

ИЗМЕНЕНИЯ:

У всех теперь ISP будет на AltJeOS

AltJeOS ничем не отличается от обычного AltServer, это просто пустышка, редактирования файла через vim, службы устанавливаете через интернет

На HQ-RTR теперь два интерфейса ISP-HQ и HQ-NET

HQ-SW – виртуальный коммутатор, настраиваете его через openvswitch

DNS и DHCP теперь настраиваем через службу dnsmasq

Везде пароли root/toor

HQ-CLI user/P@ssw0rd

1. Проведите базовую настройку устройств

!!!На всех машинах после настройки интерфейсов прописать в файл /etc/resolv.conf nameserver 77.88.8.8!!!

!!На всех машинах не забываем включать net.ipv4.ip\_forward=1

!!!ПРИ НАСТРОЙКЕ ИНТЕРФЕЙСОВ ОРИЕНТИРУЙТЕСЬ НА MAC АДРЕСА!!!

!!!ЕСЛИ У ВАС НА ISP СЛЕТАЕТ resolv.conf ТО ПРОПИСЫВАЕТЕ ЕГО НА ИНТЕРФЕЙС, КОТОРЫЙ ДАЕТ ИНЕТ!!! ИМЯ УСТРОЙСТВ МЕНЯЕТЕ ЧЕРЕЗ КОМАНДУ

hostnamectl set-hostname имя-виртуалки;exec bash

- Настройке имена устройств согласно топологии. Используется полное доменное имя.

Список названий:

ISP

HQ-RTR.au-team.irpo

BR-RTR.au-team.irpo

HQ-SRV.au-team.irpo

BR-SRV.au-team.irpo

HQ-CLI.au-team.irpo

HQ-SW.au-team.irpo

1. На всех устройствах необходимо сконфигурировать IPv4 ISP: mkdir /etc/net/ifaces/ens3/ mkdir /etc/net/ifaces/ens4/ mkdir /etc/net/ifaces/ens5/ cp –R /etc/net/ifaces/default/options /etc/net/ifaces/ens3/ cp –R /etc/net/ifaces/default/options /etc/net/ifaces/ens4/ cp –R /etc/net/ifaces/default/options /etc/net/ifaces/ens5/

vim /etc/net/ifaces/ens3/options

TYPE=eth

BOOTPROTO=dhcp

ONBOOT=yes DISABLED=no

vim /etc/net/ifaces/ens4/options

TYPE=eth

BOOTPROTO=static

ONBOOT=yes DISABLED=no

vim /etc/net/ifaces/ens4/ipv4address

172.16.4.1/28

vim /etc/net/ifaces/ens5/options

TYPE=eth

BOOTPROTO=static

ONBOOT=yes DISABLED=no

vim /etc/net/ifaces/ens5/ipv4address 172.16.5.1/28

* НА МАШИНЕ HQ-RTR

mkdir /etc/net/ifaces/ens3/

cp –R /etc/net/ifaces/default/options /etc/net/ifaces/ens3

mcedit /etc/net/ifaces/ens3/options

TYPE=eth

BOOTPROTO=static

ONBOOT=yes DISABLED=no

mcedit /etc/net/ifaces/ens3/ipv4address

172.16.4.2/28

mcedit /etc/net/ifaces/ens3/ipv4route default via 172.16.4.1 mkdir /etc/net/ifaces/ens4/ mcedit /etc/net/ifaces/ens4/options

TYPE=eth

BOOTPROTO=static

* Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов mkdir /etc/net/ifaces/ens4.100/ mcedit /etc/net/ifaces/ens4.100/options

TYPE=vlan

VID=100

HOST=ens4

BOOTPROTO=static ONBOOT=yes

mcedit /etc/net/ifaces/ens4.100/ipv4address 192.168.100.1/26

* Локальная сеть в сторону HQ-CLI(VLAN20) должна вмешать не более 16 адресов mkdir /etc/net/ifaces/ens4.200/ mcedit /etc/net/ifaces/ens4.200/options

TYPE=vlan

VID=200

HOST=ens4

BOOTPROTO=static ONBOOT=yes

mcedit /etc/net/ifaces/ens4.200/ipv4address 192.168.100.97/28

* Локальная сеть для управления (VLAN999) должна вмещать не более 8 адресов mkdir /etc/net/ifaces/ens4.999/ mcedit /etc/net/ifaces/ens4.999/options

TYPE=vlan

VID=999

HOST=ens4

BOOTPROTO=static ONBOOT=yes

mcedit /etc/net/ifaces/ens4.999/ipv4address 192.168.100.113/29

* НА МАШИНЕ BR-RTR

mkdir /etc/net/ifaces/ens3/

cp –R /etc/net/ifaces/default/options /etc/net/ifaces/ens3/

mcedit /etc/net/ifacec/ens3/options

TYPE=eth

BOOTPROTO=static

ONBOOT=yes

DISABLED=no

mcedit /etc/net/ifaces/ens3/ipv4address

172.16.5.2/28

mcedit /etc/net/ifaces/ens3/ipv4route default via 172.16.5.1

* Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов mkdir /etc/net/ifaces/ens4/

cp –R /etc/net/ifaces/default/options /etc/net/ifaces/ens4/

mcedit /etc/net/ifacec/ens4/options

TYPE=eth

BOOTPROTO=static

ONBOOT=yes DISABLED=no

mcedit /etc/net/ifaces/ens4/ipv4address 192.168.100.65/27

* НА МАШИНЕ HQ-SRV

mkdir /etc/net/ifaces/ens3/ mcedit /etc/net/ifaces/ens3/options

TYPE=eth

BOOTPROTO=static ONBOOT=yes

mcedit /etc/net/ifaces/ens3/ipv4address

192.168.100.2/26

mcedit /etc/net/ifaces/ens3/ipv4route default via 192.168.100.1

* НА МАШИНЕ BR-SRV

mkdir /etc/net/ifaces/ens3/

cp –R /etc/net/ifaces/default/options /etc/net/ifaces/ens3/ mcedit /etc/net/ifaces/ens3/options

TYPE=eth

BOOTPROTO=static

ONBOOT=yes DISABLED=no

mcedit /etc/net/ifaces/ens3/ipv4address

192.168.100.66/27

mcedit /etc/net/ifaces/ens3/ipv4route default via 192.168.100.65

2. Настройка ISP

- На ISP настройте динамическую сетевую трансляцию в сторону HQ-RTR и BR-RTR для доступа к сети интернет

apt-get update && apt-get install iptables –y

iptables –t nat –A POSTROUTING –o ens3 –s 172.16.0.0/16 –j MASQUERADE

iptables-save –f /etc/sysconfig/iptables iptables-save > /etc/sysconfig/iptables

3. Настройка виртуального коммутатора

На HQ-SW уже предустановлен opevswitch, для его работы достаточно его включить systemctl enable --now openvswitch

Далее нужно включить все интерфейсы, их должны быть 3 mkdir /etc/net/ifaces/ens3/ mkdir /etc/net/ifaces/ens4/ mkdir /etc/net/ifaces/ens5/ mcedit /etc/net/ifaces/ens3/options

TYPE=eth

BOOTPROTO=static

mcedit /etc/net/ifaces/ens4/options

TYPE=eth

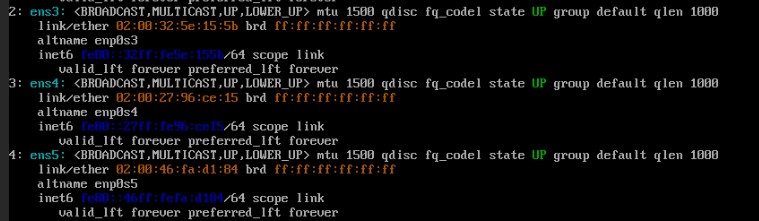
BOOTPROTO=static

mcedit /etc/net/ifaces/ens5/options

TYPE=eth

BOOTPROTO=static

Все интерфейсы должны быть подняты



Далее переходим к настройке opevswitch, **!!!ОРИЕНТИРУЙТЕ КУДА СМОТРЯТ ИНТЕРФЕЙСЫ ПО MAC-АДРЕСАМ!!!**

ovs-vsctl add-br hq-sw

ovs-vsctl add-port hq-sw ens3 trunks=100,200,999 ovs-vsctl add-port hq-sw ens4 tag=200 ovs-vsctl add-port hq-sw ens5 tag=100

После настройки openvswitch вам обязательно нужно включить модуль ядра modprobe 8021q

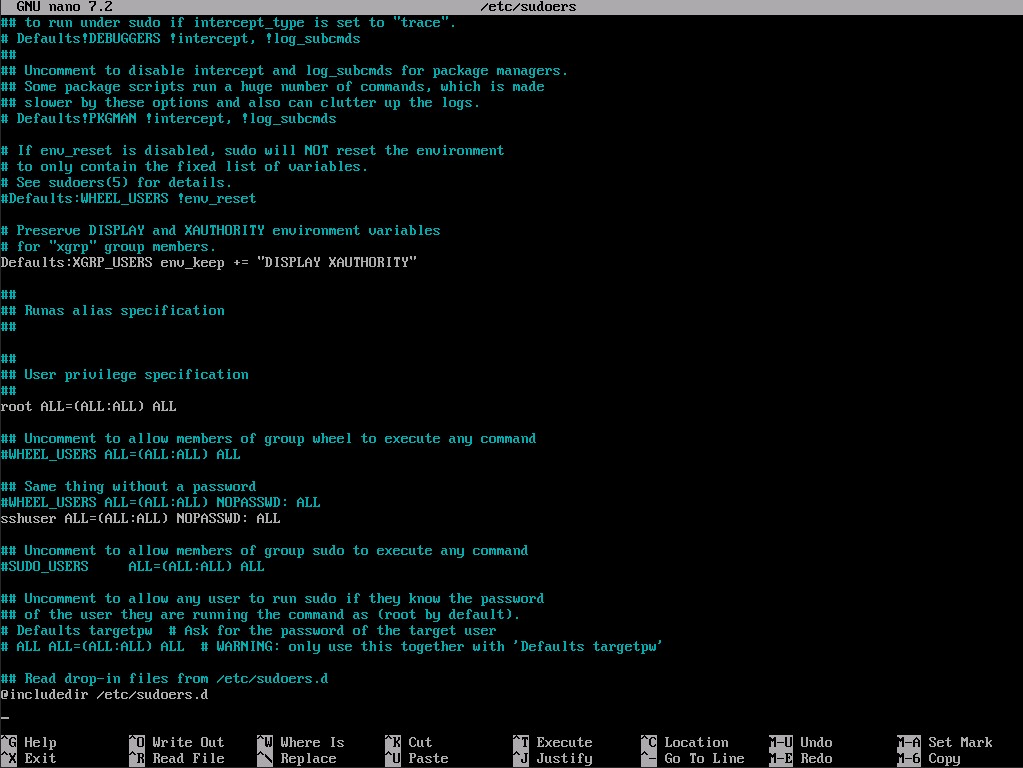
4. Создание локальных учетных записей

* Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV НА МАШИНАХ HQ-SRV и BR-SRV

adduser sshuser passwd sshuser

P@ssw0rd

usermod –u 1010 sshuser nano /etc/sudoers

 gpasswd –a sshuser wheel control sudowheel enabled

* На машинах HQ-RTR и BR-RTR создайте пользователя net\_admin НА МАШИНАХ HQ-RTR и BR-RTR

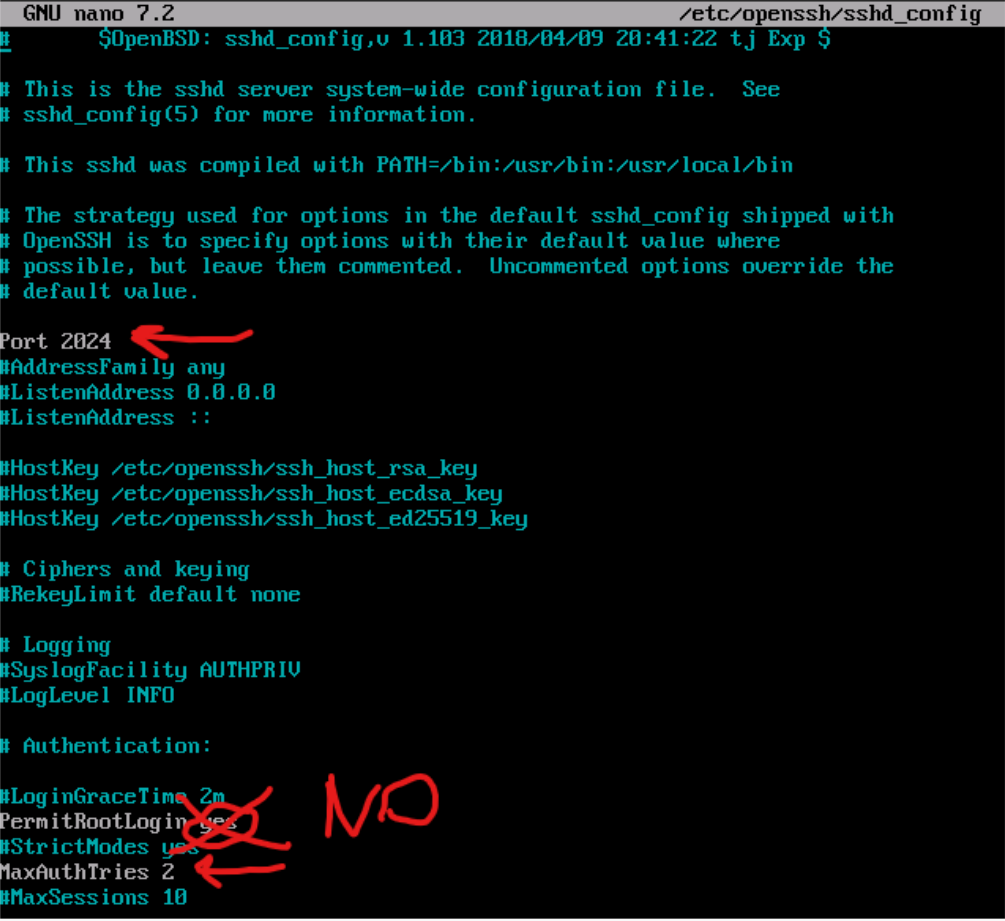
adduser net\_admin passwd net\_admin P@ssw0rd

После переходите /etc/sudoers и прописываете так же пользователя net\_admin, как sshuser gpasswd –a net\_admin wheel control sudowheel enabled

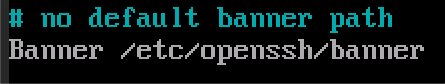
5. Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV

На машинах HQ-SRV и BR-SRV

Переходите в файл /etc/openssh/sshd\_config



Пролистываем ниже и находим строчку PasswordAuthentication и ставим “yes” Затем, в этом же конфиге спускаемся ниже и ищем данные строчки на скрине ниже, прописываем путь сами



После сохранения конфига sshd, переходим по пути, который мы написали mcedit /etc/openssh/banner и пишем “Authorized access only”



После всех действий рестартнем сервис systemctl restart sshd, после вы можете проверить что настройки и баннер есть путем захода по ssh на противоположную машину на sshuser@ipaddress Вы должны ввести пароль два раза неправильно и вас выкинет из ssh, а при первом коннекте выдаст баннер, который вы указали.

6. Между офисами HQ и BR необходимо сконфигурировать IP туннель HQ-RTR

mkdir /etc/net/ifaces/gre1/ mcedit /etc/net/ifaces/gre1/options  mcedit /etc/net/ifaces/gre1/ipv4address

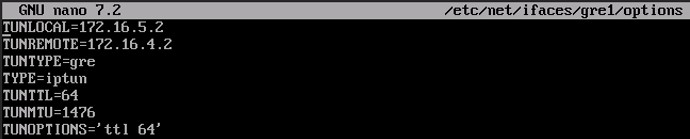
10.0.0.1 peer 10.0.0.2

После перезагружаем network [systemctl restart network]

У вас должен появится интерфейс gre1 с IP-адресом и статусом UNKNOW

На BR-RTR

mkdir /etc/net/ifaces/gre1/ mcedit /etc/net/ifaces/gre1/options

 mcedit /etc/net/ifaces/gre1/ipv4address

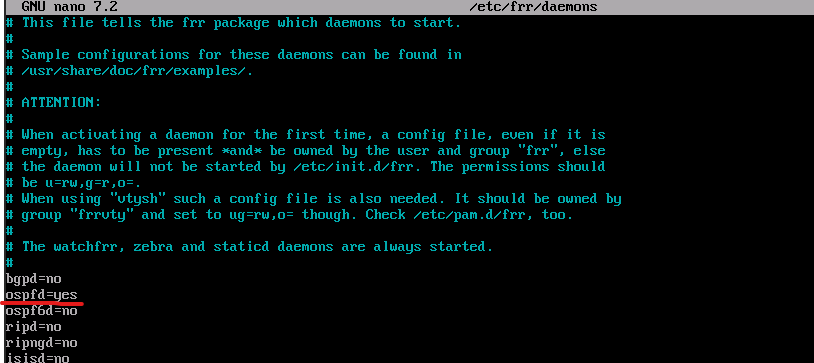
10.0.0.2 peer 10.0.0.1

После перезагружаем network [systemctl restart network]

7. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.

- На машинах HQ-RTR и BR-RTR устанавливаем службу FRR [apt-get install frr –y] После установки на обеих машинах заходим в конфигурационный файл службы /etc/frr/daemons и включаем демон ospfd.

После обязательно перезагружаем службу frr [systemctl enable --now frr]



На HQ-RTR

vtysh conf t

ip forwarding router ospf network 10.0.0.0/30 area 1 network 192.168.100.0/26 area 1 network 192.168.100.96/28 area 1 network 192.168.100.112/29 area 1

end

wr

На BR-RTR vtysh

conf t

ip forwarding router ospf network 10.0.0.0/30 area 1 network 192.168.100.64/27 area 1

end

wr

exit

На BR-RTR должны появится подсети с HQ-RTR



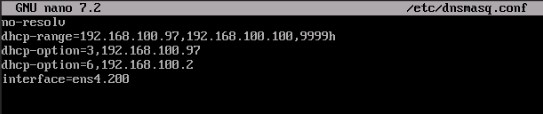
1. Настройка динамической трансляции адресов На HQ-RTR и BR-RTR

iptables –t nat –A POSTROUTING –o ens3 –j MASQUERADE

iptables-save > /etc/sysconfig/iptables systemctl enable –now iptables

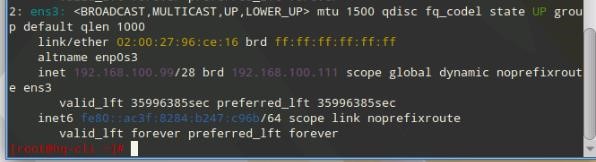
1. Настройка протокола динамической конфигурации хостов На машине HQ-RTR

apt-get install dnsmasq –y rm –rf /etc/dnsmasq.conf mcedit /etc/dnsmasq.conf

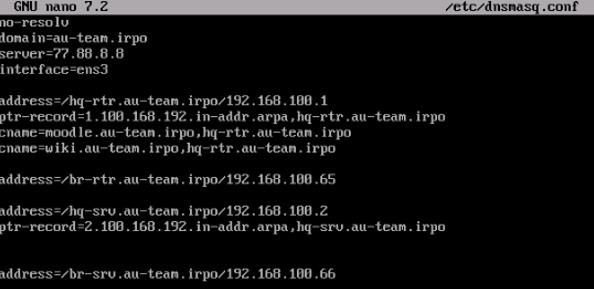


После включаем службу dnsmasq [systemctl enable --now dnsmasq]

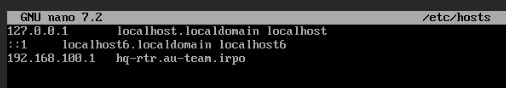
НА HQ-CLI сразу же появляется IP адрес по DHCP

10. Настройка DNS для офисов HQ и BR На машине HQ-SRV

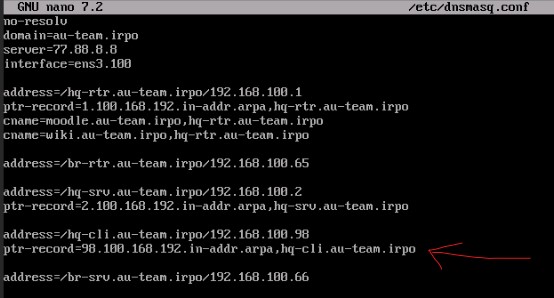
apt-get install dnsmasq -y rm -rf /etc/dnsmasq.conf mcedit /etc/dnsmasq.conf



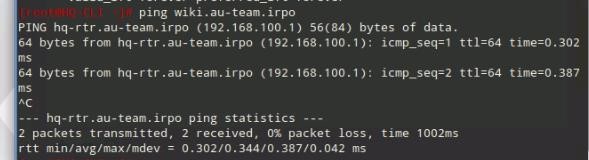
После переходите в /etc/hosts



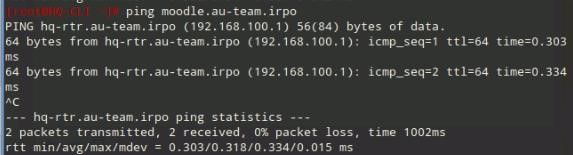
После того, как HQ-CLI получил ip адрес от DHCP вы его вручную добавляете в dnsmasq



На клиенте проверяете пинги wiki.au-team.irpo



moodle.au-team.irpo



10. Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена На всех машинах:



На ISP

apt-get install tzdata systemd systemctl restart systemd-timedated

timedatectl set-timezone Europe/Moscow