Мне не лень оформлять (Рахвалов Роман)

Login: root

Password: toor

Для клиента: пароль от user – user

Для того, чтобы зайти в root, написать su в терминале и ввести пароль toor

ip a – выводит список интерфейсов

ls -l “директория” – выводит список папок в директории

cat “директория и в конце название файла” – показывает, что находится в файле

cd "директория" – переход в директорию

/etc/net/ifaces

apt-get update

systemctl restart network

Если что-то не получается, не пингуется сеть или ещё что-то, то сначала нужно проверить настройки самой виртуалки. Нажать правой кнопкой мыши и выбрать “Edit settings”, посмотреть соединения, проверить MAC-адреса.

**Таблица адресов:**

|  |  |  |  |
| --- | --- | --- | --- |
| Имя устройства | Направление | IP-адрес | Шлюз по умолчанию |
| ISP-1сетевая |  | DHCP | Провайдер |
| ISP-2сетевая | HQ-RTR | 172.16.4.1/28 |  |
| ISP-3сетевая | BR-RTR | 172.16.5.1/28 |  |
| HQ-RTR-1сетевая | ISP | 172.16.4.2/28 | 172.16.4.1 |
| HQ-RTR-2сетевая | HQ-SRV | 192.168.1.1/26 |  |
| HQ-RTR-3сетевая | HQ-CLI | 192.168.2.1/26 (28) |  |
| HQ-SRV | HQ-RTR | 192.168.1.2/26 | 192.168.1.1 |
| HQ-CLI | HQ-RTR | 192.168.2.2/26 | 192.168.2.1 |
| BR-RTR-1сетевая | ISP | 172.16.5.2/28 | 172.16.5.1 |
| BR-RTR-2сетевая | BR-SRV | 10.0.2.1/26 |  |
| BR-SRV | BR-RTR | 10.0.2.2/26 | 10.0.2.1 |

Содержание

[**Таблица адресов:** 1](#_Toc190275267)

[**1. Смена имени хоста** 3](#_Toc190275268)

[**2. Настройка ISP** 3](#_Toc190275269)

[**2.2 Установка и настройка nftables на ISP** 7](#_Toc190275270)

[**3. Настройка роутера HQ-RTR/BR-RTR** 10](#_Toc190275271)

[**3.1 Указание DNS в resolv.conf** 12](#_Toc190275272)

[**3.2 Настройка nftbales на роутерах** 12](#_Toc190275273)

[**4. Настройка SRV** 13](#_Toc190275274)

[**6. Настройка клиента HQ-CLI (завершение пункта задания 8 про интернет на всех устройствах)** 13](#_Toc190275275)

[**Задание 3. Создание локальный учётных записей (sshuser на серверах HQ-SRV и BR-SRV)** 14](#_Toc190275276)

[**Задание 5. Настройка безопасного удалённого доступа на серверах HQ-SRV и BR-SRV** 16](#_Toc190275277)

[**Задание 6. IP-туннель** 17](#_Toc190275278)

[**Задание 7. Настройка OSPF** 18](#_Toc190275279)

[**Задание 8** 22](#_Toc190275280)

[**Задание 9. DHCP** 23](#_Toc190275281)

[**Настройка DNS (Задание 10)** 26](#_Toc190275282)

[**Настройка часового пояса (Задание 11)** 27](#_Toc190275283)

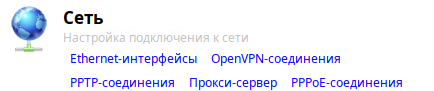
**1. Смена имени хоста**

На устройствах нужно поменять имя хоста. Сделать это нужно в файле **hostname** в директории /etc. Для ISP оставим просто isp. Для остальных устройств нужно писать полное доменное имя:

|  |  |  |
| --- | --- | --- |
| **Устройство** | **Запись** | **Тип** |
| HQ-RTR | hq-rtr.au-team.irpo | A,PTR |
| BR-RTR | br-rtr.au-team.irpo | A |
| HQ-SRV | hq-srv.au-team.irpo | A,PTR |
| HQ-CLI | hq-cli.au-team.irpo | A,PTR |
| BR-SRV | br-srv.au-team.irpo | A |
| HQ-RTR | moodle.au-team.irpo | CNAME |
| HQ-RTR | wiki.au-team.irpo | CNAME |

Проверить имя хоста можно командой hostnamectl

На HQ-CLI сменить имя в графике. Нажимаем лкм на пуск («Меню»). Затем «Центр управления», далее «Центр управления системой». В нём найти «Сеть» и выбрать «Ethernet-соединения».



Изменить имя компьютера

Сделать таблицу адресов, а потом занести эти данные в отчёт (пример таблица 3)

**2. Настройка ISP**

**По заданию:**

* интерфейс, который подключён к облаку «Internet», получает адрес по DHCP.
* Интерфейс, к которому подключён HQ-RTR, подключён к сети 172.16.4.0/28
* Интерфейс, к которому подключён BR-RTR, подключён к сети 172.16.5.0/28
* На ISP должны быть настроены сетевая трансляция в сторону HQ-RTR и BR-RTR и интернет

**Выполнение задания:**

Проверяем какие интерфейсы у нас есть при помощи команды:

[root]# ip a

В выводе команды у нас есть несколько разных интерфейсов. «lo» нас не интересует. Остаются «en или ens…» что-то там.

Затем нам нужно отредактировать файл конфигурации этого интерфейса. Здесь есть 2 путя (как в анекдоте). Можно редактировать через vim. Можно средствами командной строки. Так как я задрот, а за vim не шарю, то предлагаю второй путь.

Проверяем что есть в директории с интерфейсами:

[root]# ls -l /etc/net/ifaces/

Если нет нужной директории, то создаём её:

[root]# mkdir -p /etc/net/ifaces/наш\_интерфейс/

После того как создали директорию, нужно в неё зайти командой:

[root]# cd /etc/net/ifaces/наш\_интерфейс/

Далее нужно создать в директории файл options:

[root]# touch options

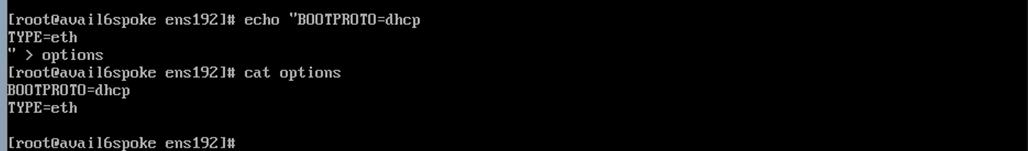
Редактируем файл при помощи команды echo:

[root]# echo «BOOTPROTO=dhcp(нажимаем Enter)

TYPE=eth (нажимаем Enter)

DISABLED=no (нажимаем Enter)

CONFIG\_IPV4=yes (нажимаем Enter)

 « > options

Разберём эту команду:

echo (буквально «эхо») выводит текст в кавычках на экран.

Символ «>» (> options) – перенаправляет вывод в файл, то есть указываем стрелочкой куда записать информацию (типо выводил на экран, теперь в файл).

options – это наш файл. И в конце файла должна быть пустая строка (потому что линукс).

Проверяем содержимое файла options (в котором пока ничего нет):

[root]# cat options

Перезапустим сеть командой:

[root]# systemctl restart network

Проверим интернет:

[root]# ping 77.88.8.8 или 8.8.8.8

Если пингуется, то интернет есть. А если есть интернет, то это значит, что можно скачать mc и накатить обновления:

[root]# apt-get update

~~# apt-get dist-upgrade (опционально)~~

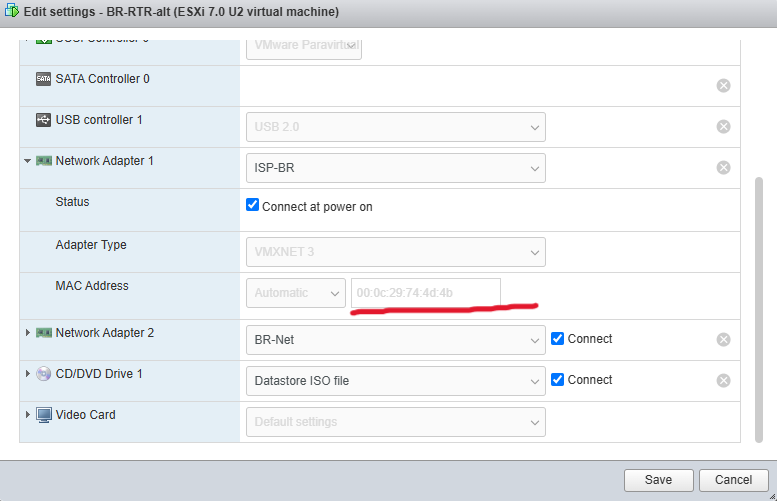
Скачиваем mc:

[root]# apt-get install mc

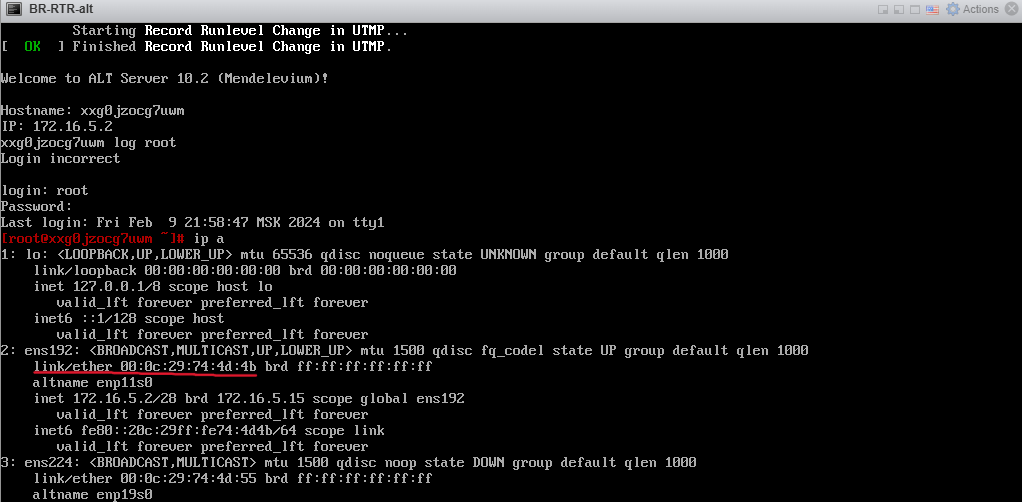
**С этого момента всё, что можно сделать в mc, мы делаем в mc, потому что на остальных устройствах mc УЖЕ УСТАНОВЛЕН.**

Теперь нужно создать 2 директории под 2 интерфейса. Мы нормальные и скачали mc, поэтому мы создаём директории при помощи него. В этих директориях нужно создать 2 файла – options (который создавался ранее) и ipv4address.

**ВАЖНО. Прежде чем назначать ip-адреса интерфейсам, нужно сверить MAC-адреса и сопоставить с соединением роутера**



MAC-адрес интерфейса роутера в настройках esxi



MAC-адрес при выводе команды ip a

Создаём файл **ipv4address**, в котором прописываем статическую настройку:

[root]# touch ipv4address

И в файле прописываем адрес нашей сети (например, 172.16.4.1/28):



[root]# touch options

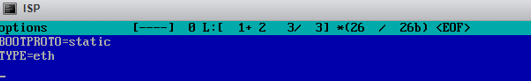
В этом файле прописываем:

BOOTPROTO=static

TYPE=eth

DISABLED=no

CONFIG\_IPV4=yes



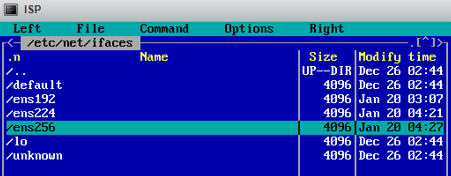
**//Не забываем про то, что последняя строка должна быть пустая//**

Те же самые инструкции повторяем для второго интерфейса, а сеть прописываем другую (172.16.5.1/28)

[root]# mkdir etc/net/ifaces/название\_2ого\_интерфейса/

[root]# touch ipv4address

[root]# touch options



Директории интерфейсов с файлами настроек

# **2.2 Установка и настройка nftables на ISP**

Устанавливаем nftables:

apt-get update

apt-get install -y nftables

Включаем и добавляем в автозагрузку службу nftables:

systemctl enable --now nftables (перед now два маленьких тире -)

**Настройка nftables:**

Далее создаём необходимую структуру для nftables (семейство, таблица, цепочка) для настройки NAT:

Cоздаём в семействе ip таблицу nat:

nft add table ip nat

Cоздаём цепочку postrouting в таблице nat семейства ip, также задаём hook и priority:

nft add chain ip nat postrouting ‘{ type nat hook postrouting priority 0; }’

Cоздаём правила настройки NAT в семействе ip, таблице nat, цепочке postrouting:

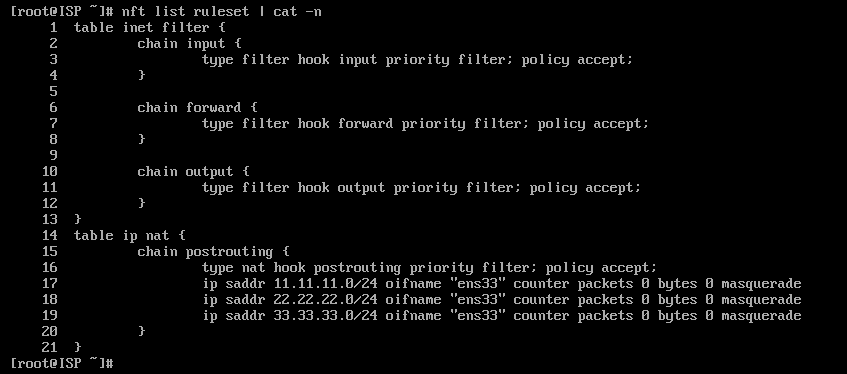
nft add rule ip nat postrouting ip saddr 11.11.11.0/24 oifname “ens33” counter masquerade

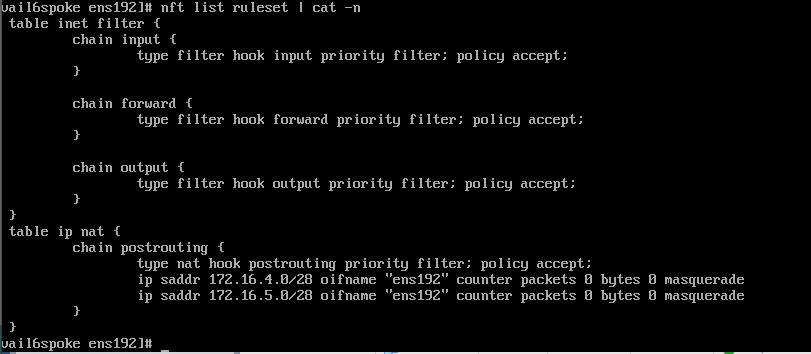
nft add rule ip nat postrouting ip saddr 22.22.22.0/24 oifname “ens33” counter masquerade

//вместо 11.11.11.0/24 написать подсети роутеров, а вместо «ens33» написать интерфейс, который получает dhcp(интернет)//

После этого нужно проверить командой:

nft list ruleset | cat -n





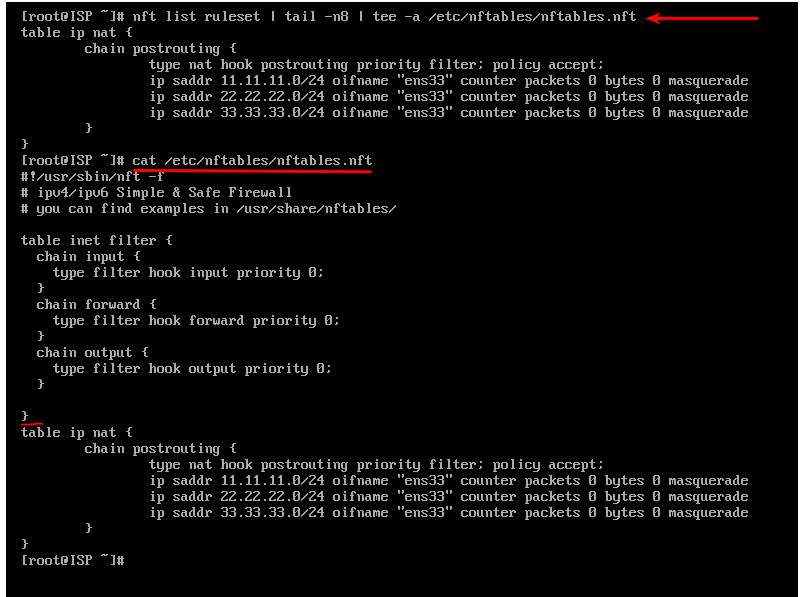
nftables с нашими сетями

Сохраняем правила nftables:

Так как в конфигурационном файле /etc/nftables/nftables.nft уже есть информация о таблице filter – необходимо дописать только что созданную информацию о таблице nat:

дозапишем в конфигурационный файл /etc/nftables/nftables.nft последние 7 строк (от 14 до 21) вывода команды nft list ruleset:

nft list ruleset | tail -n7 | tee -a /etc/nftables/nftables.nft

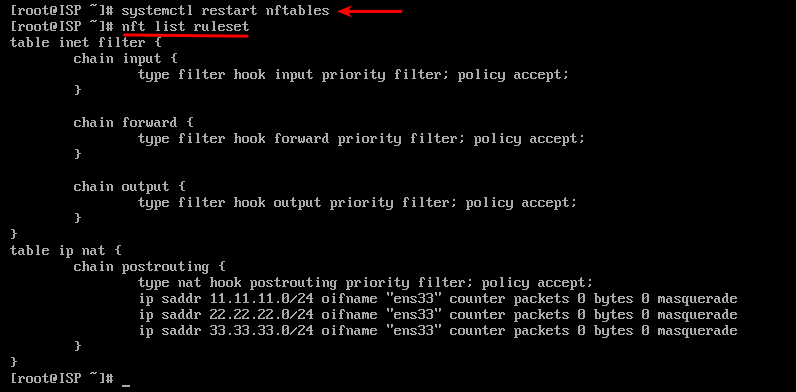


Для проверки перезагружаем службу nftables:

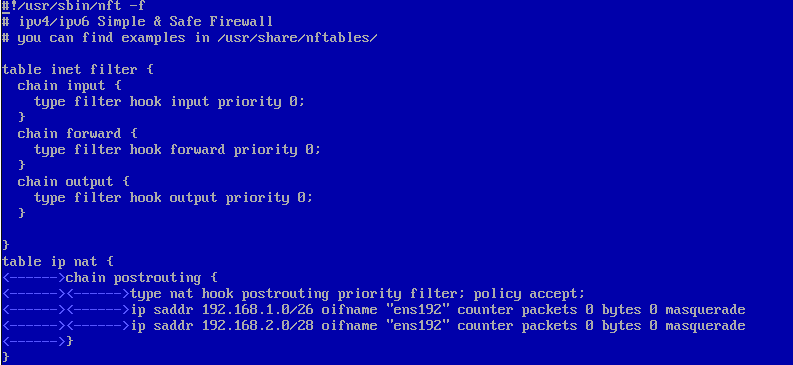
systemctl restart nftables

Смотрим правила:

nft list ruleset

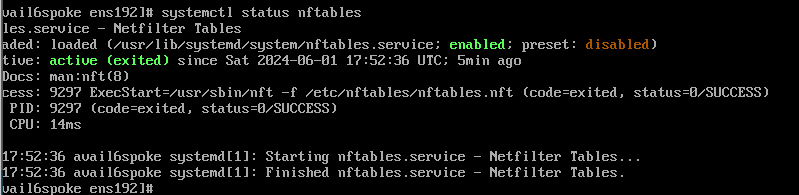


Может быть такое, что nftables могут не работать из-за лишней скобки. Для этого идём в конфиг и проверяем. Если есть лишняя скобка, то удаляем её в конфиге, сохраняем, перезапускаем службу командой systemctl restart nftables.



пример конфига nftbales.nft в mc

Проверить работу можно командой systemctl status nftables



**3. Настройка роутера HQ-RTR/BR-RTR**

На роутере нужно назначить интерфейсам ip-адреса.

Смотрим интерфейсы:

[root]: ip a

Проверяем что есть в директории с интерфейсами:

[root]# ls -l /etc/net/ifaces/

Если нет нужной директории, то создаём её:

[root]# mkdir -p /etc/net/ifaces/наш\_интерфейс/

После того как создали директорию, нужно в неё зайти командой:

[root]# cd /etc/net/ifaces/наш\_интерфейс/

Далее нужно создать в директории файл **options**:

[root]# touch **options**

Редактируем файл при помощи mc и записываем следующие строчки (если не записаны):

BOOTPROTO=static

TYPE=eth

DISABLED=no

CONFIG\_IPV4=yes

**ВАЖНО. Прежде чем назначать ip-адреса интерфейсам, нужно сверить MAC-адреса**

Назначение IP-адресов

Нужно создать файл **ipv4address**:

[root]: touch ipv4address

Пишем в файле **ipv4address** адрес интерфейса:

172.16.4.2/28

Нужно указать шлюз по умолчанию.

Есть два путя: можно настроить по гайду А.А.: создать файл **ipv4route** и в нём написать default via 'адрес шлюза' (также желательно оставить пустую строку):

[root]: touch **ipv4route**

И пишем в файле **ipv4route** шлюз по умолчанию (адрес интерфейса ISP, к которому подключён роутер). Заходим в mc и пишем:

default via 172.16.4.1

После этого проверить командой ping и пропинговать шлюз

**ВАЖНО.** Чтобы был интернет на роутерах, нужно включить форвардинг пакетов на роутерах и ISP. На роутере мы сделаем это следующим образом. Для этого нужно зайти в mc в файл **sysctl.conf** в директории /etc/net

В нём в строчке «net.ipv4.ip\_forward = 0» изменить 0 на 1.

То же самое делаем на ISP.

Теперь форвардинг включён на постоянке. Проверяем интернет, пингуя 77.88.8.8. Если пингуется, то интернет есть. Если не пингуется, то нужно указать DNS в файле **resolv.conf.**

**3.1 Указание DNS в resolv.conf**

DNS-сервер на HQ-RTR, а на всех остальных устройствах просто DNS

DNS в resolv.conf (в директории /etc)

На ISP в resolv.conf ничего не пишем

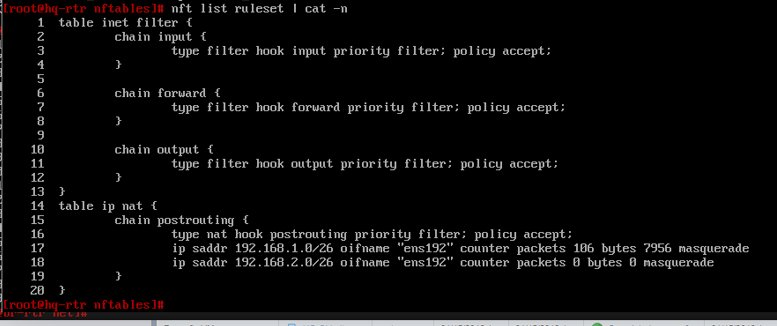
В файле **resolv.conf** пишем:

nameserver 77.88.8.8

**3.2 Настройка nftbales на роутерах**

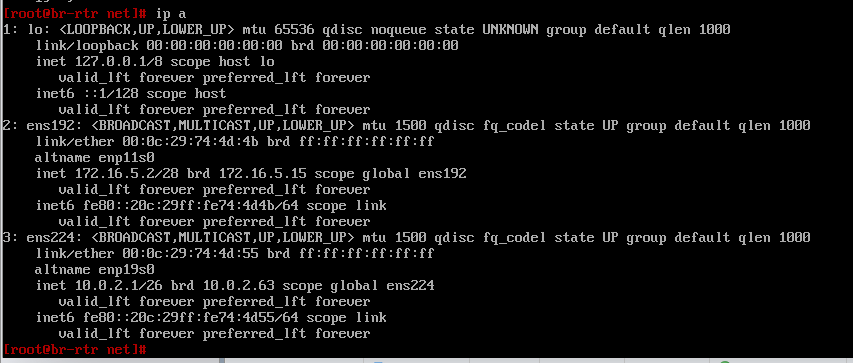
Установка такая же, как и в [пункте 2.2](#_2.2_Установка_и). Но нужно уточнить. На обоих роутерах создаём те же файлы, что при базовой настройке (options, ipv4address, ipv4route)

На HQ-RTR прописываем 2 подсети – для сервера и клиента

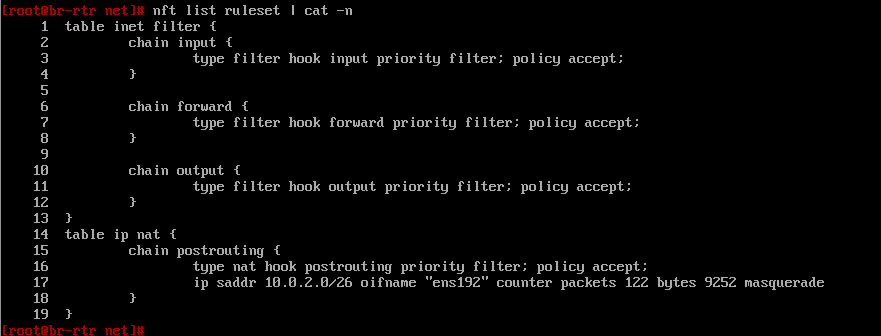


Nftables на HQ-RTR

На BR-RTR прописываем 1 подсеть и настраиваем оставшийся интерфейс



IP-адрес оставшегося интерфейса BR-RTR



nftables на BR-RTR

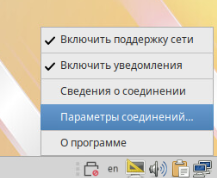
**4. Настройка SRV**

Базовая настройка. Настроить интерфейс, прописать адрес и шлюз, чтобы был доступ в интернет.

Создать в директории интерфейса файлы **options** (если не создан), **ipv4address (172.16.4.2/28), ipv4route (default via 172.16.4.1)**

**5. Настройка клиента HQ-CLI (завершение пункта задания 8 про интернет на всех устройствах)**

Для того, чтобы настроить IP-адрес на клиенте, нужно нажать ПКМ на значок сетевого соединения с двумя мониторами.



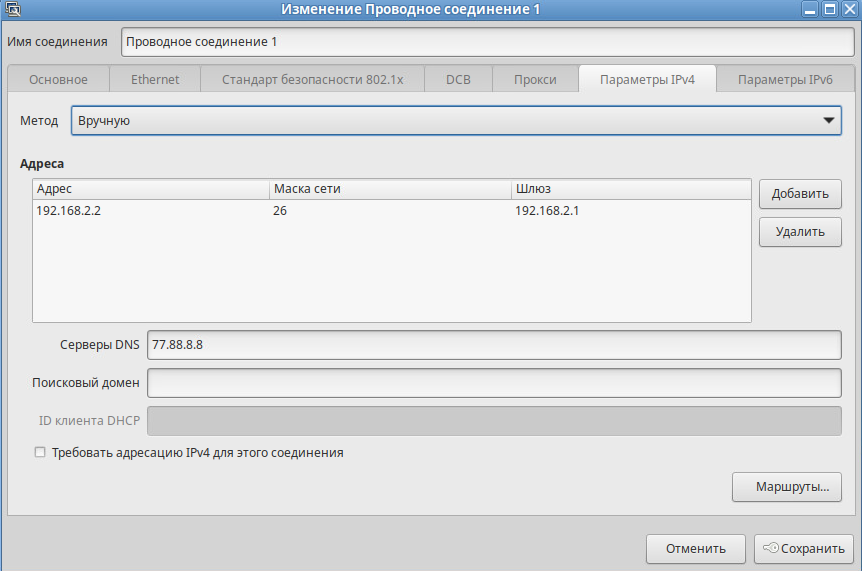
Далее нужно зайти в «параметры соединений» и выбрать проводное подключение. Основная настройка происходит в «Параметры IPV4». Выбрать метод «вручную». Прописать:

адрес 192.168.2.2

маску 26

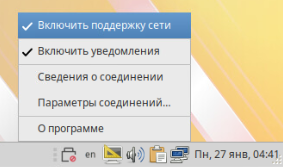
шлюз 192.168.2.1

DNS 77.88.8.8 (днс Яндекса)



Окно настроек

После этого нужно перезапустить сеть на компе. Для этого нужно включить и выключить «Поддержку сети».



После этого проверить, пропинговав шлюз и днс. Может быть такое, что пинговать не будет, потому что сетевая карта не включена и/или соединение неправильно. Сделать это нужно в «Edit settings» виртуалки.

**Задание 3. Создание локальный учётных записей (sshuser на серверах HQ-SRV и BR-SRV)**

Задание 3. Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV

Условия. Пароль пользователя sshuser – P@ssw0rd. Идентификатор пользователя 1010. Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации.

Команды:

adduser sshuser -u 1010

passwd sshuser

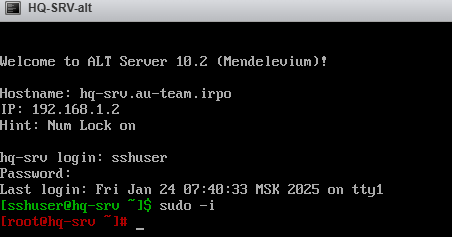
P@ssw0rd (вводим новый пароль)

P@ssw0rd (подтверждаем новый пароль)

echo "sshuser ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers

usermod -aG wheel sshuser

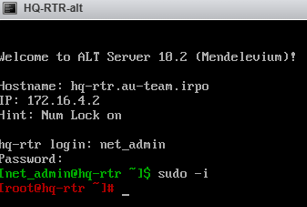
Чтобы проверить, выходим из текущего пользователя и заходим на юзера sshuser. Для выхода из пользователя нужно написать **exit** или нажат**ь CTRL+D.** Вводим логин и пароль нового юзера. Вводим **sudo -i.** Если зашли в root пользователя, то всё правильно сделано.



Проверка на серверах

Вторая часть задания. Создайте пользователя net\_admin на маршрутизаторах HQ-RTR и BR-RTR.

Те же самые команды, но только уже на роутерах и с логином net\_admin.



Проверка на роутерах

**Задание 5. Настройка безопасного удалённого доступа на серверах HQ-SRV и BR-SRV**

По заданию нужно использовать порт 2024, разрешить подключение только пользователю sshuser, ограничить количество попыток до 2-ух и настроить баннер «Authorized access only».

Меняем стандартный порт ssh (который 22) на порт согласно заданию (2024):

sed -i «s/#Port 22/Port 2024/g» /etc/openssh/sshd\_config

Перезапускаем службу sshd:

systemctl restart sshd

В папке /etc создаём файл **banner:**

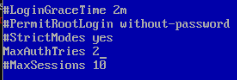
touch banner

Для того, чтобы выводился баннер, нужно в только что созданном файле **banner** написать «Authorized access only».



Теперь нужно отредактировать конфиг **sshd\_config**. Он находится в директории /etc/openssh.

В конфиге нужно изменить строчку MaxAuthTries 2



Для ограничения по логину пользователя написать строчку в конце конфига **AllowUsers sshuser**

Для вывода баннера добавить слово Banner с его директорией, в которой он находится:

Banner /etc/banner



Для подключения по ssh нужно написать следующую команду:

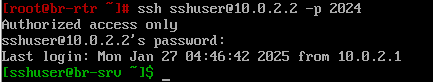
ssh sshuser@10.0.2.2 -p 2024

sshuser – имя юзера, на которого заходим

10.0.2.2 – IP-адрес

2024 – номер порта

Пароль для sshuser P@ssw0rd, который был создан в задании 3.



**Задание 6. IP-туннель**

Между офисами HQ и BR необходимо сконфигурировать ip туннель.

Необходимо создать директорию для туннельного интерфейса. Создаём новую директорию tun1 в /etc/net/ifaces.

Затем создаём в этой директории файл **options**

touch options

В файле записываем следующие строчки:

TYPE=iptun

TUNTYPE=gre

TUNLOCAL=172.16.4.2

TUNREMOTE=192.168.1.2

TUNOPTIONS='ttl 64'

HOST=ens192

**TUNLOCAL –** IP-адрес интерфейса, который получает адрес от ISP

**TUNREMOTE –** IP-адрес интерфейса второго роутера, который получает адрес от ISP

Назначаем IPv4 адрес на туннельный интерфейс. Это можно сделать с помощью команды или создать файл в mc. Создать файл **ipv4address.** В нём нужно вписать адрес из диапазона частных ip-адресов (172.16.100.1/28)

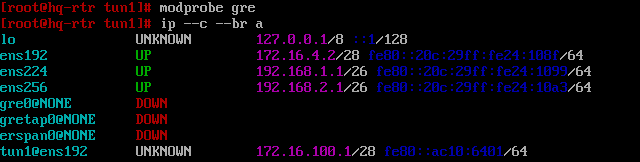
или echo 172.16.100.1/28 > /etc/net/ifaces/tun1/ipv4address

Затем перезапускаем интернет:

systemctl restart network

Включаем модуль ядра для gre:

modprobe gre



На другом роутере настройки аналогичны, но адреса TUNLOCAL и TUNREMOTE поменяны местами.

Туннель поднят, но не пингуются ротуеры между собой. Для этого нужно настроить OSPF.

**Задание 7. Настройка OSPF**

Установим пакет frr:

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

В конфигурационном файле /**etc/frr/daemons** необходимо активировать выбранный протокол для дальнейшей реализации его настройки:

строчку **ospfd=no** изменить на **ospfd=yes**

Включаем автозагрузку:

systemctl enable --now frr

Проверяем командой ss -tulpn | grep ospf



Настраиваем OSPFv2 - переходим в интерфейс frr. Для этого входим при помощи команды:

vtysh

Заходим в терминал:

configure terminal

По очереди пишем следующие команды:

router ospf

passive-interface default

network 172.16.100.0/28 area 0 (подсетка для туннеля между роутерами)

network 192.168.2.0/26 area 0 (подсетка до клиента)

network 192.168.1.0/26 area 0 (подсетка до HQ-SRV)

//**Для BR-RTR прописываем только 2 подсетки – туннельная и до BR-SRV//**

после этого пишем exit и заходим в интерфейс tun1:

exit

interface tun1

Для того, чтобы сделать его активным, нужно прописать следующие команды:

no ip ospf network broadcast

no ip ospf passive

ip ospf authentication-key PLAINPAS

ip ospf authentication

ip ospf authentication-key PLAINPAS

exit

do wr mem (сохранение конфигурации)



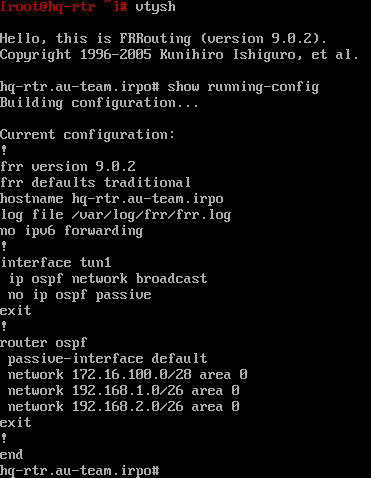
Проверяем командами:

vtysh

show running-config



BR-RTR



HQ-RTR

Если пароль не написали при настройке интерфейса. Прописываем:

vtysh

configure terminal

router ospf

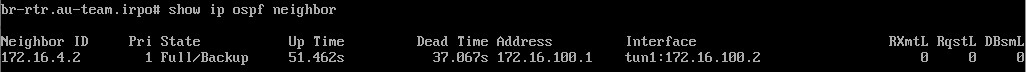
interface tun1

Если забыли прописать пароль при настройке интерфейса, то порядок команд такой:

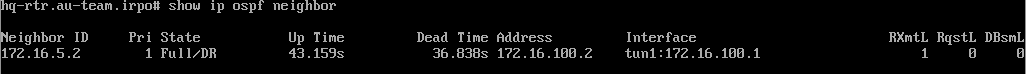
ip ospf authentication-key PLAINPAS

ip ospf authentication

Для проверки наших соседов вводим команду **show ip ospf neighbor**



BR-RTR



HQ-RTR

Для проверки работы OSPF нужно пингануть с одного сервера другой сервер. Если пингуется, то OSPF работает.



**Задание 8**

Настройка динамической трансляции адресов.

● Настройте динамическую трансляцию адресов для обоих офисов.

● Все устройства в офисах должны иметь доступ к сети Интернет

Если IP-адреса выданы, шлюзы прописаны, днс написан, интерфейсы настроены, то интернет будет. Для проверки интернета нужно пингануть DNS:

ping 77.88.8.8 или ping 8.8.8.8

**Задание 9. DHCP**

Установка dhcp:

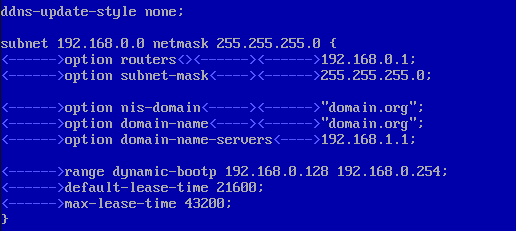
apt-get install dhcp-server

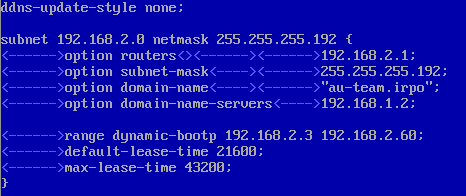
Настройка происходит в директории **/etc/dhcp**

В этой директории есть файл **dhcpd.conf.sample.** Этот файл копируем в mc при помощи сочетании клавиш **SHIFT+F5.** Меняем название на **dhcpd.conf**



Пример файла





Пример уже настроенного конфига

В этом файле:

subnet 192.168.2.0 (подсеть, которая идёт к клиенту)

netmask 255.255.255.192 (смотрим на префикс IP-адреса и пишем маску)

option routers 192.168.2.1 (IP-адрес роутера, который направлен в сторону клиента)

option subnet-mask 255.255.255.192 (маска)

строчку option nis-domain **удаляем**

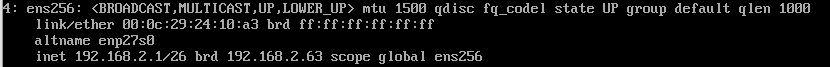
option domain-name "au-team.irpo" (DNS-суффикс написан в задании)

option domain-name-servers 192.168.1.2 (IP-адрес HQ-SRV)

range dynamic-bootp 192.168.2.3 192.168.2.60 (так как 192.168.2.1 и 192.168.2.2 заняты, то указываем, что с 192.168.2.3, а 192.168.2.60 берём из ip-калькулятора)

Сохраняем и выходим из файла. Затем заходим в **/etc/sysconfig/dhcpd** и указываем сетевой интерфейс, на котором будет работать DHCP-сервер





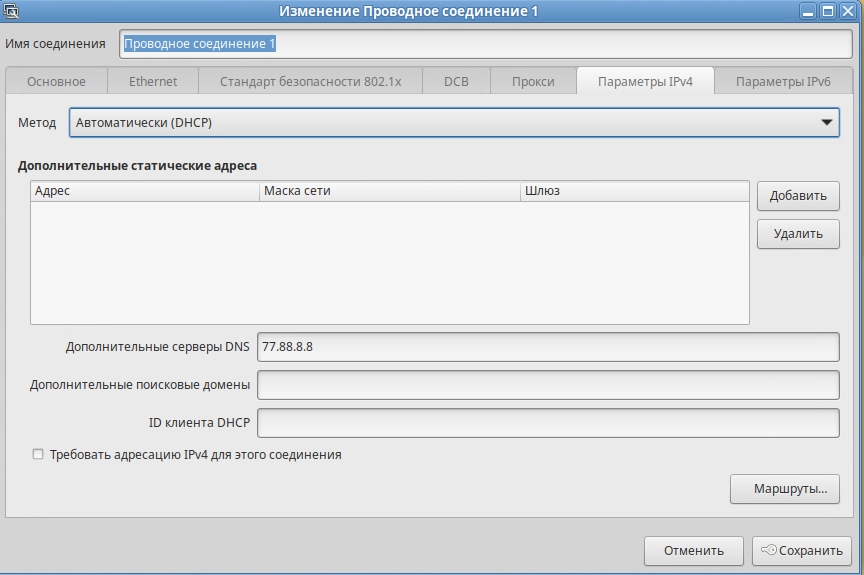
Выбираем тот интерфейс, который идёт к клиенту.

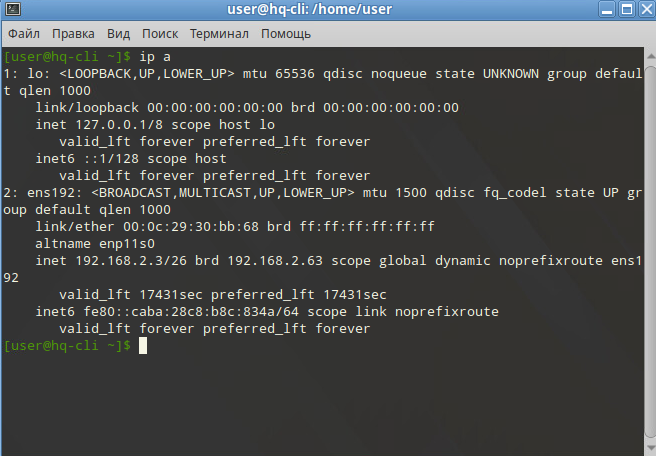
Добавление dhcp в автозагразку:

chkconfig dhcpd on

service dhcpd start

Запускаем HQ-CLI. Заходим в параметры проводных подключений. Переходим в Параметры IPv4. Выставляем метод «Автоматически (DHCP)» и удаляем статический адрес. Затем перезапускаем сеть (выключить поддержку и включить поддержку сети)





Изменённый IP-адрес, значит, DHCP работает

**Настройка DNS (Задание 10)**

Перед установкой на всякий случай прописать **apt-get update**

Для установки:

apt-get install bind

apt-get install bind-utils

Для добавления в автозагрузку написать команду:

systemctl enable --now bind

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

name\_servers=127.0.0.1

Далее пишем команду:

resolvconf -u

Для проверки интернета пишем cat /etc/resolv.conf и пингуем 77.88.8.8

В директории /etc/bind/ заходим в файл **local.conf** и описываем необходимые зоны согласно заданию:

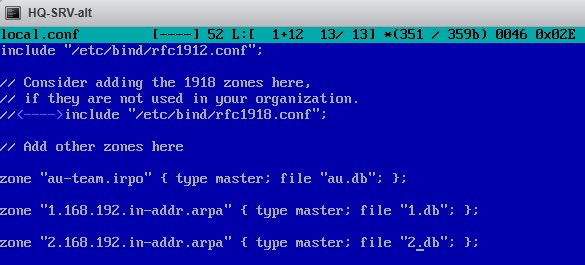
zone "au-team.irpo" { type master; file "au.db"; };

zone "1.168.192.in-addr.arpa" { type master; file "1.db"; };

zone "2.168.192.in-addr.arpa" { type master; file "2.db"; };

**au-team.irpo –** название из таблицы 2

**1.168.192 –** взять ip-адресацию между HQ-RTR и HQ-SRV и написать адрес обратной зоны (192.168.1.0 > 1.168.192)



Копируем примеры файлов для зон прямого просмотра по пути **/etc/bind/zone:**

cp /etc/bind/zone/{localdomain,au.db}

//**au.db, 1.db, 2.db –** названия файлов//

Копируем примеры файлов для зон обратного просмотра:

cp /etc/bind/zone/{127.in-addr.arpa,1.db}

cp /etc/bind/zone/{127.in-addr.arpa,2.db}

Задаём необходимые права:

chown root:named /etc/bind/zone/{au,1,2}.db

https://sysahelper.ru/mod/page/view.php?id=161

**Настройка часового пояса (Задание 11)**

Устанавливаем пакеты часовых поясов:

apt-get install tzdate

И выбираем пояс:

timedatectl set-timezone Asia/Novosibirsk

Проверяем время через команду:

timedatectl