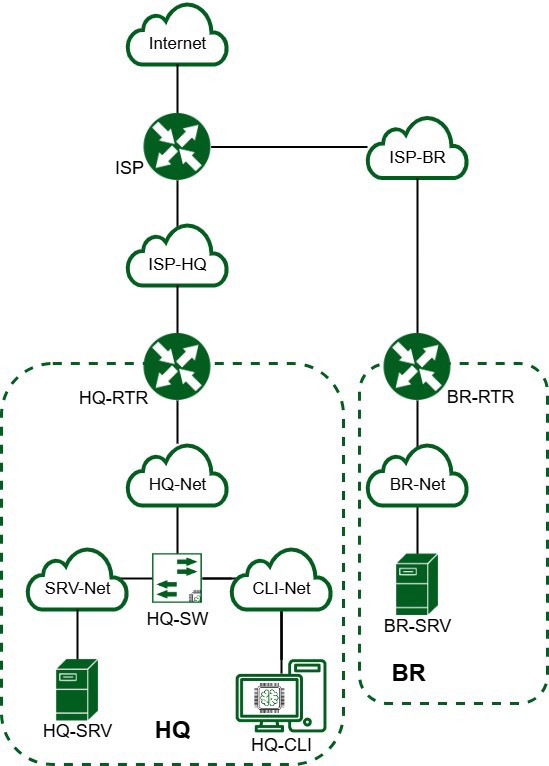
Разбор ДЭ 2025

**Сетевое и системное администрирование Модуль 1**



**Задание**

1. Произведите базовую настройку устройств
   * Настройте имена устройств согласно топологии. Используйте полное доменное имя
   * На всех устройствах необходимо сконфигурировать IPv4
   * IP-адрес должен быть из приватного диапазона, в случае, если сеть локальная, согласно RFC1918
   * Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов
   * Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 16 адресов
   * Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов
   * Локальная сеть для управления(VLAN999) должна вмещать не более 8 адресов
   * Сведения об адресах занесите в отчёт, в качестве примера используйте Таблицу 3
2. Настройка ISP
   * Настройте адресацию на интерфейсах:
     + Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP
     + Настройте маршруты по умолчанию там, где это необходимо o Интерфейс, к которому подключен HQ-RTR, подключен к сети 172.16.4.0/28
     + Интерфейс, к которому подключен BR-RTR, подключен к сети 172.16.5.0/28
     + На ISP настройте динамическую сетевую трансляцию в сторону HQ-RTR и BR-RTR для доступа к сети Интернет
3. Создание локальных учетных записей
   * Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV
     + Пароль пользователя sshuser с паролем P@ssw0rd
     + Идентификатор пользователя 1010
     + Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации.

* Создайте пользователя net\_admin на маршрутизаторах HQ-RTR и BR-RTR
  + Пароль пользователя net\_admin с паролем P@$$word
  + При настройке на EcoRouter пользователь net\_admin должен обладать максимальными привилегиями
  + При настройке ОС на базе Linux, запускать sudo без дополнительной аутентификации

1. Настройте на интерфейсе HQ-RTR в сторону офиса HQ виртуальный коммутатор:
   * Сервер HQ-SRV должен находиться в ID VLAN 100
   * Клиент HQ-CLI в ID VLAN 200
   * Создайте подсеть управления с ID VLAN 999
   * Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт
2. Настройка безопасного удаленного доступа на серверах HQ-SRV и BRSRV:
   * Для подключения используйте порт 2024
   * Разрешите подключения только пользователю sshuser
   * Ограничьте количество попыток входа до двух
   * Настройте баннер «Authorized access only»
3. Между офисами HQ и BR необходимо сконфигурировать ip туннель

* Сведения о туннеле занесите в отчёт
* На выбор технологии GRE или IP in IP

1. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.
   * Разрешите выбранный протокол только на интерфейсах в ip туннеле
   * Маршрутизаторы должны делиться маршрутами только друг с другом
   * Обеспечьте защиту выбранного протокола посредством парольной защиты
   * Сведения о настройке и защите протокола занесите в отчёт
2. Настройка динамической трансляции адресов.
   * Настройте динамическую трансляцию адресов для обоих офисов.
   * Все устройства в офисах должны иметь доступ к сети Интернет
3. Настройка протокола динамической конфигурации хостов.
   * Настройте нужную подсеть
   * Для офиса HQ в качестве сервера DHCP выступает маршрутизатор HQ-RTR.
   * Клиентом является машина HQ-CLI.
   * Исключите из выдачи адрес маршрутизатора
   * Адрес шлюза по умолчанию – адрес маршрутизатора HQ-RTR.
   * Адрес DNS-сервера для машины HQ-CLI – адрес сервера HQ-SRV.
   * DNS-суффикс для офисов HQ – au-team.irpo
   * Сведения о настройке протокола занесите в отчёт
4. Настройка DNS для офисов HQ и BR.
   * Основной DNS-сервер реализован на HQ-SRV.
   * Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 2
   * В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер
5. Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.

***Решение:***

# 1. ПРОИЗВЕДИТЕ БАЗОВУЮ НАСТРОЙКУ УСТРОЙСТВ И

**4. НАСТРОЙКА НА ИНТЕРФЕЙСЕ HQ-RTR В СТОРОНУ ОФИСА HQ ВИРТУАЛЬНОГО КОММУТАТОРА**

Настроим имена на всех устройствах полные доменные имена FQDN. Для этого используем команду *hostnamectl set-hostname FQDN*-*имя* из следующей таблицы

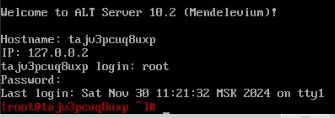
|  |  |
| --- | --- |
| **Устройство** | **FQDN устройства (полное доменное**  **имя)** |
| HQ-RTR | hq-rtr.ks54.net |
| BR-RTR | br-rtr.ks54.net |
| HQ-SRV | hq-srv.ks54.net |
| HQ-CLI | hq-cli.ks54.net |
| BR-SRV | br-srv.ks54.net |

Настроим машину на примере HQ-RTR, аналогично проделываем на BR-RTR, HQ-SRV, BR-SRV.

На машине HQ-CLI выполним настройку через графику.

**HQ-RTR**

Войдем в систему. Логин: **root**

Пароль: **toor** (при вводе он не отображается и символы не видны)

Меняем имя устройства и обновляем вход в bash:



Как видим имя изменилось в строке приветствия системы после команды exec bash

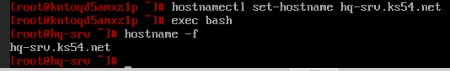
Командой *hostname –f*

Проделываем то же самое и на остальных устройствах кроме HQ-CLI:

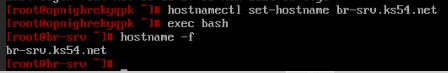
**BR-RTR**



**HQ-SRV**

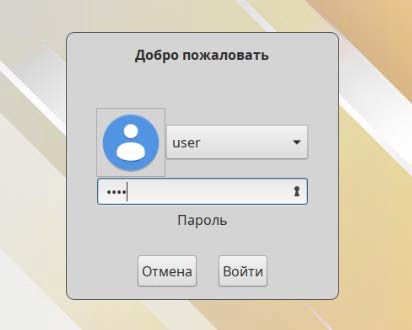


**BR-SRV**

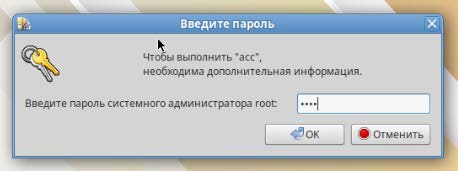
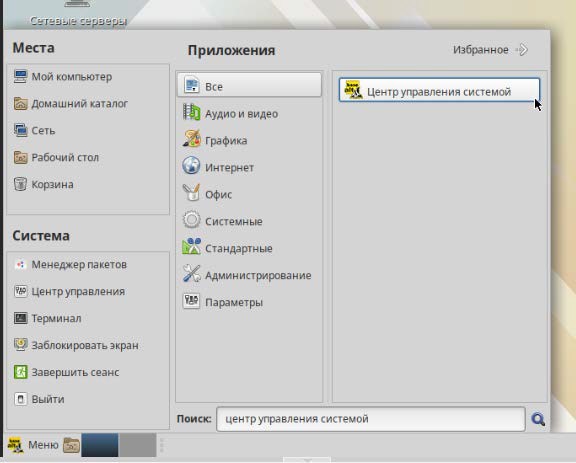


Настроим имя на машине **HQ-CLI**

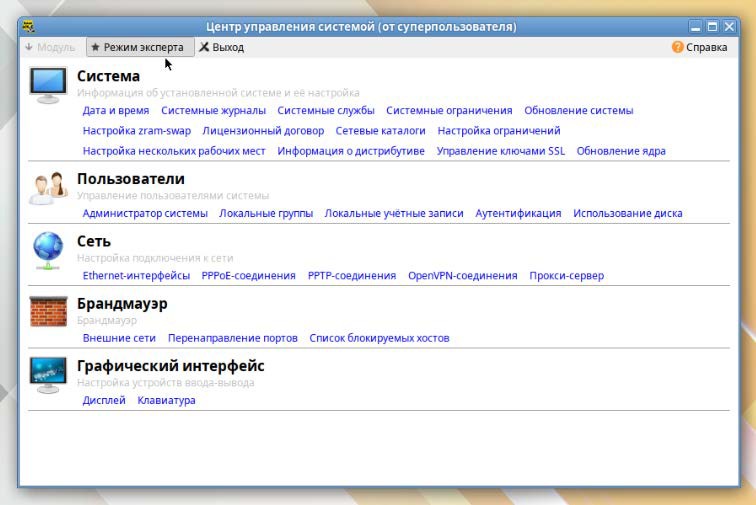
Войдем в графическую оболочку системы со следующим параметрами: Логин: **user**

Пароль: **resu**

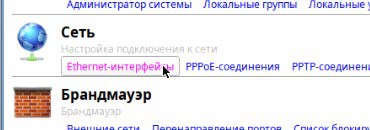
Далее находим в стартовом меню («пуск») программу «Центр управления системой», при запуске потребуется ввести пароль от суперпользователя: *toor*



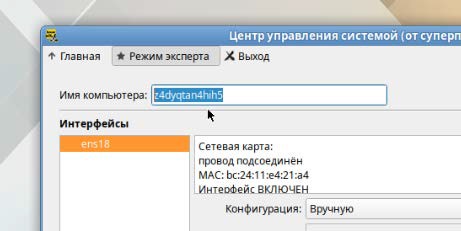
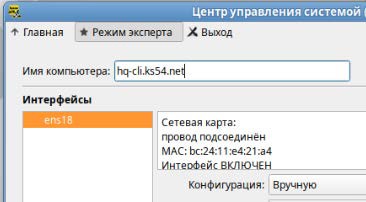
Получаем такое окно и нажимаем на режим эксперта



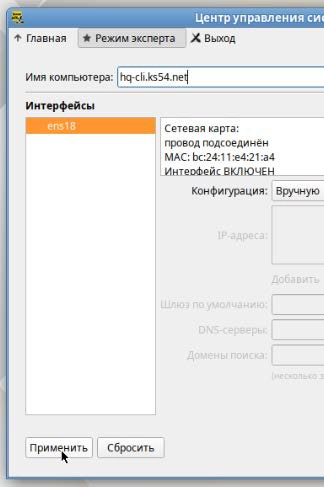
Выбираем Ethernet-интерфейсы



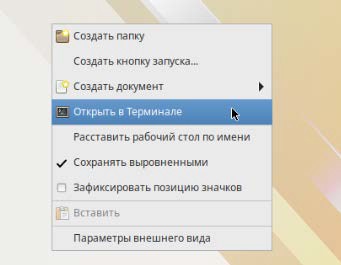
И меняем в появившемся окне имя машины на hq-cli.ks54.net

 **=> **

И нажимаем применить



Выходим из оснастки и запускаем эмулятор терминала, чтобы проверить присвоенное имя. Правой кнопкой мыши и открыть в терминале.



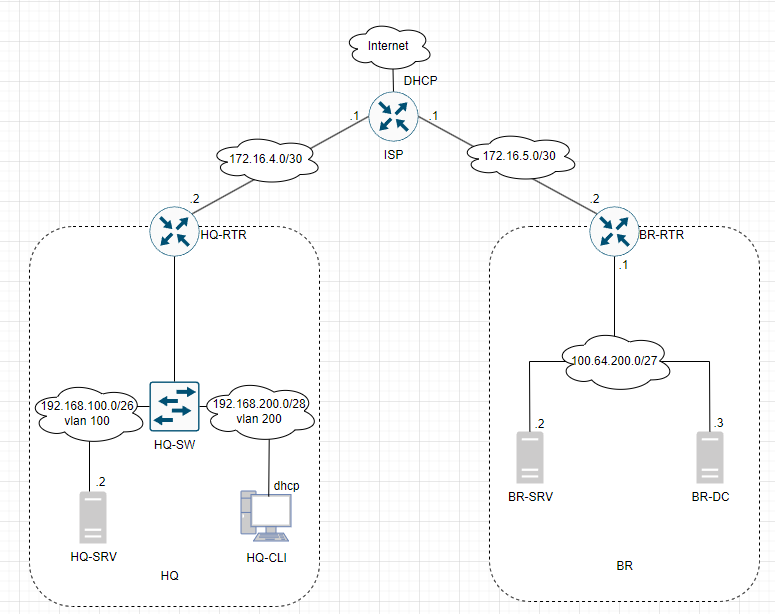
Увидим, что машине не переименовалась, даже после команды *exec bash* от лица суперпользователя. Поэтому делаем *reboot* системы и снова проверяем, и видим, что все выполнилось.



Перед настройкой IPv4 адресов необходимо сперва распределить адреса по всем интерфейсам. Сделаем такую таблицу по примеру Таблицы 3 из задания. (в нашем случае машина ISP пред настроена уже, там ничего менять не нужно)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска** | **VLAN** | **Подсеть** | **Шлюз** |
| **ISP** | ens18 (к  интернету) | DHCP | DHCP | - | DHCP | DHCP |
| ens19 (к HQ-  RTR) | 172.16.4.1 | 255.255.255.252 | - | 172.16.4.0/30 | - |
| ens20 (к BR-  RTR) | 172.16.5.1 | 255.255.255.252 | - | 172.16.5.0/30 | - |
| **HQ-RTR** | ens18 (к ISP) | 172.16.4.2 | 255.255.255.252 | - | 172.16.4.0/30 | 172.16.4.1 |
| ens19 (Trunk) | - | - | Trunk | - | - |
| ens19.100 | 192.168.100.1 | 255.255.255.192 | 100 | 192.168.100.0/26 | - |
| ens19.200 | 192.168.200.1 | 255.255.255.240 | 200 | 192.168.200.0/28 | - |
| ens19.999 | 192.168.3.1 | 255.255.255.248 | 999 | 192.168.3.0/29 | - |
| tungre (IP  туннель) | 10.10.10.1 | 255.255.255.252 | - | 10.10.10.0/30 | - |
| **HQ-SRV** | ens18 (Trunk) | - | - | Trunk | - | - |
| ens18.100 | 192.168.100.2 | 255.255.255.192 | 100 | 192.168.100.0/26 | 192.168.100.1 |
| **HQ-CLI** | ens18.200 | 192.168.200.2 | 255.255.255.240 | 200 | 192.168.200.0/28 | 192.168.200.1 |
| **BR-RTR** | ens18 (к ISP) | 172.16.5.2 | 255.255.255.252 | - | 172.16.5.0/30 | 172.16.5.1 |
| ens19 (к BR-  SRV) | 100.64.200.1 | 255.255.255.224 | - | 100.64.200.0/27 | - |
| tungre (IP  туннель) | 10.10.10.2 | 255.255.255.252 | - | 10.10.10.0/30 | - |
| **BR-SRV** | ens18 (к BR- RTR) | 100.64.200..2 | 255.255.255.224 | - | 100.64.200.0/27 | 100.64.200.1 |

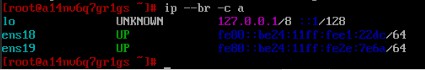
На основе данной таблицы сделаем схему для более наглядного представления структуры сети



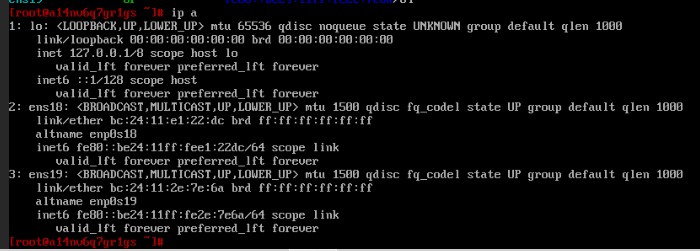
Теперь настроим адресацию на всех машинах.

# HQ-RTR

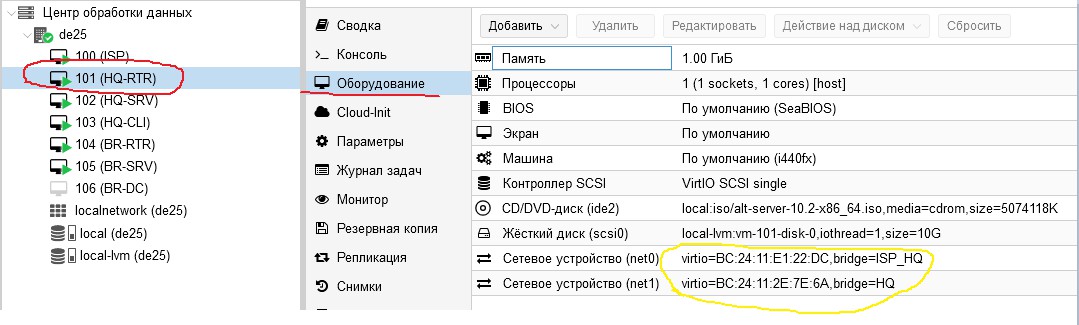
Проверим какие интерфейсы активны в окружении системы с помощью команды *ip --br -c a*



Для более подробного отображения информации о сетевых параметрах интерфейсов можно использовать команду *ip a*



Необходимо соотнести MAC-адреса интерфейсов и понять куда какой интерфейс смотрит. Для это сравниваем эти параметры из самой системы и из свойств соответствующей виртуальной машины на стенде.



Зайдем в директорию интерфейсов и настроим их. Первый интерфейс ***ens18*** смотрит в сторону машины ISP, ***ens19*** – транковый порт, разделяющийся на VLANы для HQ-SRV и HQ-CLI, следовательно, навешиваем на них соответствующие параметры:

***ens18:***

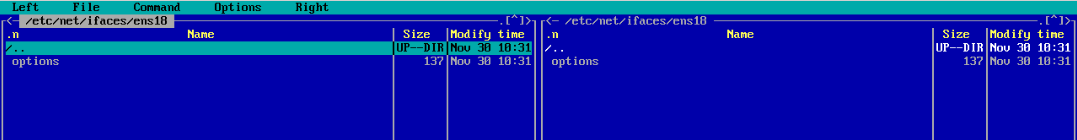


проверяем какие файлы имеются в папке интерфейса, для этого пишем либо ***ls***

***,***

либо запускаем миднайт командер командной ***mc***





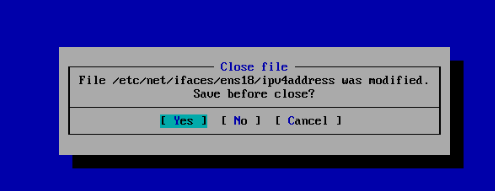
Для выхода можно используем клавишу F10.

Создадим в этой папке файл, отвечающий за подтягивание параметров ipv4-конфигурации на данный интерфейс в систему. Для этого есть несколько способов:

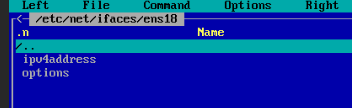
1. echo 172.16.4.2/30 > ipv4address
2. mcedit ipv4address



затем вписать 172.16.4.2/30, нажать F10 и подтвердить сохранение параметров.



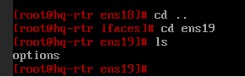
Проверяем, что появился файл ipv4address через ***ls*** или ***mc***

 или  Также можно прописать ссылку на DNS сервер, чтобы в будущем наша машина могла стучаться до сети Интернет. Для этого в этой же папке создаем файл ***resolv.conf*** со следующим содержимым: ***nameserver 77.88.8.8***.

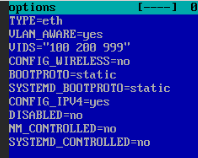
Аналогично создаем файл со шлюзом по умолчанию на ISP.



Теперь настроим остальные интерфейсы. Перейдем в папку интерфейса ***ens19.*** Либо командой из текущего каталога ***cd ..*** далее ***cd ens19****,* либо через переход по полному пути ***cd /etc/net/ifaces/ens19/*** и проверим содержимое этой папки

 или 

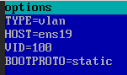
Настроим интерфейс в транковый режим и создадим виртуальные интерфейсы как по таблице. Для этого отредактируем файл ***options*** в интерфейсе ens19 и приведем к следующему виду:



Создадим папки с подинтефейсами в директории **/etc/net/ifaces/**, которые будут работать, используя мощности и пропускную способность физического интерфейса ens19.



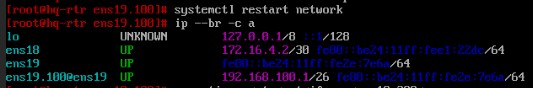
Создадим файл ***options*** и ***ipv4ddress*** в каждой созданной папке



А также навесим ipv4-адрес на этот интерфейс:



Для проверки сделаем рестарт сетевых параметров и проверим ip-конфигурацию

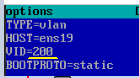


Далее скопируем созданные файлы для ens19.100 для остальных подинтерфейсов и отредактируем по необходимым параметрам.



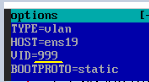
Отредактируем файлы: Для ***ens19.200***



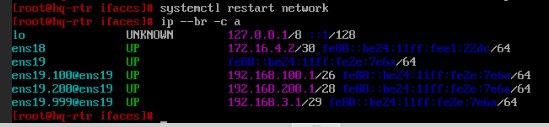


Для ***ens19.999***

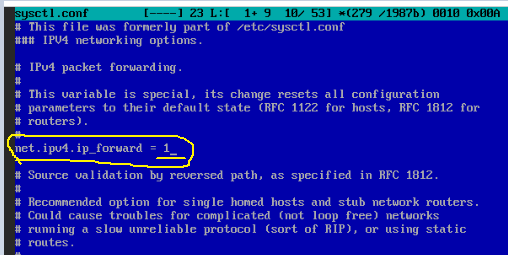




Делаем рестрат сетевых параметров и проверяем ip-конфигурацию



Для пересылки пакетов между подсетями включим forwarding на машине.



# HQ-SRV

Проверим интерфейсы в системе

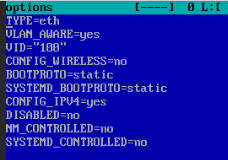


Настроим интерфейс в транковый режим и создадим виртуальные интерфейсы как по таблице.

Для этого отредактируем файл ***options*** в интерфейсе ens18



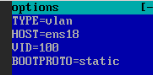
и приведем к следующему виду:



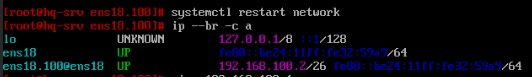
Создадим папку с подинтефейсом, который будут работать на физическом интерфейсе ens18.



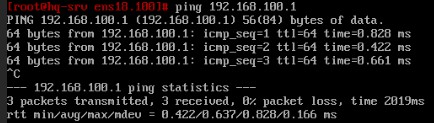
Настроим этот интерфейс



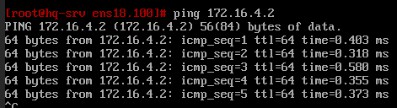
Сделаем рестарт сетевой конфигурации и проверим адресацию



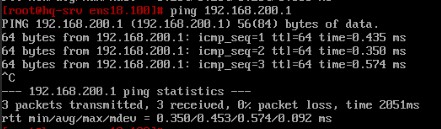
Проверим доступность ближайшего интерфейса роутера HQ-RTR



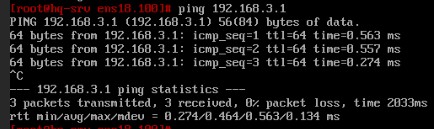
Как видим есть базовая сетевая связанность с роутером. Мы можем простучать и интерфейс роутера, который смотрим в ISP за счет форвардинга.



И второй виртуальный интерфейс с VLAN200



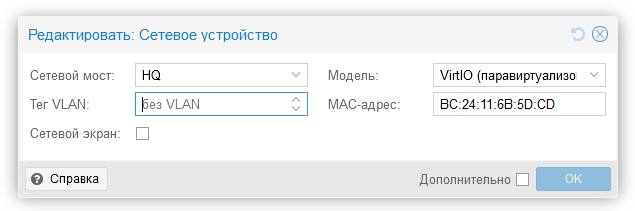
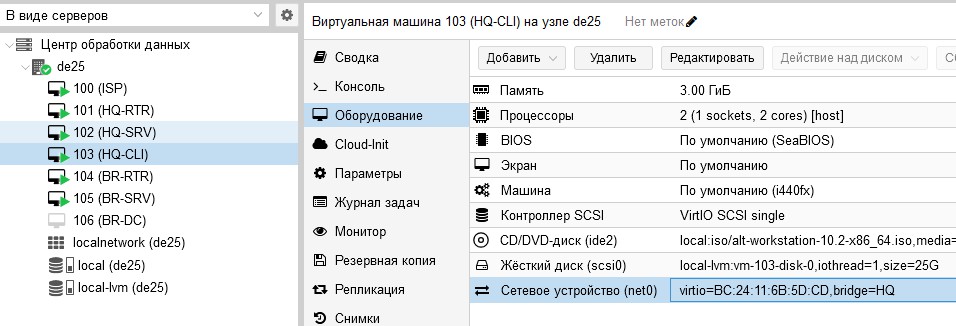
И vlan999

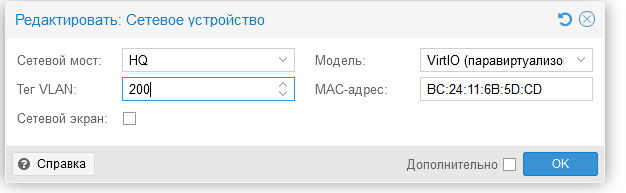


# HQ-CLI

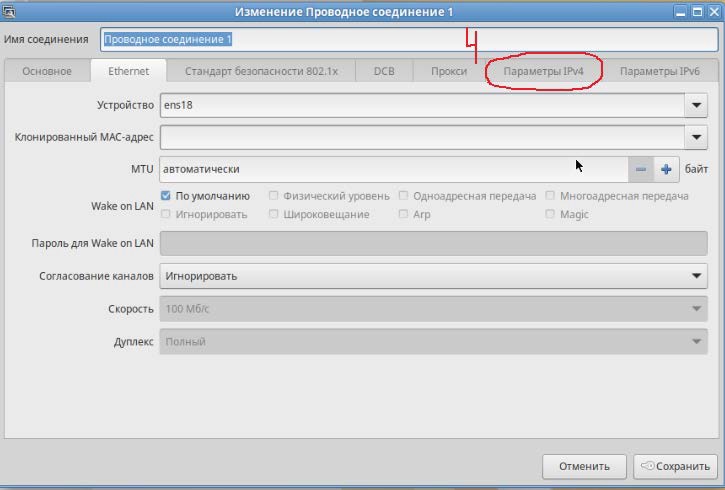
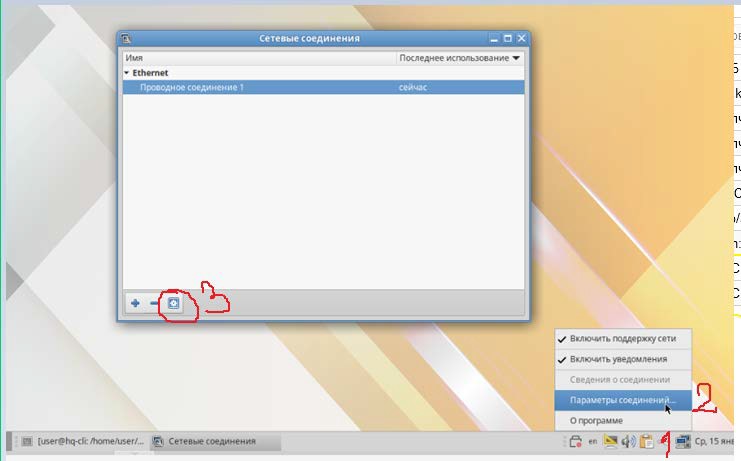
По заданию дальше адресация для данной машины должна выдаваться автоматически, но для теста, настроим адресацию статически, дальше, когда будет поднят сервер DHCP, тогда установить автоматическое получение адреса.

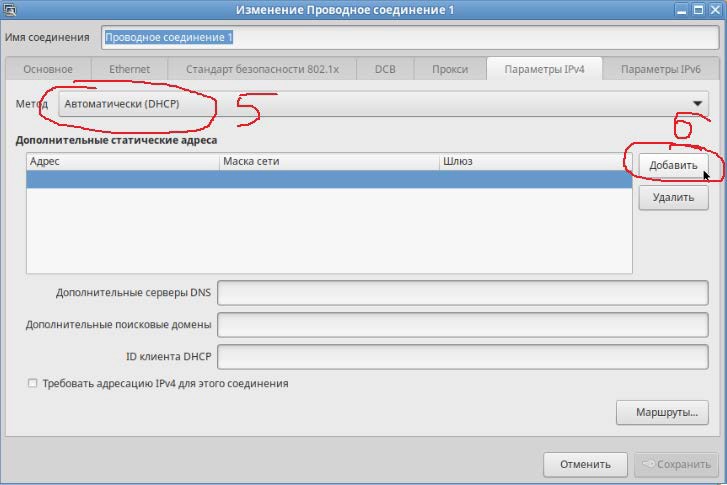
Для начала нам необходимо на интерфейсе в настройках оборудования машины выставить разрешение влана 200. Для этого не будем использовать виртуальный подинтерфейс, а используем второй способ – в свойствах виртуальной машины в оборудовании находим сетевую карту, кликаем дважды и в параметре VLAN выставляем значение 200.



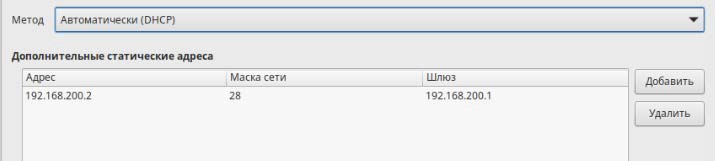


Далее в настройках адаптера выставляем нужные параметры:

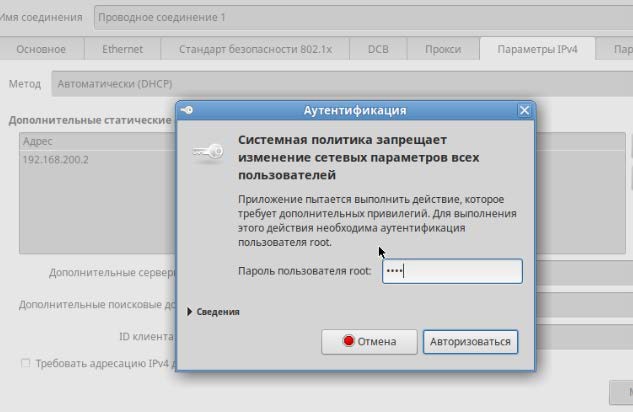




И прописываем айпи из таблицы, которая приведена в начале.

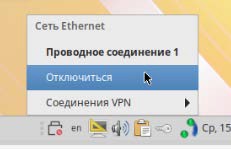
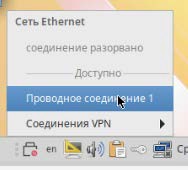


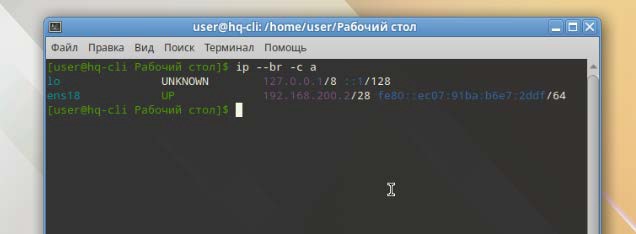
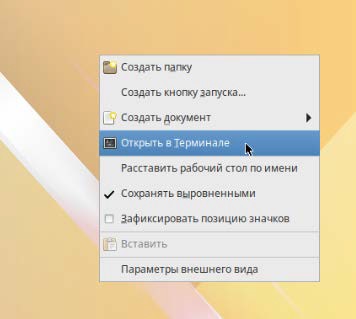
Нажимаем сохранить и вбиваем пароль ***toor***



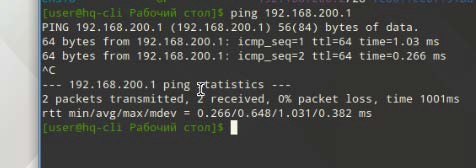
Далее применим полученные параметры отключив и включив адаптер через апплет в строке меню.

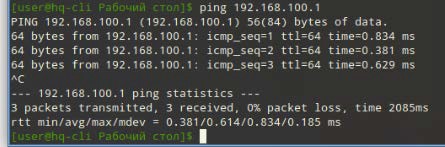
Левой кнопкой мыши щелкаем на апплет, нажимаем отключиться, затем тоже самое и выбрать проводное соединение. Он начнет грузить подключение, не подтверждая успешное подключение (так как у нас остался параметр получать айпи по DHCP), но мы можем удостовериться, что параметры применились, зайдя в консоль и вбив ip –br –c a.

 **=> **



Проверяем сетевую связанность клиента с роутером HQ-RTR



Также доступны и другие интерфейсы на роутере

***НО как только в трее апплет перестанет грузится и выдаст недоступное подключение, параметры сети сбросятся, так как у нас стоит параметр получать по DHCP. Можно на время поставить статический адрес, но потом не забудьте изменить его на DHCP, когда поднимите сервер DHCP.***

# BR-RTR

Настроим айпи конфигурацию для роутера аналогично HQ-RTR, за исключением подинтерфейсов.

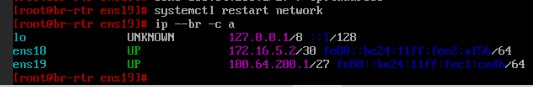
## Настройка ens18 смотрящего в сторону ISP



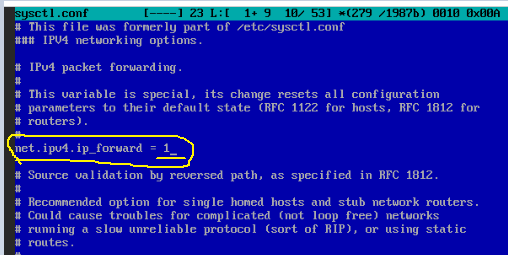
**Настройка ens19 в сторону BR-SRV**



Делаем рестарт сети и проверяем конфигурацию

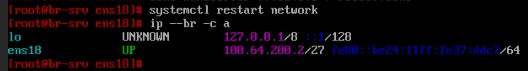
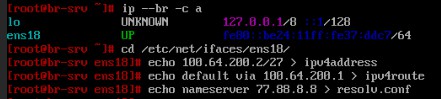


Для пересылки пакетов между подсетями включим forwarding на машине.



# BR-SRV

Аналогичным способом настраиваем конфигурацию сети



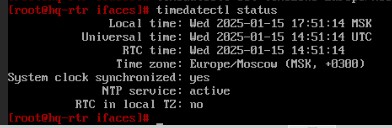
# ​НАСТРОЙКА ЧАСОВОГО ПОЯСА НА ВСЕХ УСТРОЙСТВАХ

Настройка производится встроенной службой, настроим зону на **HQ-SRV** следующей командой:

## timedatectl set-timezone Europe/Moscow

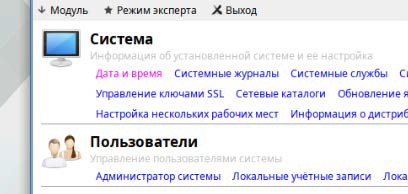
Настроим на примере HQ-RTR

Проверим командной **timedatectl status**

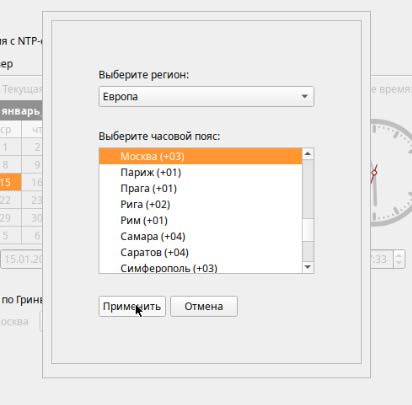
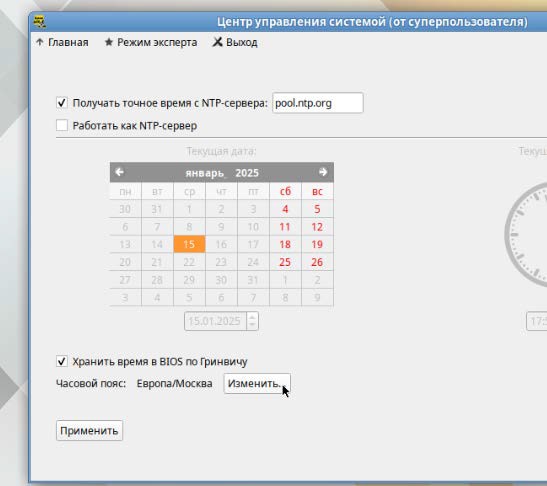


Аналогично проделываем на всех машинах без графики. На HQ-CLI можно выполнить также в терминале данную команду, либо через центр управления в графическом режиме выбрать таймзону.

Для это в стартовом меню выбираем Центр управления системой (или вбиваем в поисковой строке

**acc**), затем вбиваем пароль от суперпользователя **toor,** выбираем в разделе системы **Дата и время**

Нажимаем внизу **Изменить** и проверяем, что установлено Европа/Москва



И нажимаем применить параметры.

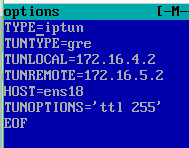
# ​НАСТРОЙКА IP-ТУННЕЛЯ МЕЖДУ ОФИСАМИ HQ И BR:

Создание туннеля производится на маршрутизаторах **HQ-RTR** и **BR-RTR**. **HQ-RTR:**

По аналогии с созданием подинтерфейсов для VLANов создается папка для виртуального интерфейса **tungre** и создаем файл **options**



со следующим содержимым



Навешиваем ip-адрес на интерфейс



Включаем **модуль gre**



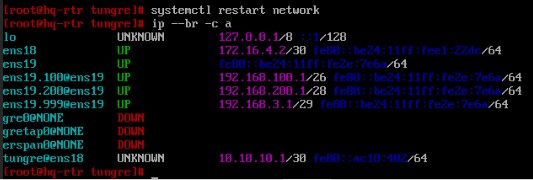
Сохраняем:



На выходе получим сообщение



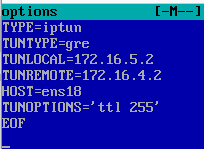
Перезапускаем сетевые службы и проверяем ip-конфигурацию, что появился туннель



# BR-RTR:

Аналогичным образом настраиваем туннель с обратной стороны, только поменяв значения

TUNLOCAL и TUNREMOTE.



Навешиваем адрес



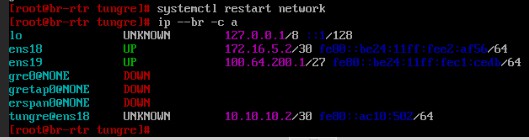
Включаем модуль



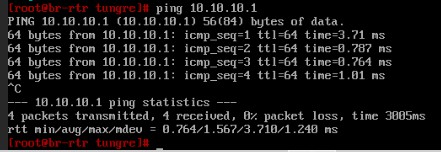
Сохраняем загрузку этого модуля и смотрим вывод



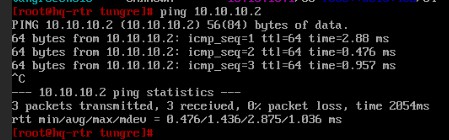
Перезапускаем службу и проверяем конфигурацию



Протестируем работу нашего тоннеля



Перейдем на HQ-RTR и сделаем ping



Туннель работает

# 8. НАСТРОЙКА ДИНАМИЧЕСКОЙ ТРАНСЛЯЦИИ АДРЕСОВ NAT

Настроим NAT на роутерах HQ-RTR и BR-RTR

# HQ-RTR:

Сделаем трансляцию адресов с помощью iptables.

Введем правила для трансляции подсетей во внешнюю сеть

## iptables –t nat –A POSTROUTING –s 192.168.100.0/26 –o ens18 –j MASQUERADE iptables –t nat –A POSTROUTING –s 192.168.200.0/28 –o ens18 –j MASQUERADE iptables –t nat –A POSTROUTING –s 192.168.3.0/29 –o ens18 –j MASQUERADE



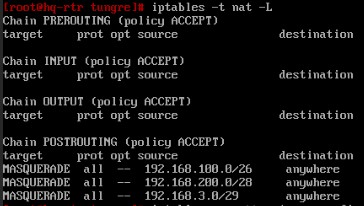
Сохраним правила и поставим сервис в автозагрузку системы

## iptables-save >> /etc/sysconfig/iptables systemctl enable -- now iptables.services

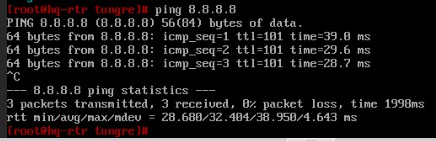


Для проверки введенных правил вбиваем команду

## iptables –t nat -L



Проверяем доступ в интернет



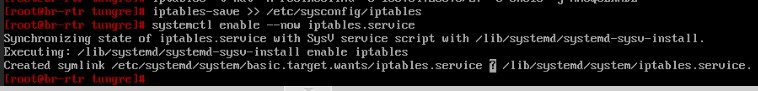
# BR-RTR:

Выполняем аналогично по тому же принципу, но с другими данными Введем правила для трансляции подсетей во внешнюю сеть

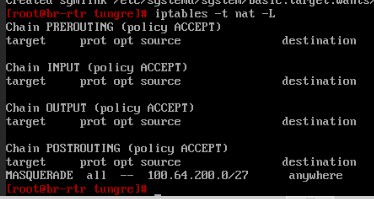
## iptables –t nat –A POSTROUTING –s 100.64.200.0/27 –o ens18 –j MASQUERADE



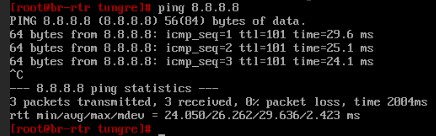
Сохраняем и добавляем в автозагрузку



Проверим правило



Проверяем доступ в интернет



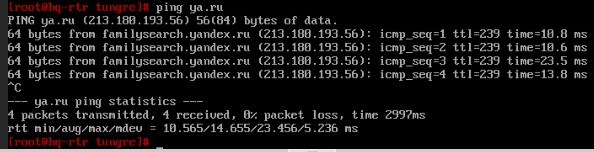
# НАСТРОЙКА ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ С ПОМОЩЬЮ LINK-STATE

**ПРОТОКОЛА OSPF:**

Настройку маршрутизации будем проводить, используя пакет **frr. HQ-RTR:**

Для начала проверим, что с роутера есть доступ в интернет по доменным именам. Для этого сделаем команду **ping ya.ru**

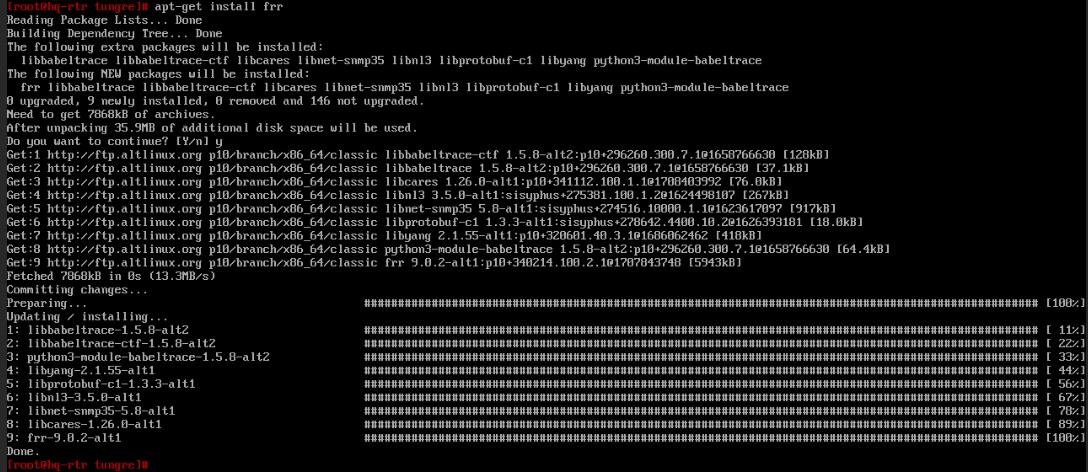
Если пинг идет, значит можем приступать к обновлению списка пакетов в репозитории и установке пакета frr.



Обновляем список репозиториев



Устанавливаем пакет frr и подтверждаем установку нажав Y



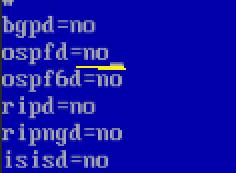
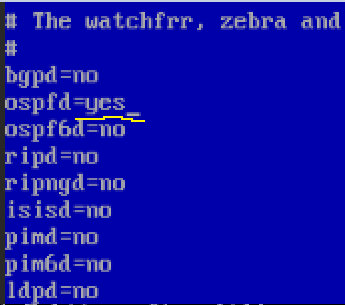
Далее нам нужно включить поддержку модуля ospf. Для этого заходим в файл daemons в директории

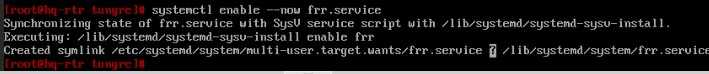
/etc/frr/

Откроем этот файл любым удобным для вас текстовым редактором (mcedit/vi/можете установить предварительно nano и использовать его)

## mcedit /etc/frr/daemons



 меняем на **yes ** и сохраняем.

Далее перезагружаем работу сервиса frr



и делаем для него автозагрузку

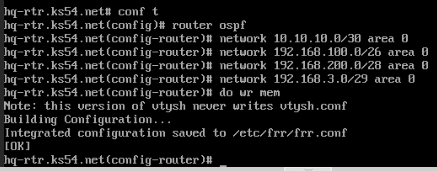
Входим в окружение нашего виртуального роутера командой **vtysh**



А дальше как в циско настраиваем ospf на роутере с нашими подсетями. Помним, что нам необходимо выставить работу протокола маршрутизации по туннелю с внутренними подсетями, не задействовал внешние сети, которые идут к ISP (см. задание)

## conf t router ospf

**network 10.10.10.0/30 area 0 network 192.168.100.0/26 area 0 network 192.168.200.0/28 area 0 network 192.168.3.0/29 area 0 do wr mem**



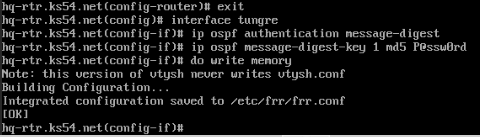
Теперь настроим парольную защиту на нашем GRE туннеле через frr

**exit**

**int tungre**

**ip ospf authentication message-digest**

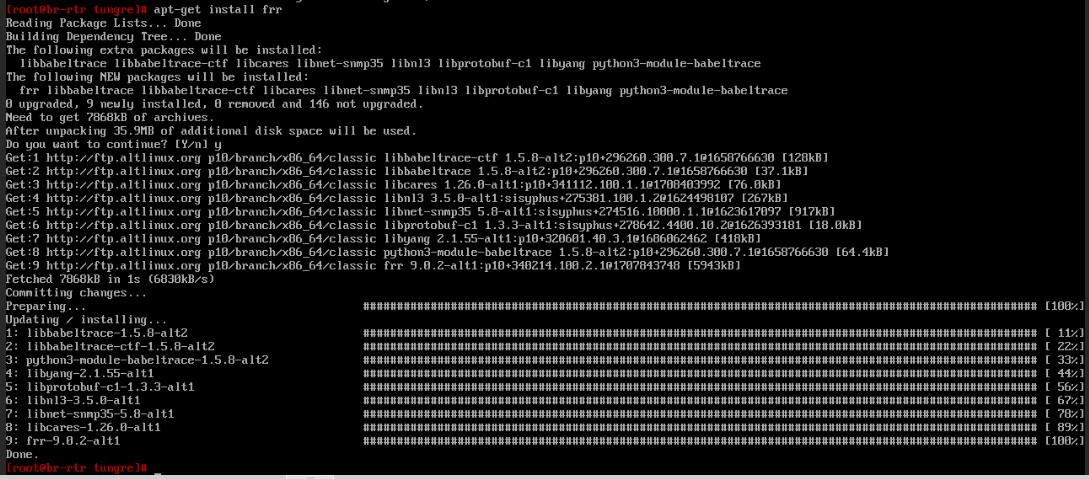
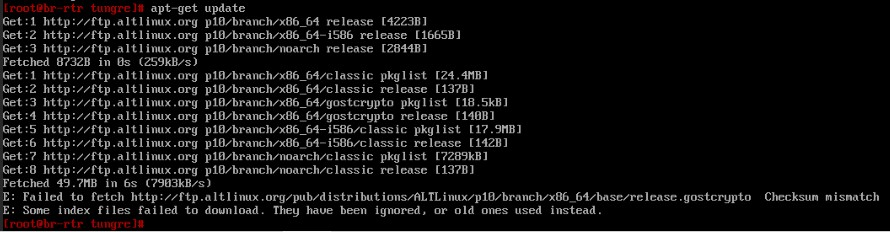
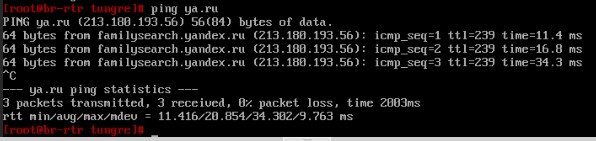
**ip ospf message-digest-key 1 md5 P@ssw0rd do write memory**

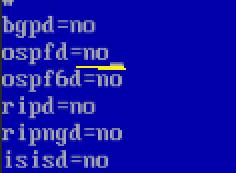
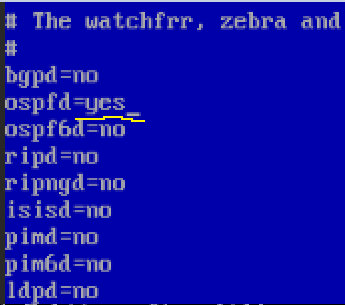


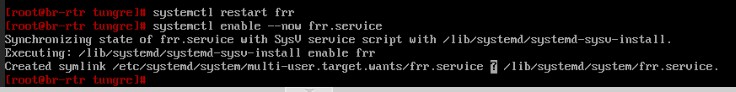
Таким образом OSPF на HQ-RTR настроем. Приступаем ко второй стороне.

# BR-RTR:

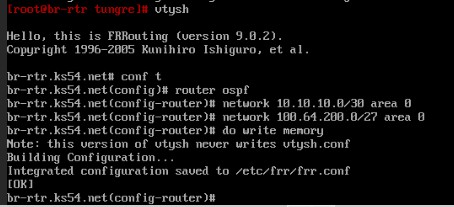
Аналогично прошлому роутеру нам нужно установить данный пакет.



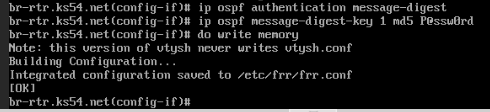
 меняем на **yes ** и сохраняем.



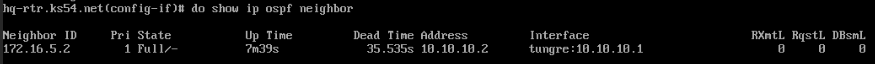
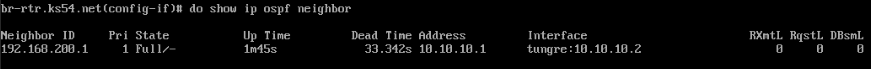
Настраиваем OSPF для туннеля и внутренних подсетей роутера BR-RTR



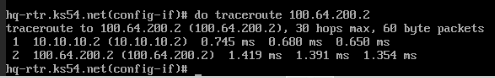
Теперь также настроим парольную защиту на нашем GRE туннеле через frr

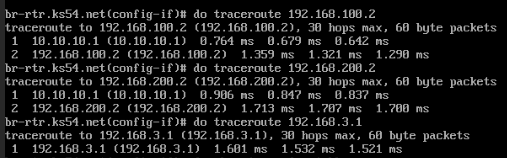


Теперь проверим наших соседей



Проверяем пинг с одного роутра на все интерфейсы второго, должно все пинговаться. Можно проверить трассировку

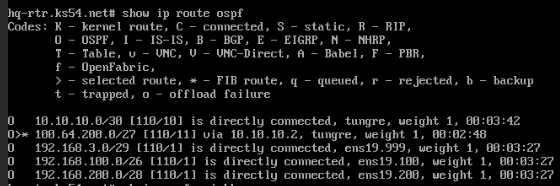




Но иногда ospf некорректно отображает свою работу, поэтому –

лучше сделать **reboot** роутеров HQ-RTR и BR-RTR.

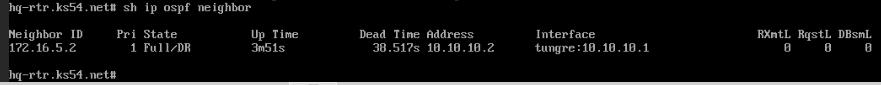
После зайти в vtysh и вбить команду: **show ip route ospf**, она покажет какие сети объявлены.



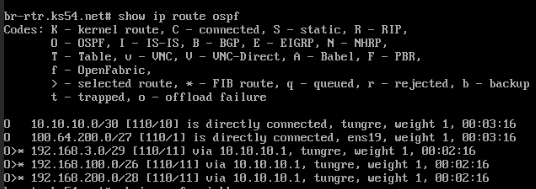
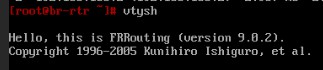
Как видим на HQ-RTR объявлены все сети, что прописаны в настройках ospf и \* отмечена сеть BR,

которая объявлена через ospf.

Проверим соседей снова, чтобы корректно отобразить связь через наш тоннель.



Проверим теперь на роутре BR-RTR.



Как видим теперь все корректно отображается.

# 9. НАСТРОЙКА ПРОТОКОЛА ДИНАМИЧЕСКОЙ КОНФИГУРАЦИИ ХОСТОВ:

Настройка DHCP-сервера может быть осуществлена различными способами, либо через установку и настройку напрямую dhcp-сервера из пакета, либо с помощью альтератора на клиенсткой машине. Но есть еще один способ, как на мой взгляд достаточно упрощенный и быстрый.

Если знаете, как альтернативную установку и настройку делать, то, пожалуйста, главное, чтобы цель была достигнута – установлен и настроен DHCP-сервер и выдает адрес для HQ-CLI из диапазона адресов.

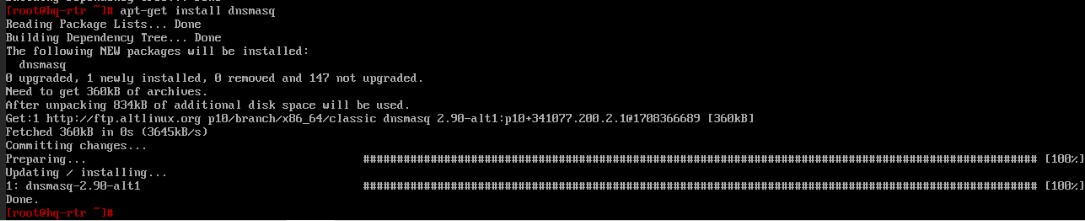
Итак, приступим:

# HQ-RTR:

Установим пакет **dnsmasq** (не удивляйтесь названию, все верно)



Получаем



Заходим в настройки конфигурационного файла сервиса

## mcedit /etc/dnsmasq.conf

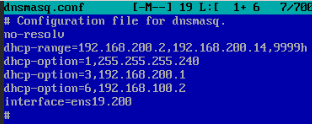


Вносим следующие строки в начало файла:

**no-resolv**

**dhcp-range=192.168.200.2,192.168.200.14,9999h**

**dhcp-option=1,255.255.255.240 dhcp-option=3,192.168.200.1 dhcp-option=6,192.168.100.2 interface=ens19.200**



dhcp-option=**1** отвечает за маску подсети, передаваемого диапазона

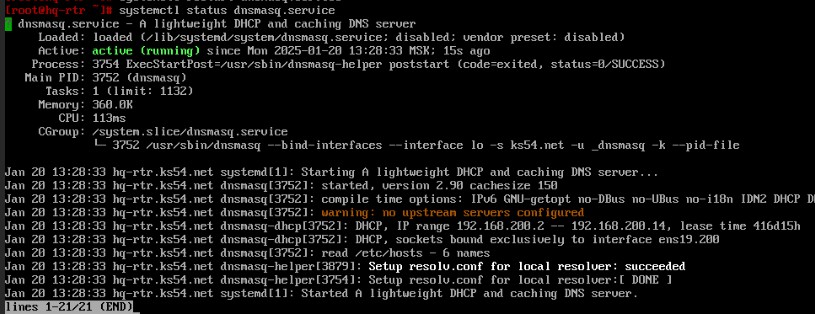
dhcp-option=**3** отвечает за пересылаемый dhcp-сервером адрес шлюза по умолчанию dhcp-option=**6** отвечает за пересылаемый dhcp-сервером адрес dns-сервера по умолчанию С полным списком опций (Tag) можетt ознакомиться по адресу: <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml>

Далее нужно подтянуть параметры, которые мы указали. Для этого рестартуем сервис

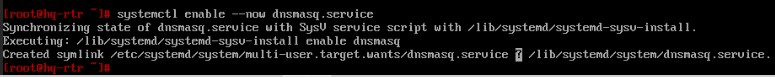
## systemctl restart dnsmasq.service



Проверим статус запущенного сервиса **systemctl status dnsmasq.service**



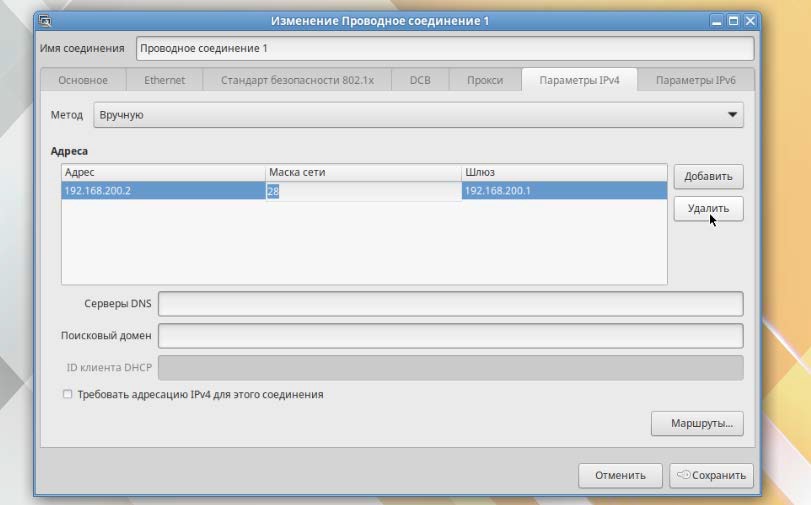
Чтобы этот сервис запускался автоматически после перезагрузки системы добавим его в автозагрузку: **systemctl enable --now dnsmasq.service**

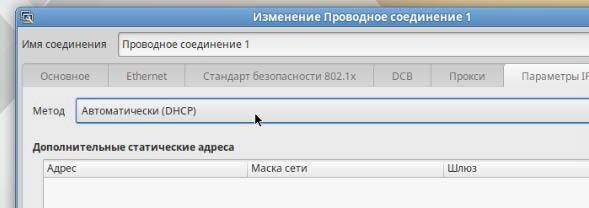


# HQ-CLI:

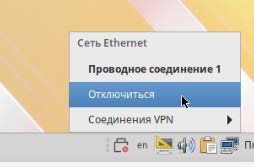
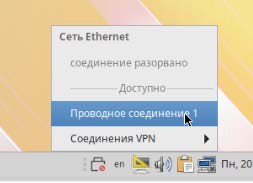
Осталось проверить раздает ли ip-адрес на клиента HQ-CLI

Зайдем на HQ-CLI и обновим конфигурацию сетевых параметров

Удалим созданный нами ранее статический ip и оставим только получать DHCP автоматически

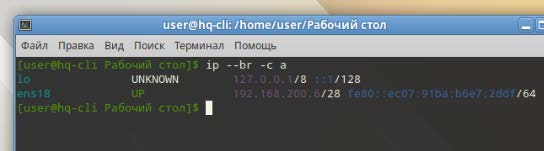


Нажимем Сохранить, вводим пароль toor и затем переактивируем сетевое подключение (левой кнопкой мыши на апплете сетевого подключения => отключиться, затем то же самое и выбираем название проводного соединения

 => 

Получаем анимацию загрузки сетевых параметров и если все хорошо, то она сменяется обычным видом апплета сетевого подключения

 => 

Проверим адрес, который получили, откроем терминал и командой ip --br –c a удостоверимся, что выдан корректный ip-адрес из введенного нами диапазона.

Все окей, значит наш DHCP-сервер работает корректно.

# 10. НАСТРОЙКА DNS ДЛЯ ОФИСОВ HQ И BR:

Настройку DNS-сервера можно выполнять стандартными способами, такими как конфигурирование сервиса из пакета bind9, а можно использовать уже знакомый нам сервис **dnsmasq**.

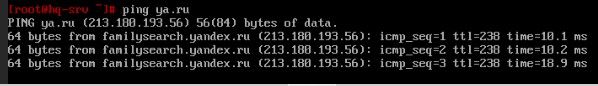
# HQ-SRV:

Первым делом проверим, что мы можем пропинговать сайт ya.ru с HQ-SRV. Если не выдает пинг, тогда нужно на интерфейс машины в файл **/etc/net/ifaces/ens18.100/resolv.conf** дописать строчку **nameserver 77.88.8.8** с общедоступным сервером dns от яндекса. Рестартанув сетевую службу мы получим возможность скачивать пакеты.



Проверим что файл записан в файл



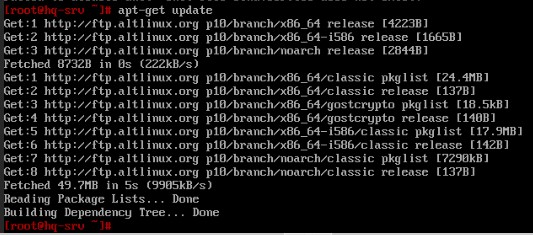
Делаем рестарт сетевых сервисов И пингуем ya.ru

Все окей, можем идти дальше.

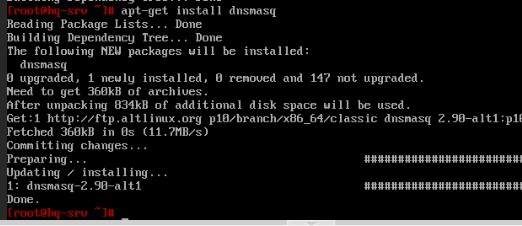
Для начала нам нужно отключить несовместимую с dnsmasq службу bind, чтобы не возникло конфликтов. Для этого на сервисе пропишем **systemctl disable --now bind**

В нашем случаем его нет, поэтому он ругается, но на всякий случай лучше проверить. Теперь установим на сервер dnsmasq.

## apt-get update

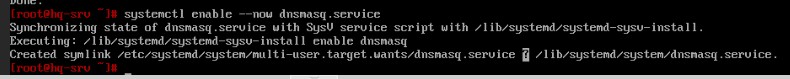


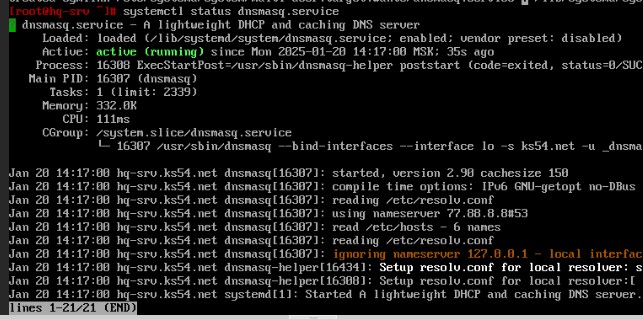
**apt-get install dnsmasq**



Добавим наш сервис dns-сервера будущего в автозагрузку системы, который в свою очередь инициализирует его первый запуск. Для этого используем нам известную команду

## systemctl enable --now dnsmasq.service



Проверяем статус сервиса

Открываем файл для редактирования конфигурации нашего будущего DNS-сервера:

## mcedit /etc/dnsmasq.conf



И добавляем в неё строки (для удобства прям с первой строки файла):

**no-resolv** (не будет использовать /etc/resolv.conf)

## domain=ks54.net

**server=77.88.8.8** (адрес общедоступного DNS-сервера)

**interface=ens18.100** (на каком интерфейсе будет работать служба)

## address=/hq-rtr.ks54.net/192.168.100.1

**ptr-record=1.100.168.192.in-addr.arpa,hq-rtr.ks54.net**

**cname=moodle.ks54.net,hq-rtr.ks54.net (**Запись, которая понадобиться во 2 модуле для работы Moodle)

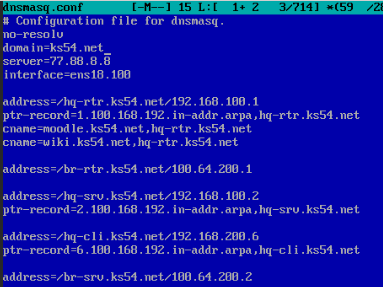
**cname=wiki. ks54.net,hq-rtr. ks54.net (**Запись, которая понадобиться во 2 модуле для работы Wiki)

## address=/br-rtr. ks54.net /100.64.200.1 address=/hq-srv. ks54.net /192.168.100.2

**ptr-record=2.100.168.192.in-addr.arpa,hq-srv. ks54.net**

**address=/hq-cli.au-team.irpo/192.168.200.6 (**Смотрите адрес на **HQ-CLI**, т.к он выдаётся по DHCP**) ptr-record=6.2.168.192.in-addr.arpa,hq-cli. ks54.net**

## address=/br-srv. ks54.net /100.64.200.2



Теперь добавим в файл **/etc/hosts** строчку **192.168.100.1 hq-rtr.ks54.net,** чтобы система могла интерпретировать роутер hq-rtr по доменному имени и по ip-адресу.

## mcedit /etc/hosts

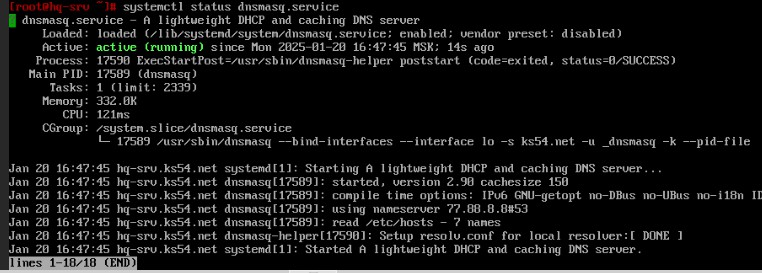


Перезапустим сервис dnsmasq

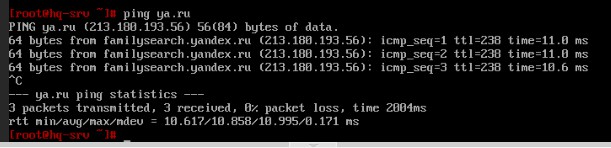
## systemctl restatrt dnsmasq.service



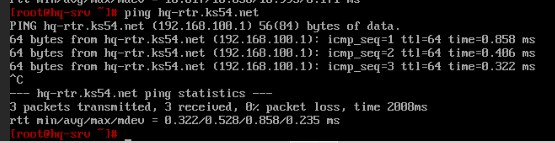
Проверяем статус сервиса и убедимся, что он работает без ошибок. (если ошибки есть, внимательно читаем мануал, смотрим и сверяем конфигурационные файлы, а также читаем журнал ошибок в системе)



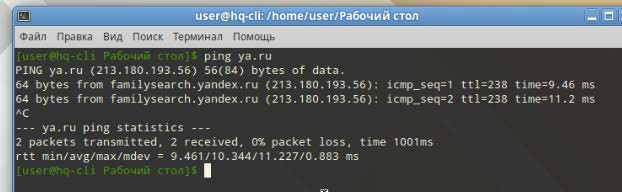
Проверим пинг до яндекса по доменнмоу имени (или гугла, кому что больше нравится)

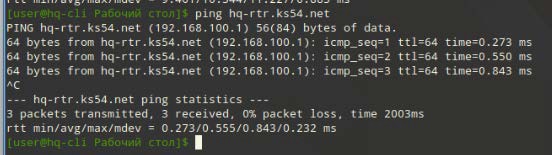


Проверим локальную dns-запись на доступность по доменному имени и если пинг идет, то тогда

dns-сервер работает.

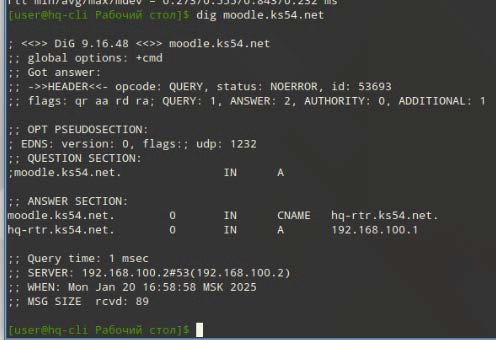
Все работает. Осталось протестировать работу с другой машины, например, с HQ-CLI



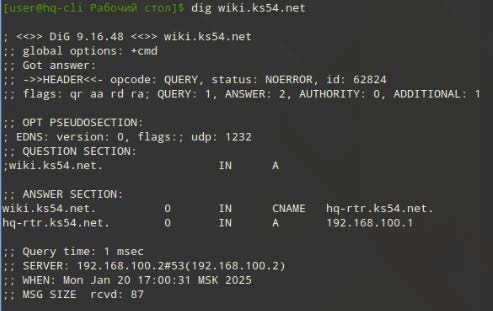
Проверим другие записи:

Проверим CNAME записи с помощью команды **dig**

В выводе команды в разделе ANSWER SECTION должны увидеть наши записи, что мы создавали.



## Wiki.ks54.net



Все работает. DNS-сервер готов.

# 3. СОЗДАНИЕ ЛОКАНЫХ УЧЕТНЫХ ЗАПИСЕЙ:

Создадим пользователей sshuser на серверах подстетей HQ и BR.

**Создание на HQ-SRV:**

Для создания пользователя с заданным идентификатором (как сказано в задании – см. задание Модуль 1) на машине под управлением ОС ALT Linux используем команду **useradd sshuser –u 1010**

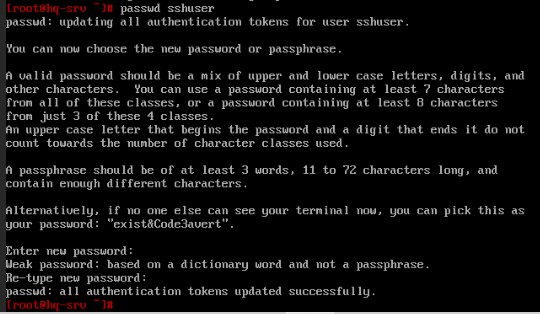


Удостовериться в правильности создания пользователя с заданным id можно командной **id sshuser**



Зададим пароль на нашего пользователя, используя команду **passwd sshuser** и вводим пароль

P@ssw0rd и еще раз для подтверждения.



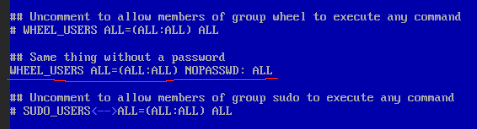
Чтобы **sshuser** мог запускать **sudo без дополнительной аутентификации**, необходимо убрать комментарий строки в файле **/etc/sudoers**, откроем его командой:

## mcedit /etc/sudoers



И уберём комментарий (знак #) на следующей строке:

# WHEEL\_USERS ALL=(ALL:ALL) NOPASSWD: ALL



Сохраняем и затем добавляем нашего пользователя sshuser в группу wheel. Для этого используем команду **usermod –aG wheel sshuser**

Проверим теперь нашего пользователя командами и удостоверимся, что все сделали правильно: выставили id и добавили в группу wheel

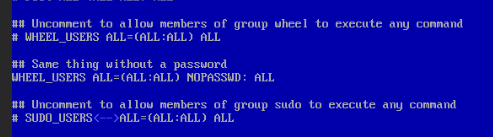
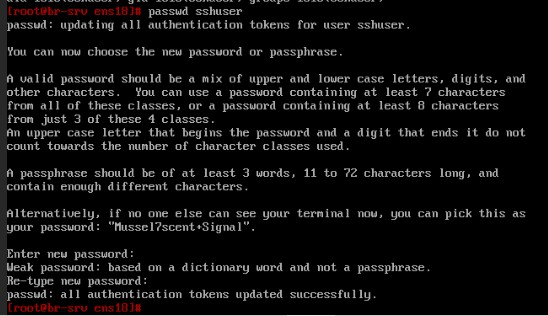


Группы можно проверить более явно следующей командой



**Создание на BR-SRV:**

Проделаем тоже самое для сервера BR-SRV. Создадим такого же пользователя с теми же параметрами, что и для HQ-SRV (более подробные пояснения можно посмотреть выше)



Проверим аналогичными командами



Пользователей для ssh мы создали, теперь создадим пользователей net\_admin для наших роутеров

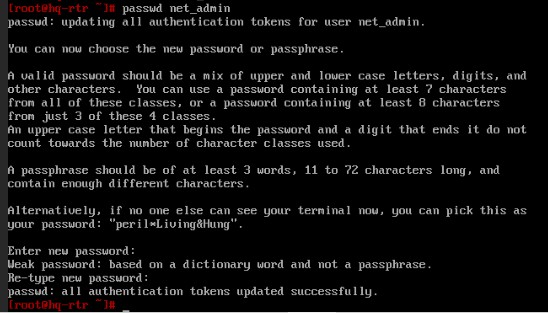
**Настройка пользователя net\_admin на HQ-RTR:**

В целом добавление и настройка пользователя похожа на предыдущий пункт, но есть некоторые особенности согласно заданию.

Сперва добавляем пользователя с домашним каталогом командой **useradd net\_admin –m**

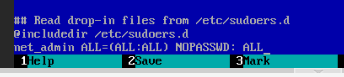


Ставим пароль на него командой **passwd net\_admin** и вводим дважды пароль P@ssw0rd



По заданию необходимо, чтобы net\_admin мог запускать команду sudo без дополнительной аутентификации (то есть без запроса пароля), необходимо отредактировать файд **/etc/sudoers,** а именно добавить в конец файла строчку **net\_admin ALL=(ALL:ALL) NOPASSWD: ALL**

И в конце файла пропишем сточку



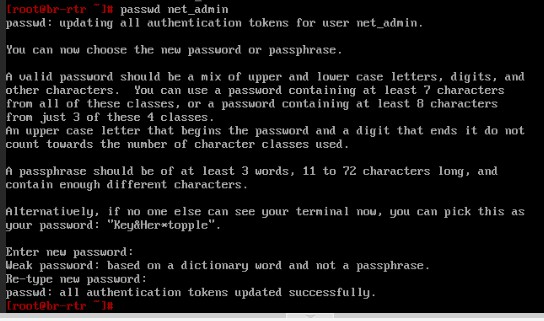
**Настройка пользователя net\_admin на BR-RTR:**

Аналогичным способом создаем пользователя и на втором роутере, более подробные комментарии смотри в пункте выше.

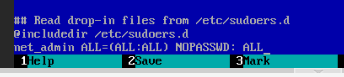
Создаем пользователя net\_admin



Устанавливаем пароль P@ssw0rd



Редактируем файл /etc/sudoers



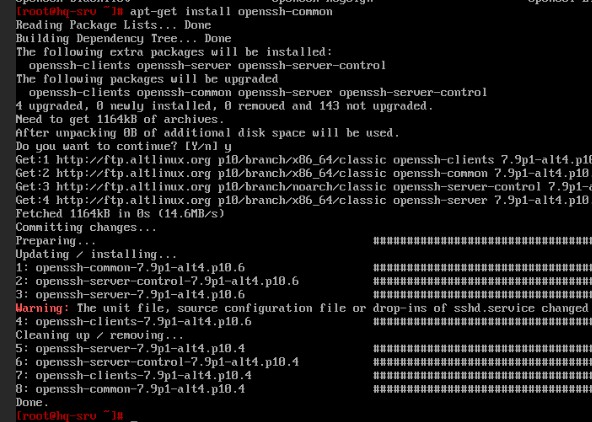
На этом создание локальных учетных записей пользователей по заданию 1 модуля завершено.

# 5. НАСТРОЙКА БЕЗОПАСНОГО УДАЛЕННОГО ДОСТУПА НА СЕРВЕРАХ HQ-SRV И

**BR-SRV:**

Выполним настройку по заданию сперва на машине **HQ-SRV:**

Для работы SSH нам понадобится служба **openssh-common**, которой изначально нет, поэтому установим её: **apt-get install openssh-common**



Далее вносим изменения в конфигурационный файл openssh командой

**mcedit /etc/openssh/sshd\_config**

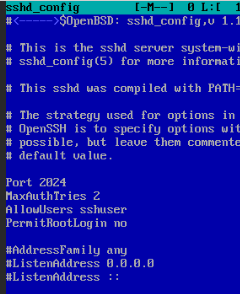


**(внимательно пишите файл конфигурации, так как там есть в директории два файла, один**

**ssh\_config, а второй sshd\_config, так вот нам нужен именно второй с буквой d)**

Вбиваем в этот конфигурационный файл следующие строки:

**Port 2024** (меняем порт подключения по ssh со стандартного 22 на 2024) **MaxAuthTries 2** (выставляем ограничение попыток входа равное двум) **AllowUsers sshuser** (разрешаем подключение только пользователю sshuser) **PermitRootLogin no**(запрещаем вход по ssh от имени root)



Также по заданию нам нужен баннер. Для этого надо нам создать его. Создаем командой файл

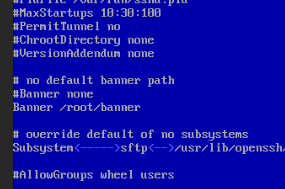
## mcedit /root/banner



Внутри пишем **Authorized access only** и обязательно после этой строчки нажимаем Enter чтобы создалась пустая строка после введенной строки. Это обязательно, иначе баннерная фраза не считается системой и не будет работать.



После создания баннера нам нужно сделать ссылку на наш созданный файл в конфигурационном файле openssh. Поэтому обратно открываем файл **mcedit /etc/openssh/sshd\_config** и добавляем в конце файла строчку **Banner /root/banner**

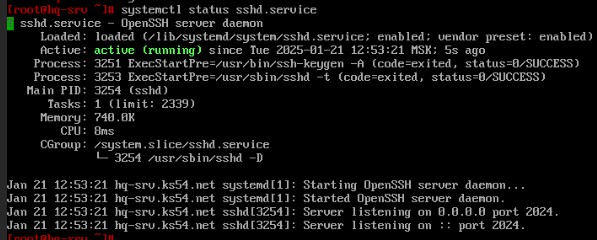


После внесения изменений, сохраняем и выходим. Перезапускаем службу командной **systemctl restart sshd.service**

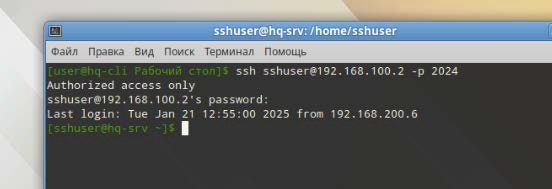
И делаем автозапуск службы после перезагрузки системы: **systemctl enable --now sshd**



Проверим на сервере работу сервиса ssh



Теперь проверим работу нашего сервера через HQ-CLI. Попробуем подключиться из терминала к нашему серверу **ssh** [**sshuser@192.168.100.2**](mailto:sshuser@192.168.100.2) **-p 2024**



**sshuser** – пользователь, под которым вы подключаетесь

**192.168.100.2** – адрес сервера, к которому мы подключаемся (**HQ-SRV**)

**-p 2024** – порт, по которому мы подключаемся (мы заменили со стандартного 22 на 2024)

Выполним настройку ssh на машине **BR-SRV:**

## Проделываем абсолютно все тоже самое и на сервере BR-SRV.

"l1t.-1\_1г-t i,1:-:1.ct 11 111.1r11·-- .l1-1·1.1n1111111 Г,11.l-..,,111: 1. i , t.:-;. . IJ111н:

Rr:,1.-i i нц

Вн i 1(1 i 11tJ Ikpr11riг-111:1J T!'t-:r ... D1111r

Tl11: 1'11 I 1 ow i 1·11:, 1,:, f.r·,, p,11.k,"[1::-, w i 1 1 1,,: i 1·1·•; f.,1 1 l 1·:rl:

оре 1Е:с:·l1-г- 1 i f'1·1

|  |  |  |
| --- | --- | --- |
|  | t ,, | opf'11: ·с:·11 |
| 11,н:k,11Jr:.-, ui | | |
| пt·c; | |  |

Tl11· Г11l low i 1·11:,

- - ·P.c•Jf'Г opP.11,;:c:-l1-•;:f'Г1Jf'P-c п1·1t гп 1

11 1)1: 111111т,1,t1:rl

ope11-::s·l1-c 1 ie



1

ореп-с:s·l

1·1·n,11н·,1

opeп-:·s·l1-con111oн

--с:ег1..1е1·· орен-с:-:·1·1--с:ег•.J

**·1** 11p<jr0,нl,:,·t, П 111·ul11 i11 .l.,1ll1:,t, **П**

Nccd to qct llb1kM of aгchiucs.

flft.1·1· 1111p,11ki1111 ПП оГ мl,titi11н,1l

**tн·** 11:-.1·,t.

-р,11.1· will

,lisk

,11"1 141 1101. ll\"Jf',1rlr:,·

Do цо11 uaпt to сопt i пнс'1 **L** 'r'/п J **ц**

r.,:t:1 l1il.11://fl11.,1lili1111(.lll'IJ 111П,1,1',lнt11г,П(, r,4/1:l,,s·,it

|  |
| --- |
| 11111·11 |
| арен |
| 1111r11 |
| арен |

l,ct:*i* l1ttp: /.'ftp. J.lt 1 i 1шх. orq plU.,..Ьr.:1пcJ1.•xl:Jь Ь1.'с la:::c: ic

r,,..,t:l l1l l.11://fl11.,1li l i1111(.lll'1J 111П,1,1·,1н1 !1/111,,1r·1 l1/1:l<1s·,i1

l,ct:**1** l1ttp: .··.•f tp. J. l t 1 i 11ш<. orq

p1U.,..Ьr.:1пcl1•xl:Jb

Ь1.'с !а::ic

fг"t1l1г"rl 1Н14kП i11 Пs (1П.ПМR,s) lomnittiнq C)IJ.ll(/CS ...

UIIUUUtlUt

Pr·,..,1•e1r· i11'.J ...

UpdJ.tiнq.,.. iн:::t,,lliпq ..

111/U tllttlllt

1: f•[IГ:ll ,"/1-1.•.11111110ll-7.'.lj11-c1114.Jl1fl.f1

L: opcнssh scrucr control J. pl alt1.p1U.L

|  |  |
| --- | --- |
| llllltllll\:llt | |
| 111111 tlltt/111 | |
| 11.гор | i11. |

1: 11pг:11 .•;J1-:-,,..,l'lJl"l'-7. ".111 l-c1 **l t** 4. JI lfl .f,

1н1it

ll.111,11111 Н1с

l'ilc, .:;онгсс coпliq1.1r,:it,io11

l'i !с *ос*

4 .' l-'[l"'ll .-;}1-c] j 1"'111.•-:-·,'. 'JI' 1-ct] t,4. **1'**1 fl. f,

11111111111111!

С lc:,111 i )H.f 1Jp *,/*

11111:11,,•;!1

t!p"11:.,;}1-1.l

,;r:гt!• •·

i"11t•-:-'?.Чp1-ctlt4.p1fl.4

11r11:11,;:;l1

11pг:11:-.·;J1-:-,,..,f'llf-:['-i.

.... :

i

*ч*1' l-c11 t 4 . JI 10. 4

r·CMIJlJ

...

Н1:(

ltlll1tllltll1t

f,: ',': В:

Doпf'.

-11, t

I о"

1.11111.r·ol 7,'-,111 ,11t.1.J11П.·1

1ommo11 7.'1111 ,,11.1.J11П.·1

IHlltllllf:llt 11n111111n111 UUUII UUU

.

, •/

.

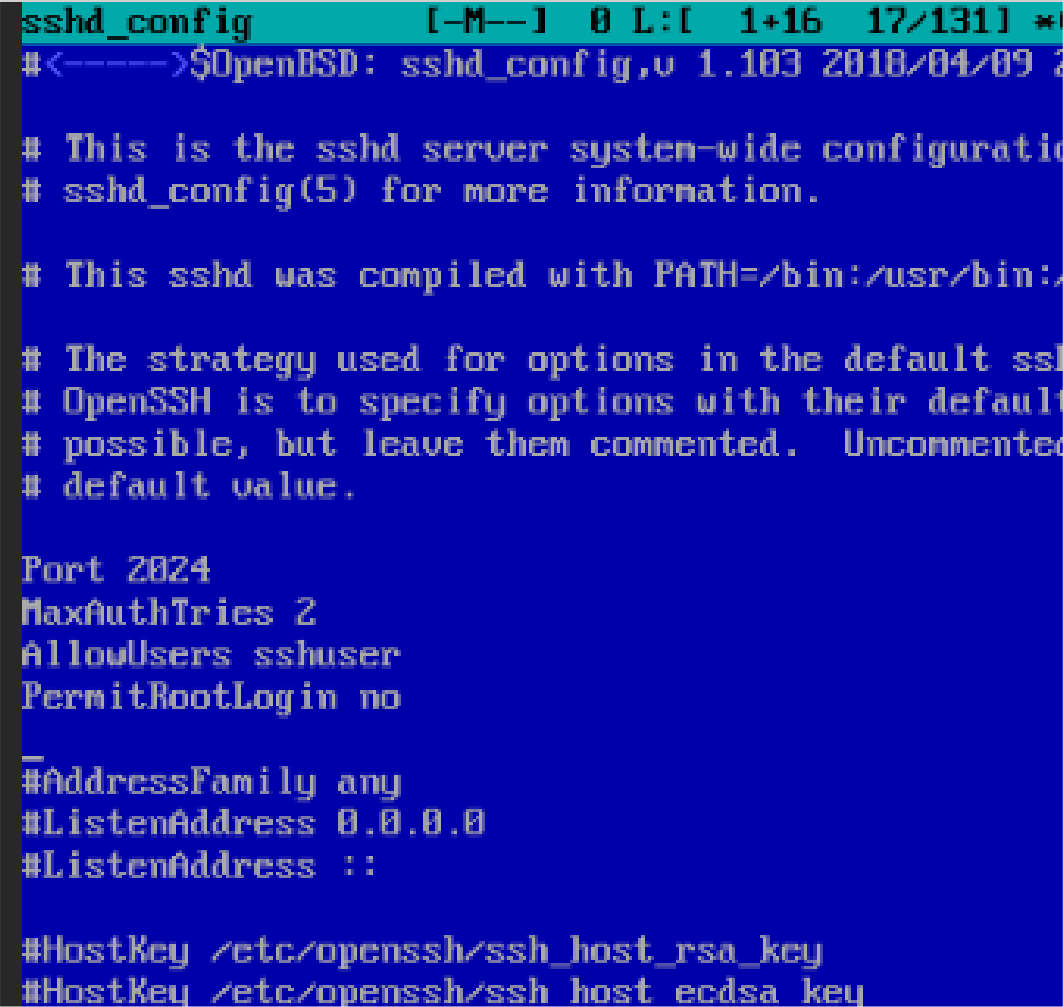
/ 1, •

.

1111 , •, t,i

1 1111•, 1·-. ,J ,/ •...

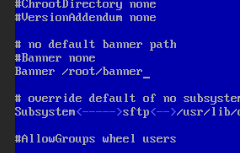
r·i Jr

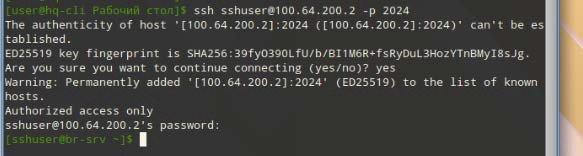
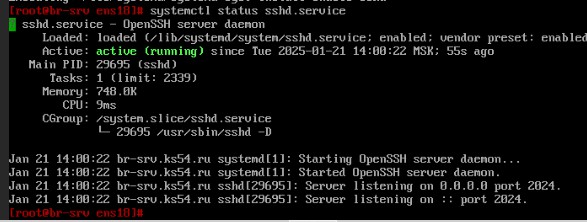


/Y'l 101*/* J,., 11111•1'

1111 1•,i j f

fl111 l11н· i ;•.,:11 ,11.1.1·:-., 1111 11,1





**Результат показывает, что сервер ssh работает на обоих серверах по заданным параметрам**

**ВСЕ ЗАДАНИЯ 1 МОДУЛЯ ДЭ ВЫПОЛНЕНЫ**