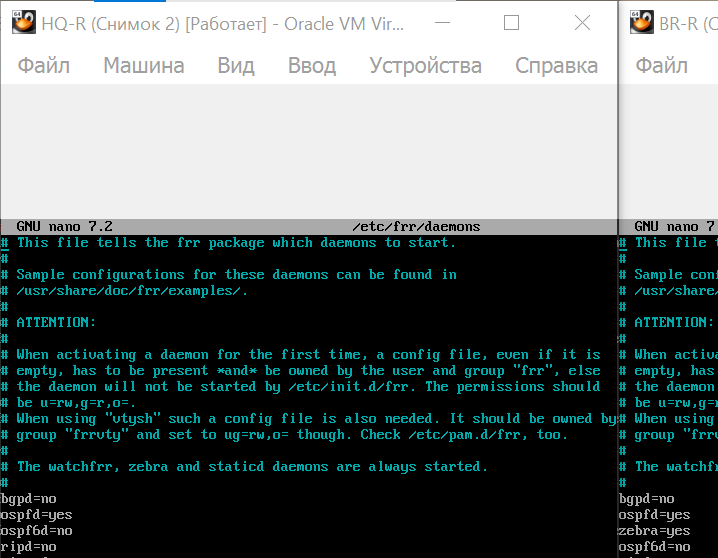




Включим демон ospf

Это необходимо сделать на HQ и BR

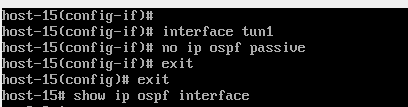
На ISP необходимо просто включить пересылку, отредачив файл /etc/net/sysctl.conf

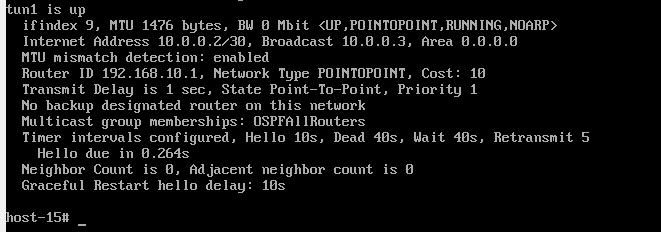


Настроим разрешение для пересылки маршрутов OSPF

Вот так должно выглядеть

Для этого





Теперь всё должно работать

В противном случае пробуйте systemctl restart NetworkManager network frr

Если не помогло проверьте работоспособность туннеля, если он рабочий, но маршрутов всё равно нет (их наличие проверяется командой ip route) то добавляйте соседей вручную

vtysh

#conf t

#router ospf

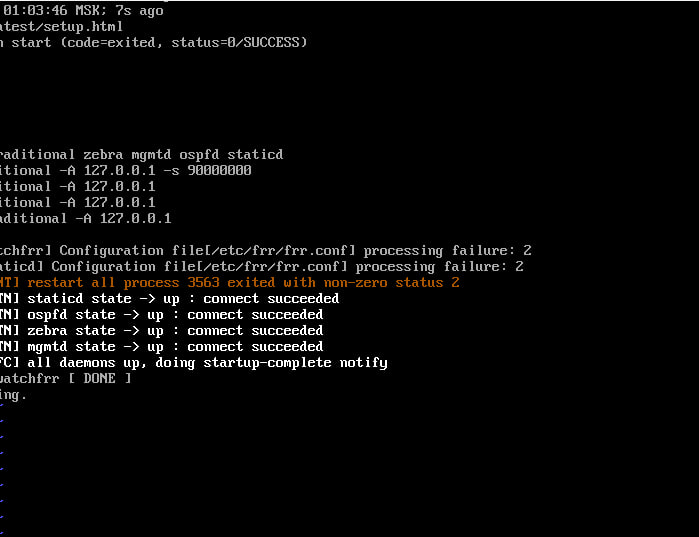
#neighbor *адрес соседнего роутера*

Если после этих команд не заработало ищите ошибку в конфигурационном файле /etc/frr/frr.conf, если ошибку не видите, то воcпользуйтесь journalctl и как только откроется журнал жмете либо до упора пробел, либо клавишу end.

Если в логах написана ошибка, которую исправить невозможно (вы исправляете, а она остаётся, то в таком случае настроить OSPF невозможно из-за лагов VB на экзамене зовите эксперта, вне экзамена жалуйтесь C.A.Показаньевой)

Примерно так может выглядеть ошибка, решение которой я не нашёл







**Настройка DHCP**:

[**ЧЁ**](#ЧЁ)

* Организуйте DHCP на HQ-RTR для офиса HQ:
  + Исключите из выдачи адрес маршрутизатора.
  + Укажите адрес сервера HQ-SRV как DNS-сервер.
  + Установите шлюз по умолчанию как HQ-RTR.
  + Добавьте DNS-суффикс au-team.irpo.

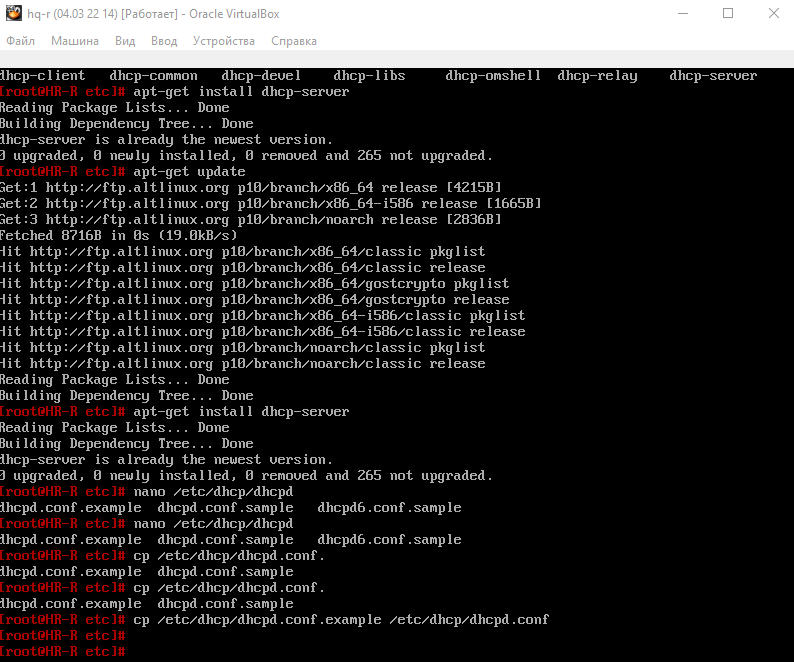
Для настройки понадобится скачать dhcp

Команда: apt-get install dhcp-server

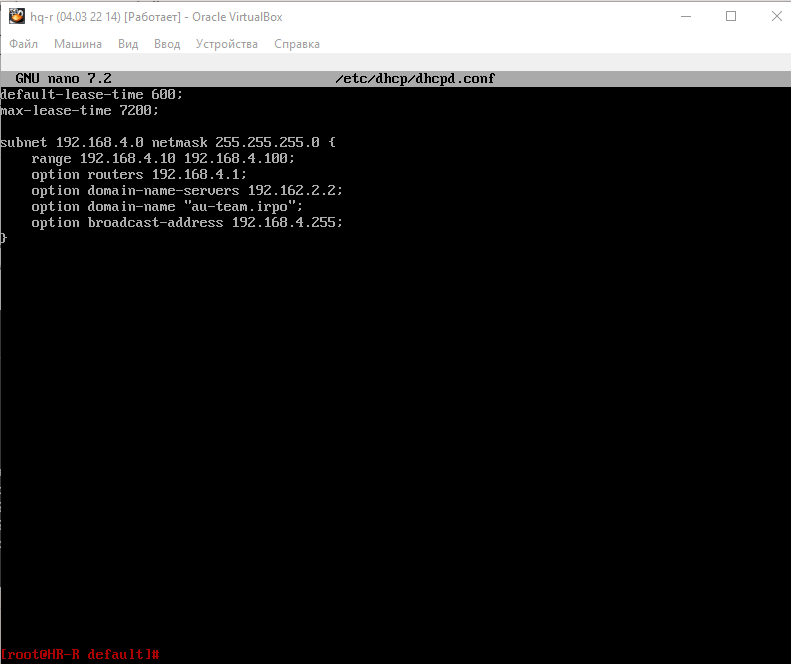
И нам нужен файл dhcpd.conf

Если его нет, стоит сделать

cp /etc/dhcp/dhcpd.conf.example /etc/dhcp/dhcpd.conf

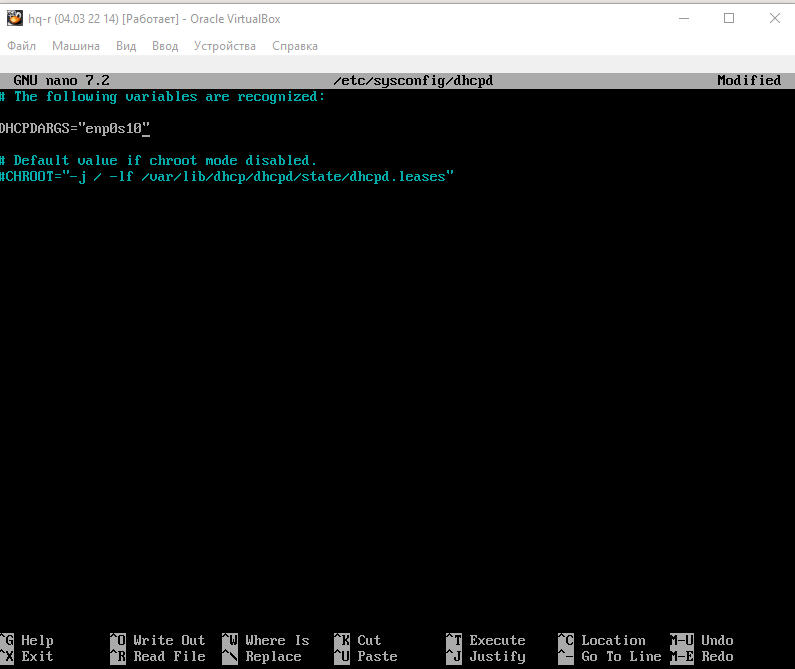


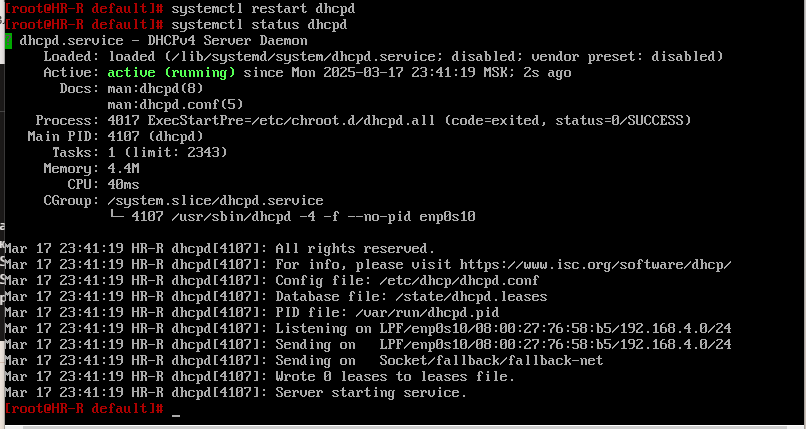
Перешли в файл dhcpd.conf и вносим изменения(содержимое можно удалить и заполнить чем нужно)



Присвоение интерфейса, на котором будет работать dhcp

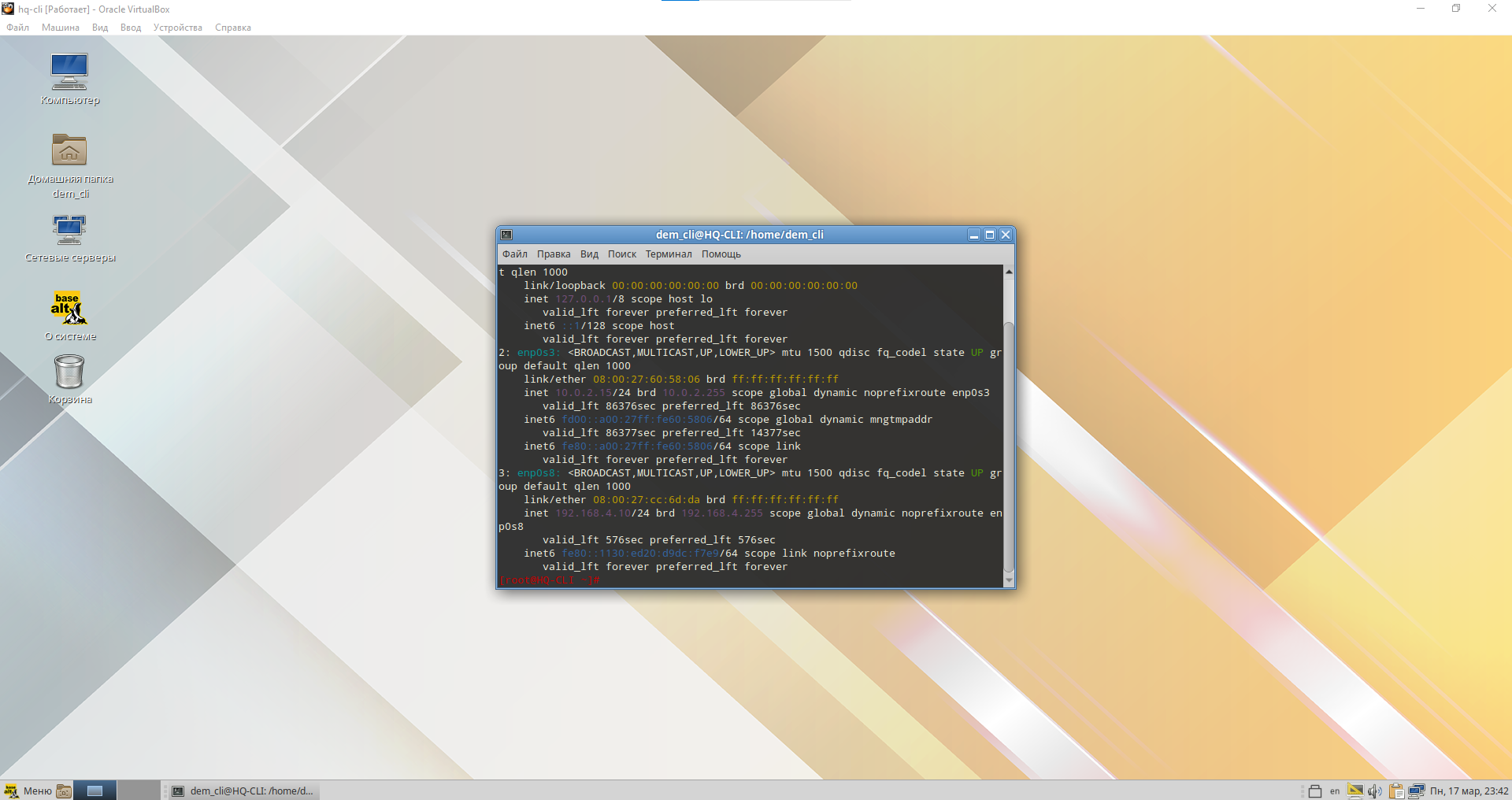
Откройте файл /etc/sysconfig/dhcpd





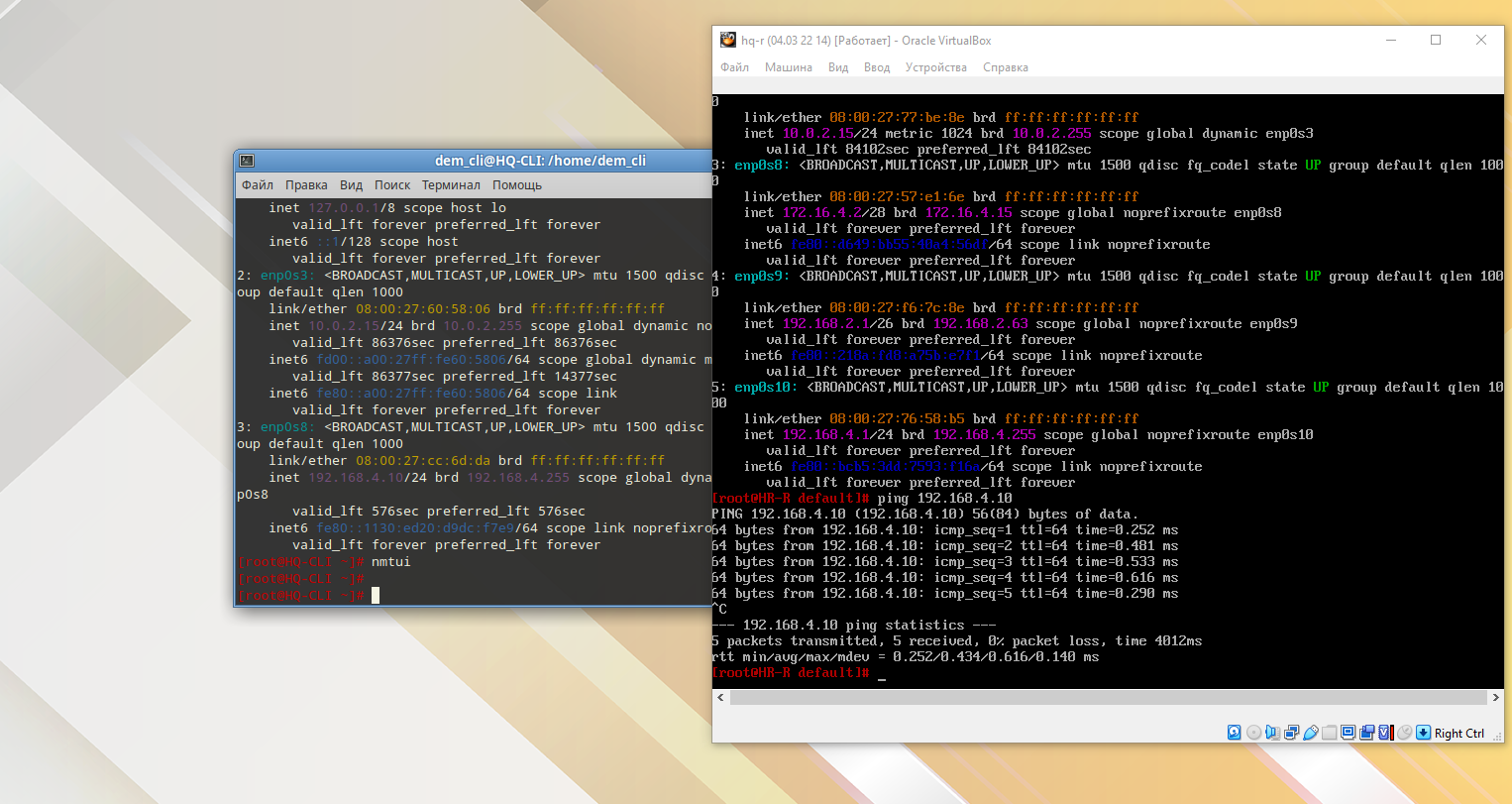
Если будет написано вместо active что либо другое, лезем в журнал, команда journalctl

Переходим на HQ-CLI и проверяем, раздался ли адрес



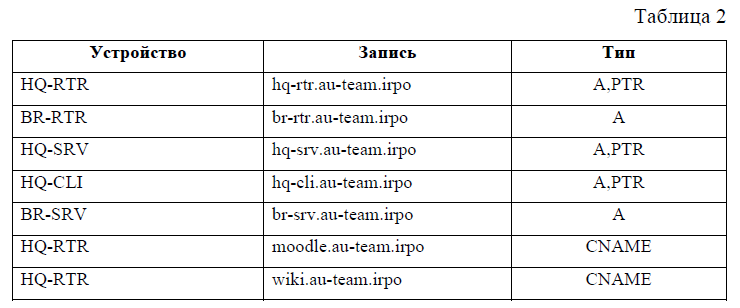
Видим, что да

И проверим ping



[Настройка DNS](#НАСТРОЙКА_DNS)

* Настройте HQ-SRV как DNS-сервер для офисов HQ и BR.
* Обеспечьте разрешение имён согласно таблице 2.
* Укажите общедоступный DNS-сервер в качестве пересылочного.

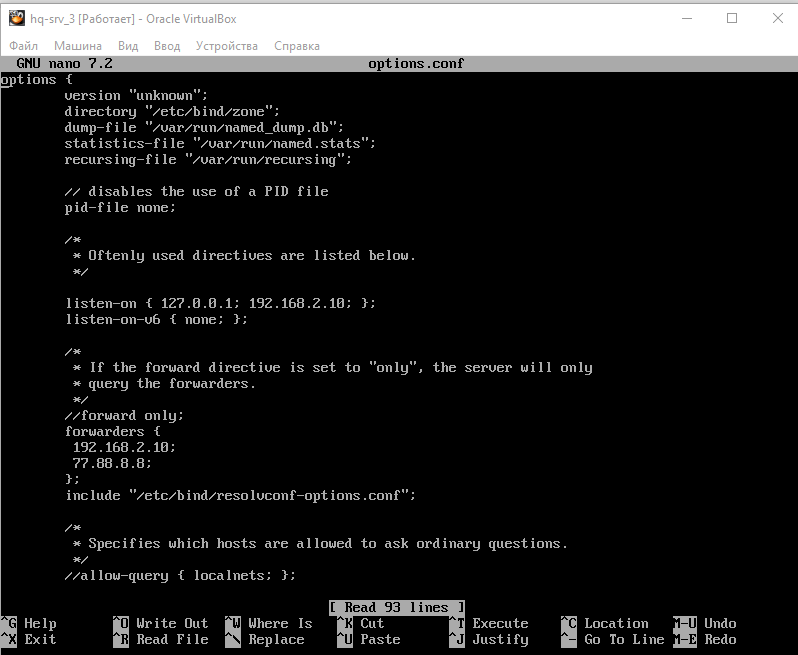


Устанавливаем bind на HQ-SRV apt-get install bind

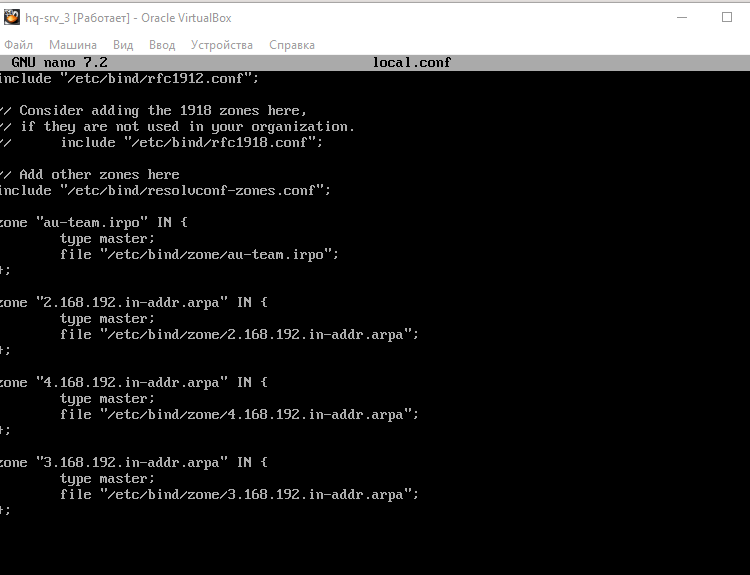
Создаем зоны

файл зоны прямого разрешения:

Изменение настроек в options conf



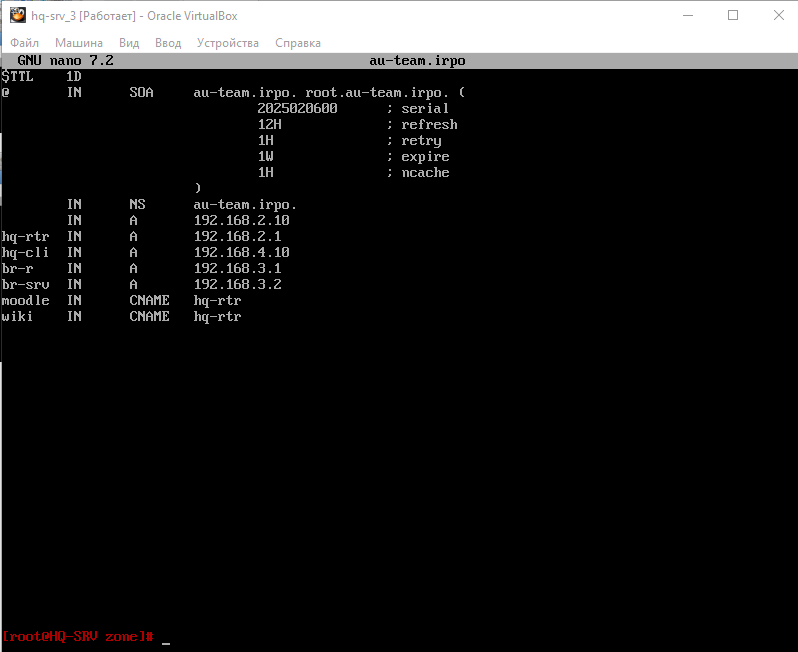
Оформление зон в bind



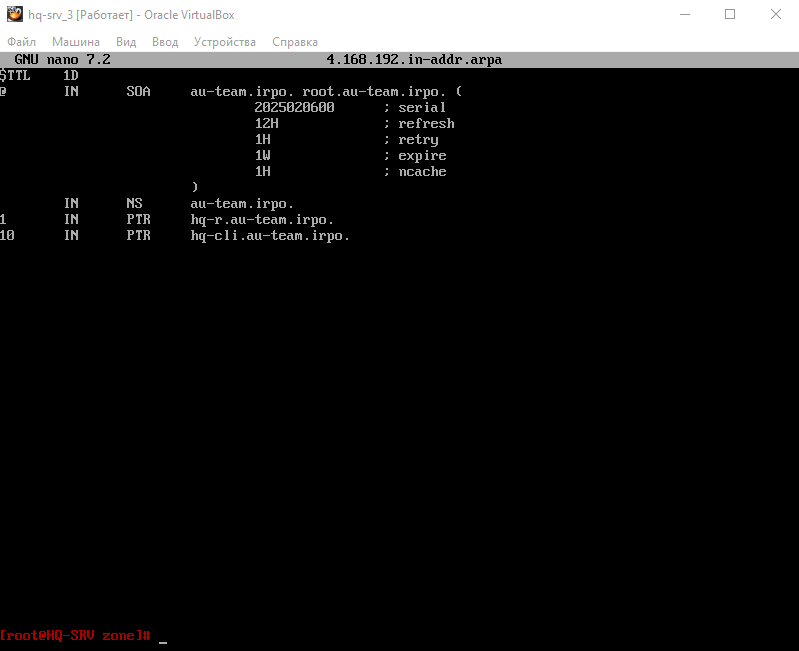
Создание файлов зон

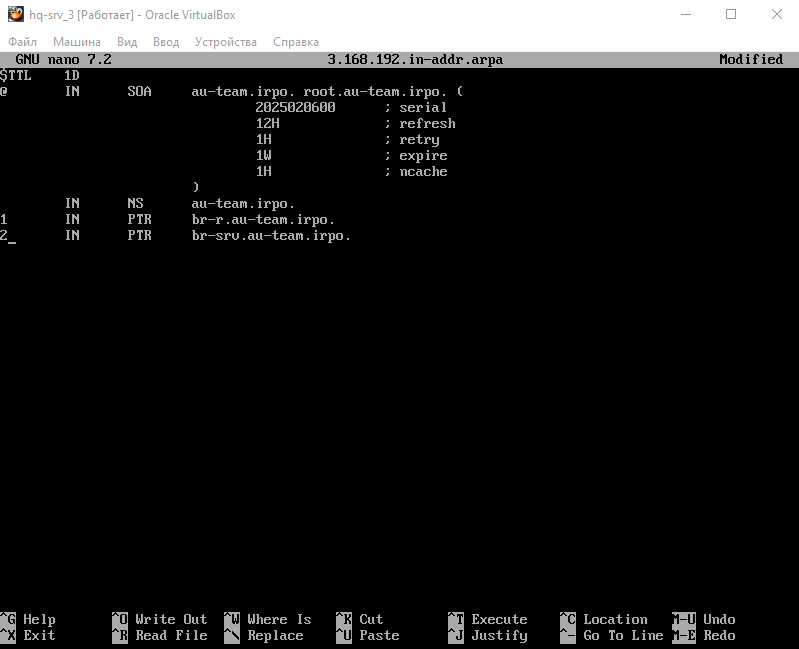


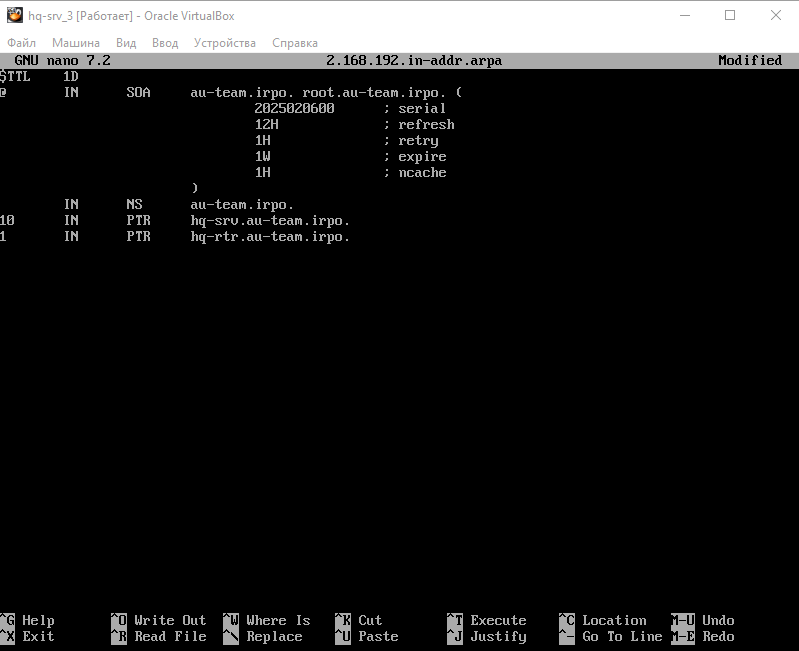
Прямая зона

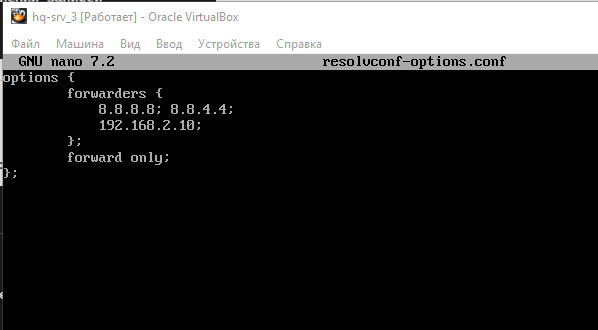


Создание обратных зон









**При настройке важно смотреть ваш текущий используемый dns**

**сat /etc/resolv.conf**

**Если там адрес не соответствует вашим желаниям, то редактируйте в файле**

**/etc/systemd/resolved.conf**

**Отключите dnssec**

**Раскоментируйте DNSsec и поставьте no**

**И установите параметр no на против dnstublistener**

**Так же раскоментировав строчку**

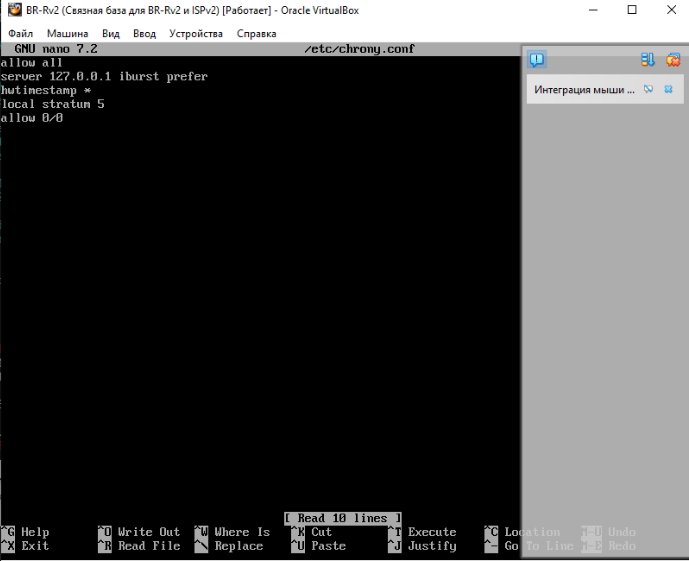
[Настройка часового пояса:](#Ten)

* Синхронизируйте все устройства с часовым поясом экзамена.

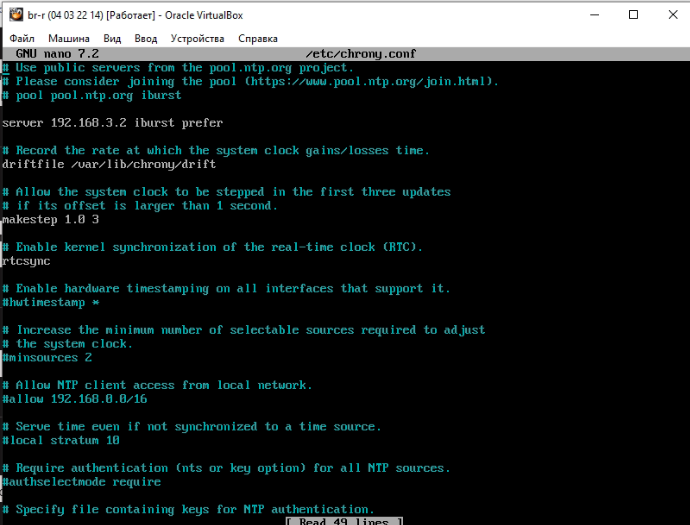
Будем синхронизировать с BR-SRV

Скачиваем chrony

apt-get install chrony



На клиент тоже скачиваем и прописываем в конфиге



Вписываем адрес устройства, с которым синхронизируется

[Ansible](#ansible)

apt-get install openssh

настройте вход по ключу

1)Откроем подключение на стандартный порт 22(port 22)

2)Будем использовать только ipv4 адресацию (AddressFamily inet)

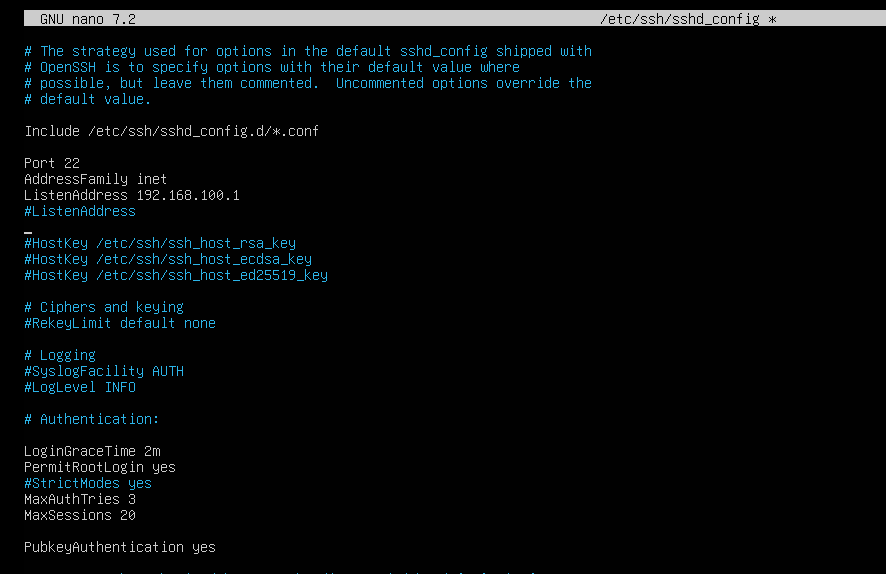
3)Разрешим подключение только на адрес из локальной сети (Listen address 192.168.100.1)

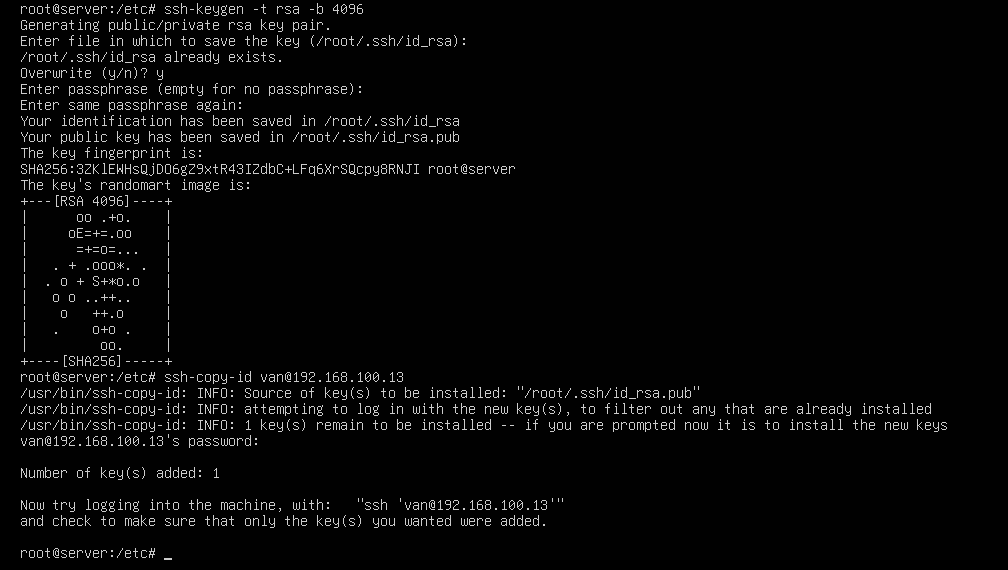
4)Оставим время аунтификации 2 минуты(LoginGraceTime)

5)разрешим вход для root

6)Количество попыток ввода пароля 3(MaxAuthTries)

7)Время ssh сессии 20 минут(MaxSession





Подобные манипуляции нужно проделать для каждой из машин что бы сделать полностью бесшовную связь по ssh.

Возьмём условно 2 машины br-srv и isp

Для того что бы сделать меж ними полностью бесшовную связь вам необходмо

1)ssh-keygen –t rsa –b 4096 (гинерация ключа)

2)ssh-copy-id –p 22 sshuser@172.16.5.1

-p 22 –указвает порт подключения, поэтому если вы в конфиге указали 2024 здесь так же пишите 2024.

sshuser –локальная учётка на которую мы копируем ключ, на неё же мы и будем подключатся по ssh.

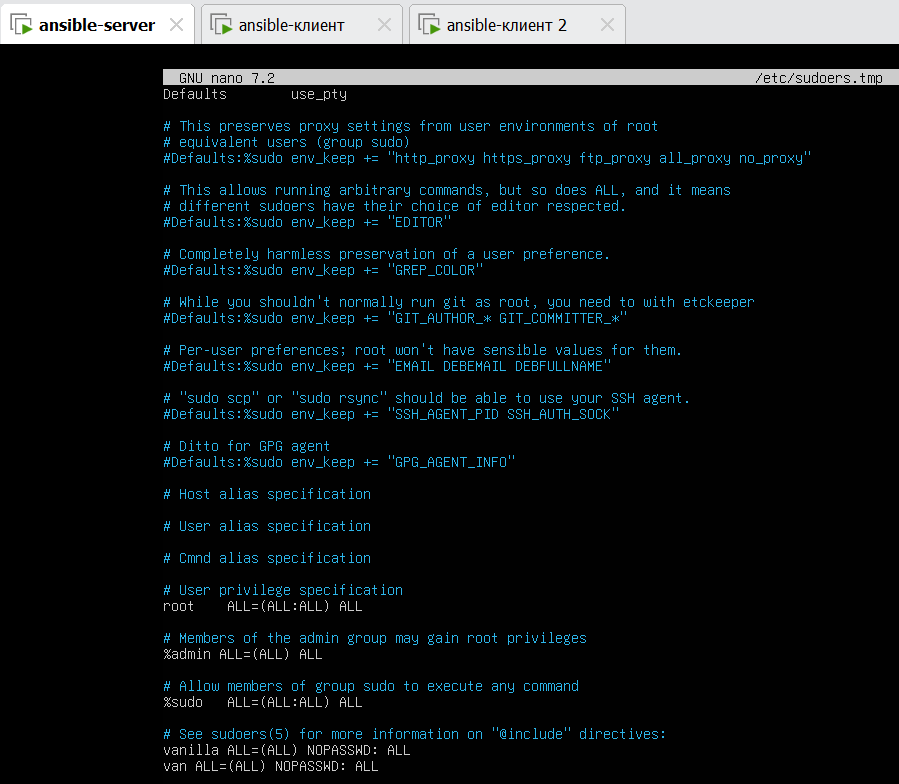
172.16.5.1 адрес машины на которую мы копируем ключ

КЛЮЧ ДОЛЖЕН БЫТЬ СГИНЕРИН НА ОБЕИХ МАШИНАЯ И ПРОБРОШЕН ДРУГ НА ДРУГА, например, с ISP НА И BR-SRV и с BR-SRV

на ISP.

С **каждой машиной** сот которой хотите получить пинг сделайте так же

Я не хочу подключатся с помощью учётной записи root, хочу исполнять плэйбук от имени учётной записи. Для этого на каждой из машин выдам исполнения команд sudo без пароля

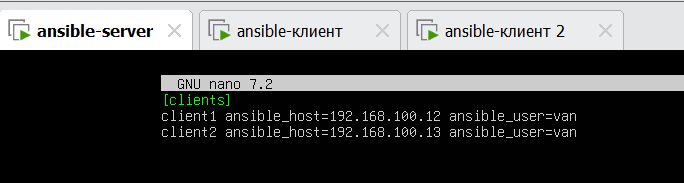


На этом моменте стоит быть аккуратнее, ибо может получится так что система зачтёт учётку рутовской и не пропустить вовремя аунтификации



Если здесь заменить 500 на 0 то может получится выше указанный случай

Теперь пропишем ansible клиентов. Я делал это в файле /etc/ansble/hosts



Введённые адреса написаны для примера

По факту каждая строчка будет выглядеть в стиле

isp ansible\_host=172.16.5.1 ansible\_user=sshuser

hq-r ansible\_host=172.16.4.2 ansible\_user=sshuser

br-r ansible\_host=172.16.5.2 ansible\_user=sshuser

cli ansible\_host=192.168.2.10 ansible\_user=sshuser

И попробуем с ними связаться



Связь прошла, а значит ssh настроен верно и связь для получения данный может быть установлена

Если вы всё сделаете, как написано и по всем канонам вам не понадобится писать playbook единственное изменение которое может вас постигнуть это изменение в команде в конце которой нужно будет добавить расположение файла hosts

ansible clients –m ping –I /etc/ansible/hosts

**Trable shutting**

Дорогой дневник, мне не передать боли и унижений, которые я испытал(а) сегодня работая с ALT Linux.

Опять сломался интернет на альте? Не работает днс? Не назначался адрес?

Хватит это терпеть!

Давайте вместе дадим отпор злу.

1. [Модуль 1](#Модуль_1)

ЧЁ ГДЕ ЕСТЬ Trable shutting

1. [Не назначался адрес](#НЕТ_АДРЕСА)
2. Нет интернета
3. [На клиенте из-за NAT](#Из_ЗА_NAT)

1. [На ISP](#НЕТ_ИНТЕРНЕТА)

1. [Не работает утилита](#УТИЛИТА)

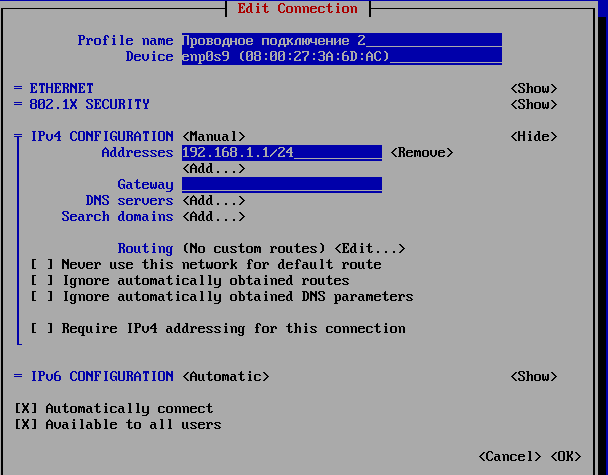
1. [Не работает Туннель](#тун1)

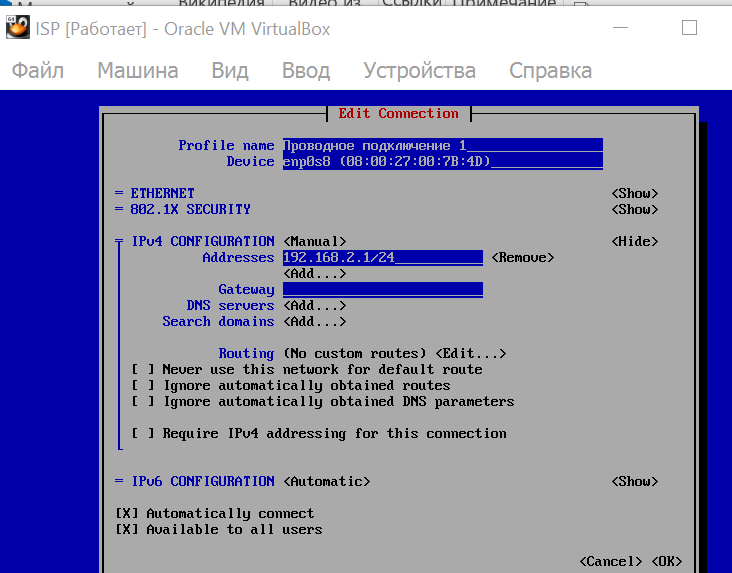
1. [ans](#iptables2)ible

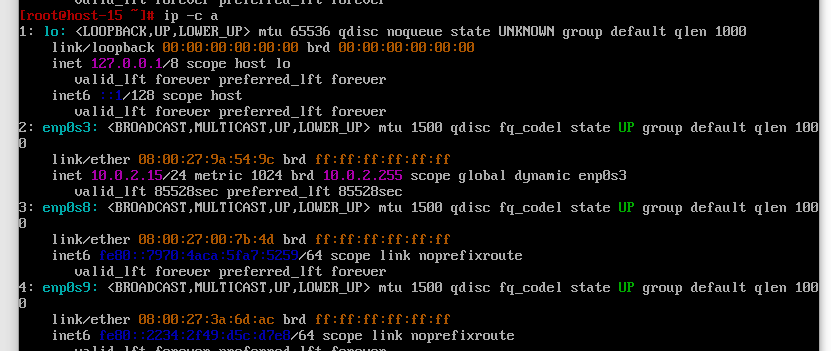
Нет адреса

[Trable shutting](#Trable_shutting2)

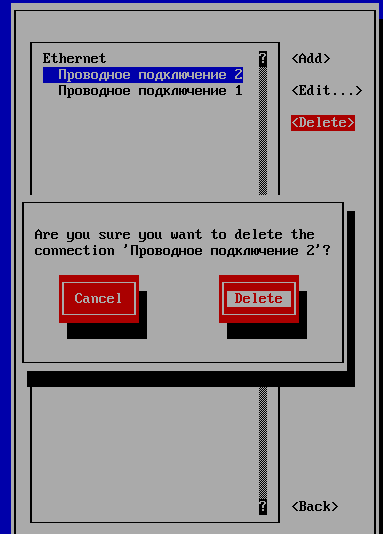
Описание ситуации: в nmtui адреса заданы, а при команде ip a они отсутствуют

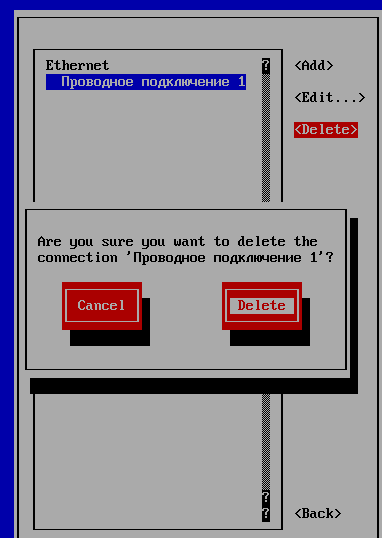




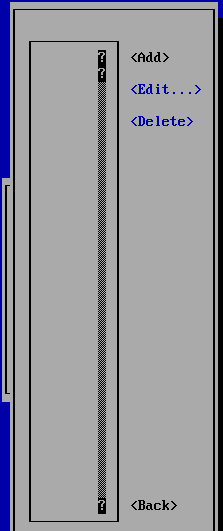


1)Удаляем адаптер

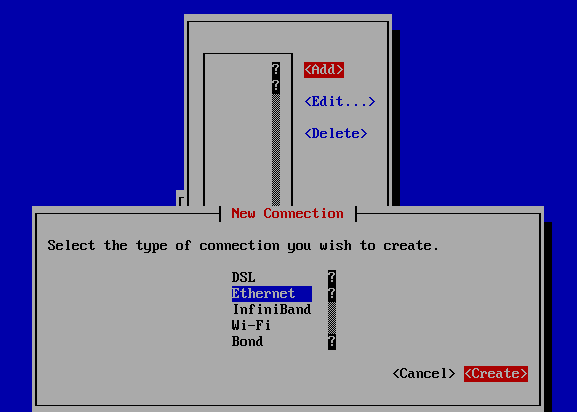


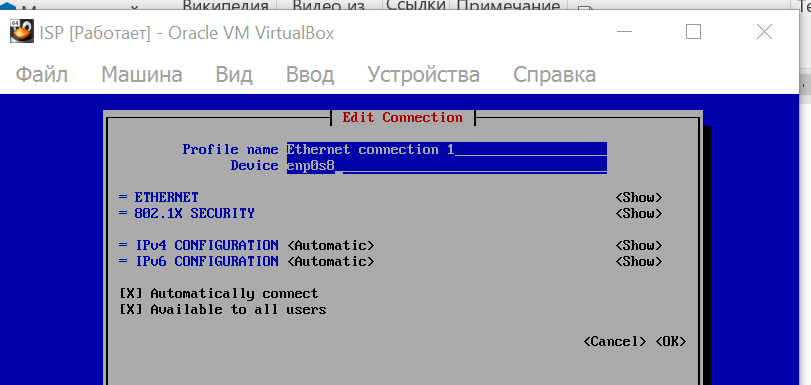
2) 

Получаем следующую ситуацию

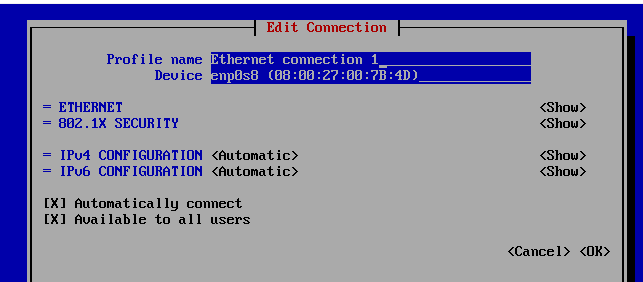


Теперь создадим интерфейс





Нажимаем ок и потом снова зайдём на интерфейс



Теперь задаём адреса и всё должно заработать.

В противном случае попробуйте

apt-get update

systemctl restart NetworkManager

systemctl reinstall NetworkManager

nmcli device down enp0s8

nmcli device up enp0s8

[Trable shutting](#Trable_shutting2)

[Нет интернета](#НЕТ_ИНТЕРНЕТА2)

Способ 1 выключить все интерфейсы и оставить только 1 NAT иногда помогает

Способ 2 Просмотрите /etc/resolv.conf

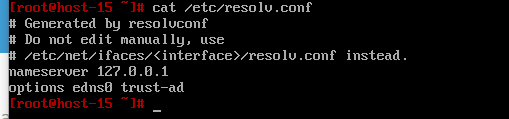
Там должно быть 1 или 2 dns адреса один из которых

77.88.8.8

А второй должен быть адресом вашего dns сервера в соответствии с заданием демо экзамена

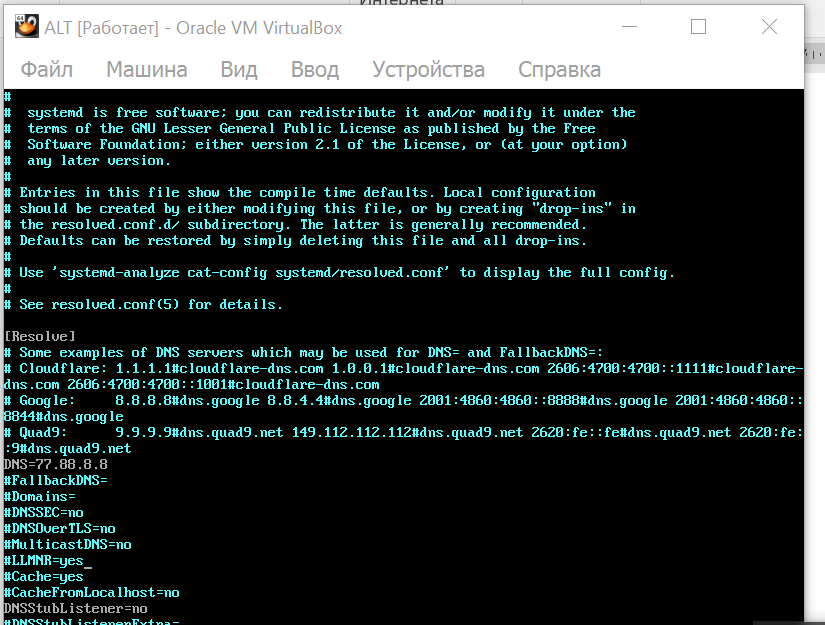
Итак посмотрим

Если мы видим следующе состояние /etc/resolv.conf

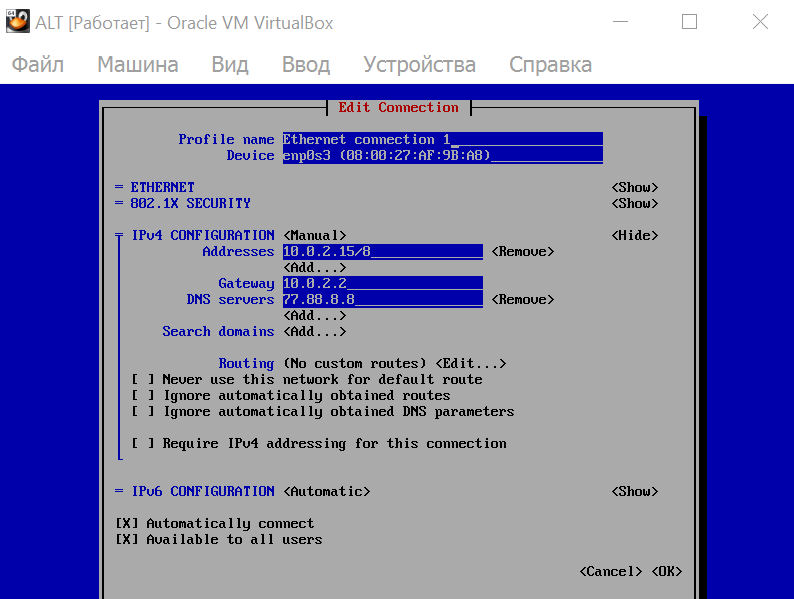


Или подобное

1)Открываем файл ./etc/systemd/resolved.conf

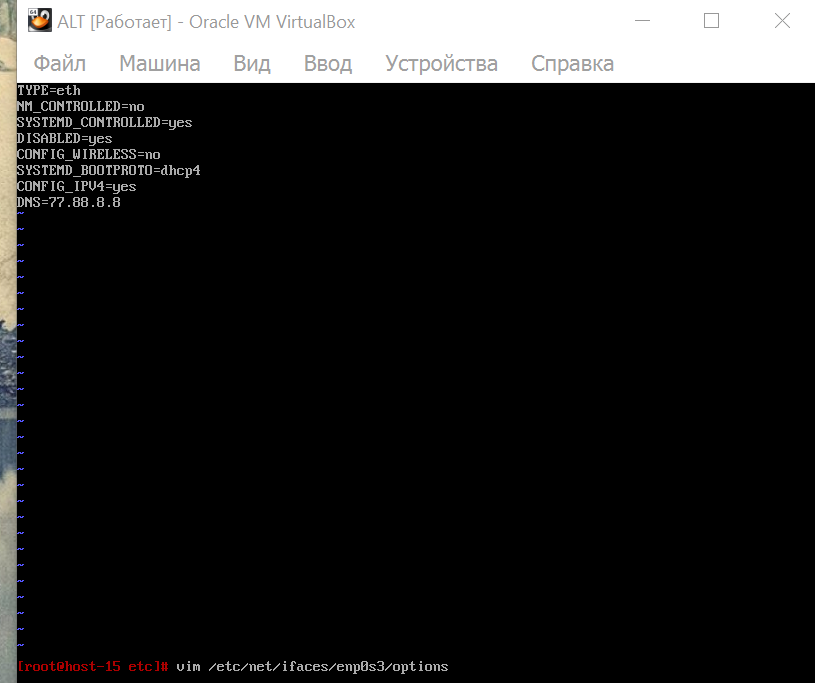


2)Выставим статику



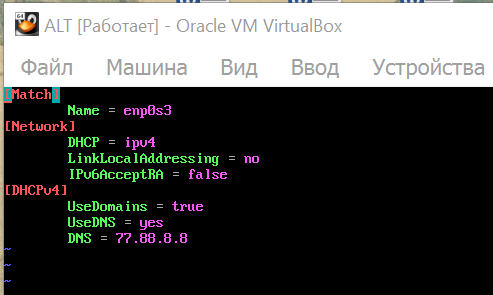
3)systemctl restart NetworkManager network sysytemd-resolved

4)можно исправить этот файлик



5) и на край





После этого должно заработать

Если нет попробуйте стереть файл /etc/resolv.conf именно стереть, а не удалить

После этого перезапустите сервисы

systemctl restart NetworkManager network sysytemd-resolved

если не помогло стоит позвать на помощь, хотя тут уже ничем не помочь

можно попробовать переустановить машину или откатиться к снимку, когда dns работал

на край можно перезапустить машину или вернуться к способу 1

+ ко всему systemctl restart NetworkManager network sysytemd-resolved

[Нет интернета](#НЕТ_ИНТЕРНЕТА2)

[На клиенте из-за NAT](#НА_ISP)

1)для начла проверьте dns на ISP

Если его нет проверьте предыдущий пункт

2)Если не помогло проверьте следующие пункты:

**НА СЕРВЕРЕ**

(Сервером считается машина, которая уже подключена к интернету) (Клиентом - машина, которую нужно выпустить в интернет через сервер)

Например

Если у нас есть интернет на ISP (интернет есть если мы можем сделать ping на ya.ru)

и хотим выпустить BR-R интренет, то срвером будет считаться ISP, а клиентом BR-R

nano /etc/net/sysctl.conf

net.ipv4.ip\_forward = 1

sudo sysctl -p

На редос sysctl -p /etc/sysctl.conf

На шлюзовой машине (на машине, подключённой к интернету)

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -A FORWARD -i enp0s8(интерфейс поключённый к машине, которую нужно выпустить в интернет)-o (интерфейс подключённый к интернету )enp0s3 -j ACCEPT

eth0 - интерфейс подключённый к интернету

**ПОЯСНИТЕЛЬНАЯ ЧАСТЬ**

-t nat:

Указывает, что команда применяется к таблице nat (Network Address Translation).

-A POSTROUTING:

-A — добавляет новое правило в указанную цепочку.

POSTROUTING — цепочка, которая обрабатывает пакеты после того, как они прошли маршрутизацию, но перед тем, как они покинут систему. Это идеальное место для настройки маскарадинга.

-o enp3s0:

-o — указывает исходящий интерфейс (output interface).

enp3s0 — имя интерфейса, потключённого к интернету

-j MASQUERADE:

-j — указывает действие, которое нужно выполнить с пакетом.

MASQUERADE — действие, которое подменяет исходный IP-адрес пакета на IP-адрес внешнего интерфейса (eth0). Это позволяет внутренним устройствам использовать один внешний IP-адрес для выхода в интернет.

**НЕОБЯЗАТЕЛЬНАЯ ЧАСТЬ**

сохраняем изменения iptables

sudo iptables-save

пробуем создать файлик и записать вывод команды в отдельный файлик

это прокатывает не всегда (команда выполняется из под директории etc)

mkdir iptables | touh iptables/rules.v4 | sudo iptables-save | tee /etc/iptables/reles.v4

создание папки | создание файла |сохранение правил| запись вывода в файл

**НЕОБЯЗАТЕЛЬНАЯ ЧАСТЬ ЗАКОНЧЕНА**

**НА КЛИНЕТЕ**

sudo ip route add default via 192.168.1.1(можно задать шлюз и по другому. 192.168.1.1 адрес шлюзовой машины)

Теперь можно отключить адаптер NAT и наслаждаться жизнью.

**КОМАНДЫ ОТКЛАДКИ**

systemct restart network NetworkManager,

иногда всё ломается и нужно прописать это сначало на сервере, а потом на клиенте.

Проверьте файл /etc/resolv.conf

если вы ещё не делали настройку dns сервера, то адрес вашего dns дожен быть 77.88.8.8

**Важно помнить, что описанные действия должны быть выполнены профессианалами и я не несу ответственности за ваши травмы.**

3)если снова не помогло проверьте ip route

Первым маршрутом должен быть маршрут в сторону ISP.

Если другой, то пропишите

ip route del default via “адрес в сторону ISP” enp0s.. “интерфейс написанный в выводе команды ip route”

теперь пропиши статику в сторону ISP

например, ip route add default via 192.168.1.1 dev enp0s8.

[Trable shutting](#Trable_shutting2)

[Не работает утилита](#Не_РАБОТАЕТ_УТИЛИТА)

1)переустановить apt-get reinstall “утилита”

2)Если ошибки в стиле файл короткий

То повторите команду и выведите ошибки в файл

1)nano txt.txt

2) apt-get reinstall “утилита” | tee txt.txt

Или apt-get reinstall “утилита” 2> txt.txt

или apt-get remove “утилита” и затем apt-get install “утилита” 2> txt.txt

3)Откройте файл в которой должны были записаться не установленные библиотеки в начало файла добавьте #! /bin/bash

4)уберите всё лишнее оставьте только названия библиотек

5)На следующую строчку после #! /bin/bash добавьте apt-get install

Сохрани файл как txt.sh

chmod +x txt.sh

теперь выполним

./txt.sh

[Не работает Туннель](#ТУН)

Туннель заводится всегда, даже когда не зводится всё остальное

Он может не установить связь из-за не настроенной ранее связности между роутреами BR-R и HQ-R, НА ЭТИХ РОУТЕРАХ ДОЛЖЕН БЫТЬ ОТКЛЮЧЁН NAT интерфейс ибо в таком слуае пакеты могут уходить на 10.0.2.15

Что бы посмотреть куда уходят пакеты, используйте команду

traceroutе *адрес*

Если вы верно проставили адреса в соответствии с mac адресами ваших сетевых карт и интерфейсами, которые прописали в nmtui у вас прежде всего должен появится ping от 172.16.4.2 до 172.16.5.2

Повторюсь, он должен ходить БЕЗ настроенной маршрутизации

Если вы столкнулись с такой ошибкой, что при использовании команды ping 172.16.4.2 на isp пакеты не уходят, но адресация настроена верно пишите команду traceroute 172.16.4.2 (на isp) она покажет куда ушли ваши пакеты и если они уходят на 172.16.5.1 и дальше звёздочки, то ошибка в ip route

Попробуйте удалить маршруты по типу

172.16.4.0 dev enp0s8 (ip route del 172.16.4.0 dev enp0s8)

172.16.5.0 dev enp0s9 (ip route del 172.16.5.0 dev enp0s9)

И задать их заново в соответствии с интерфейсами, которые уходят на br и hq

Команда ip route и далее по аналогии

После сделайте рестарт сети и если проблема осталась, то она не излечима и появилась скорее всего из-за глюков VirtualBox. НЕ ТЕРЯЙТЕ ВРЕМЯ ЗОВИТЕ ЭКСПЕРТА

[ansible](#iptables)

ошибка 1 permission denied

1)проверьте разрешение логиниться под определённым юзером

То есть если вы хотите допустим войти по ssh на сервер где в конфиге указано allowuser sshuser под root у вас хрен что получится

2)проверьте порт на который подключаетесь

Команда для копирования ключа

ssh-copy-id –p 2024 sshuser@172.16.5.1

этой командой вы скопируете ключ на пользователя sshuser на машине isp.

и после этого с машины isp будет доступ по ключу без пароля на машину на которой была вбита команда

3)если ключ не копируется или не гинерится, или есть другие проблемы, связанные с ключом зовите эксперта, на решение таких проблем можно потрать очень много времени ибо вариаций по котором это может происходить очень много.

[Trable shutting](#Trable_shutting2)