**Задание 1 настройка имён.**

**ISP (jeos)**

hostnamectl set-hostname isp; exec bash

**HQ-RTR (ecorouter)**

hostname hq-rtr

ip domain-name au-team.irpo

write memory

**HQ-SRV (alt)**

hostnamectl set-hostname hq-srv.au-team.irpo; exec bash

**HQ-CLI**

Через графический интерфейс задаем имя

hq-cli.au-team.irpo

Перезагрузить машину

**BR-RTR**

hostname br-rtr

ip domain-name au-team.irpo

write memory

**BR-SRV**

hostnamectl set-hostname br-srv.ae-team.irpo; exec bash

**Задание 1 настройка IP-адресов.**



**HQ-RTR**

показывает порты

show port br

создание логического интерфейса в сторону ISP

interface isp

description “connect isp”

ip address 172.16.4.14/28

exit

сведения физического порта

do sw port te0

привязка физического и логического портов

port te0

servise-instance te0/isp

encapsulation untagged

connect ip interface isp

exit

создание интерфейса для влана 100

interface vl100

description “server vlan 100”

ip address 192.168.100.1/26

exit

создание интерфейса для влана 200

interface vl200

description “clients vlan 200”

ip address 192.168.100.65/28

exit

создание интерфейса для влана 999

interface vl999

description “managements vlan 999”

ip address 192.168.100.81/29

привязка интерфейса te1 к влану 100

port te1

service-instance te1/vl100

encapsulation dotlq 100 exact

rewrite pop 1

connect ip interface vl100

exit

привязка интерфейса te1 к влану 200

service-instance te1/vl200

encapsulation dotlq 200 exact

rewrite pop 1

connect ip interface vl200

exit

привязка интерфейса te1 к влану 999

service-instance te1/vl999

encapsulation dotlq 999 exact

rewrite pop 1

connect ip interface vl999

exit

сохранение

write memory

проверка описания интерфейсов

do sh int description

проверка портов

do show int br

маршрутизация

ip route 0.0.0.0/0 172.16.4.1

проверка статических маршрутов

do show ip route static

**BR-RTR**

просмотр портов

show port br

создание логического интерфейса в сторону ISP

interface isp

description “connect isp”

ip address 172.16.5.14/28

привязка физического и логического портов

port te0

service-instance te0/isp

encapsulation untagged

connect ip interface isp

exit

маршрутизация

ip route 0.0.0.0/0 172.16.5.1

создание логического интерфейса в сторону BR

interface BR-Net

description “connect BR-Net”

ip address 192.168.200.1/27

exit

привязка физического и логического портов

port te1

service-instance te1/BR-Net

encapsulation untagged

connect ip interface BR-Net

exit

write memory

**HQ-SRV**

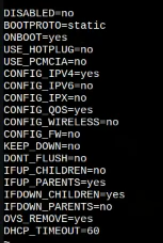
**Mcedit**- типа нано но не нано

Файл директории 18 интерфейса **/etc/net/ifaces/ens18/options** должен иметь вид:



TYPE=eth – обязательный параметр

Общий файл для всех интерфейсов /**etc/net/ifaces/default/options:**



cat - посмотреть файл

**Mcedit** – изменить файл

**НАСТРОЙКА ЧЕРЕЗ nmcli(можно на все по аналогии уебать)**

echo “nameserver 77.88.8.1 (интернет)”> /etc/net/ifaces/ens19/resolv.conf

systemctl restart network

systemctl enable --now NetworkManager

nmcli connection add type vlan con-name ens33 ifname ens33.100 dev ens33 id 100 ip4 192.168.100.2/26(IP самого интерфейса) gw4 192.168.100.1(гетевей)

**КОНЕЦ НАСТРОЙКИ ДАЛЬШЕ ХУЙНЯ**

mv /etc/net/ifaces/ens1{8,9}/ - изменить имя директории, если интерфейс не работает

Изменение параметра ens19

vim /etc/net/ifaces/ens19/options

оставляем

TYPE=eth

Прописываем IP

echo “192.168.100.2/26” > /etc/net/ifaces/ens19/ipv4address

echo “default via 192.168.100.1” > /etc/net/ifaces/ens19/ipv4route

echo “nameserver 77.88.8.1 (интернет)”> /etc/net/ifaces/ens19/resolv.conf

systemctl restart network

**HQ-CLI**

Графический интерфейс

Network Manager

Выбираем интерфейс и меняем на DHCP

Интерфейс -> Ipv4 -> DHCP

**BR-SRV**

Ip -c a

Изменение названия

mv /etc/net/ifaces/ens1{8,9}/

переход в файл

vim /etc/net/ifaces/ens19/options

оставляем

TYPE

systemctl enable --now NetworkManager

nmcli connection add type ethernet con-name ens33-static ifname ens33 ip4 192.168.200.2/27 gw4 192.168.200.1

Прописываем IP

echo “192.168.200.2/27” > /etc/net/ifaces/ens19/ipv4address

echo “default via 192.168.200.1” > /etc/net/ifaces/ens19/ipv4route

echo “nameserver 77.88.8.1 (интернет)”> /etc/net/ifaces/ens19/resolv.conf

systemctl restart network

**HQ-SRV**

systemctl enable --now NetworkManager

nmcli connection add type vlan con-name ens32 ifname ens32.100 dev ens32 id 100 ip4 192.168.100.2/26 gw4 192.168.100.1

**CLI**

systemctl enable --now NetworkManager

nmcli connection add type vlan con-name ens32 ifname ens32.200 dev ens32 id 200 ip4 192.168.100.66/28 gw4 192.168.100.65

**Задание 2 настройка ISP**

Интерфейсы

ip -c a

Проверка директории

ls /etc/net/ifaces/

Проверка значений

cat /etc/net/ifaces/ens19/options



Изменяем статические адреса

Меняем уже на nmtui вот так вот как снизу не меняем

echo “172.16.4.1/28” > /etc/net/ifaces/ens20/ipv4address

echo “172.16.5.1/28” > /etc/net/ifaces/ens21/ipv4addressNM

Заходим в файл и меняем значение

nano /etc/net/sysctl.conf

net.ipv4.ip\_forward = 1

systemctl restart network

Настройка NAT

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

Вывод интерфейсов

ip -c -br -4 a

Создание правила для интерфейса, который смотрит в сторону интернета

iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

Сохранение правила

iptables-save >> /etc/sysconfig/iptables

Добавление в автозагрузку

systemctl enable - -now iptables

Проверка наличия правила

iptables -t nat -L -n -v

**Задание 3 создание локальных учетных записей.**

**HQ-SRV**

Создание пользователя sshuser

useradd sshuser -u 1010

Проверка

id sshuser

Пароль для пользователя sshuser

passwd sshuser

P@ssw0rd

P@ssw0rd

Добавляем в группу wheel

usermod -aG wheel sshuser

Позволяем пользователю sshuser заходить в sudo без пароля

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

Пробуем перейти

su - sshuser

**BR-SRV**

Создание пользователя sshuser

useradd sshuser -u 1010

Проверка

id sshuser

Пароль для пользователя sshuser

passwd sshuser

P@ssw0rd

P@ssw0rd

Добавляем в группу wheel

usermod -aG wheel sshuser

Позволяем пользователю sshuser заходить в sudo без пароля

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

Пробуем перейти

su - sshuser

sudo -i

**HQ-RTR**

Создание пользователя net\_admin

username net\_admin

password P@$$word

role admin

write memory

Проверка пользователей

show users localdb

**BR-RTR**

Создание пользователя net\_admin

username net\_admin

password P@$$word

role admin

write memory

Проверка пользователей

show users localdb

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

**HQ-SRV**

Переходим в файл и меняем значение порта

mcedit /etc/openssh/sshd\_config

#Port 22 → Port

#Logging → (добавить) AllowUsers sshuser

#MaxAuthTries 6 → MaxAuthTries 2

Banner none → Banner /etc/openssh/banner

Выходим из файла и прописываем баннер

echo “Authorized access only” > /etc/openssh/banner

Перезагрузка сервиса ssh

systemctl restart sshd.service

Проверка

systemctl status sshd.service

ssh -p 2024 user@localhost → yes

Два раза неправильный пароль → не удалось войти → всё верно

ssh -p 2024 sshuser@localhost

P@ssw0rd

**BR-SRV**

Переходим в файл и меняем значение порта

mcedit /etc/openssh/sshd\_config

#Port 22 → Port 2024

#Logging → (добавить) AllowUsers sshuser

#MaxAuthTries 6 → MaxAuthTries 2

Banner none → Banner /etc/openssh/banner

Выходим из файла и прописываем баннер

echo “Authorized access only” >> /etc/openssh/banner

Перезагрузка сервиса ssh

systemctl restart sshd.service

Проверка

systemctl status ssh.service

ssh -p 2024 user@localhost → yes

Два раза неправильный пароль → не удалось войти → всё верно

ssh -p 2024 sshuser@localhost

P@ssw0rd

**Задание 6 настройка туннеля между офисами HQ и BR.**

**HQ-RTR**

Создание туннеля

interface tunnel.0

description “GRE-to-BR”

ip address 10.10.10.1/30

Указываем внешние адреса (внешний адрес hq-rtr и внешний адрес br-rtr)

ip tunnel 172.16.4.14 172.16.5.14 mode gre

write memory

Проверка

do show ip interface br

do show interface tunnel.0

**BR-RTR**

interface tunnel.0

description “GRE-to-HQ”

ip address 10.10.10.2/30

Указываем внешние адреса (внешний адрес br-rtr и внешний адрес hq-rtr)

ip tunnel 172.16.5.14 172.16.4.14 mode gre

write memory

Проверка

do show ip interface br

do show interface tunnel.0

Проверка связности

do ping 10.10.10.1

**Задание 7 динамическая маршрутизация между офисами HQ и BR, выбор протокола, его защита.**

**HQ-RTR**

Создание ospf

router ospf 1

Айди ospf

ospf router-id 10.10.10.1

Делаем порты пассивными, чтобы только роутеры могли обмениваться

passive-interface default

Исключаем из этого списка tunnel.0

no passive-interface tunnel.0

Объявляем сети

network 10.10.10.0/30 area 0

network 192.168.100.0/26 area 0

network 192.168.100.64/28 area 0

network 192.168.100.80/29 area 0

exit

Обеспечение защиты протокола посредством защиты паролем

interface tunnel.0

ip ospf authentication massage-digest

ip ospf message-digest-key 1 md5 P@ssw0rd

exit

write memory

Проверка

do show ip ospf interface tunnel.0

**BR-RTR**

Создание ospf

router ospf 1

Айди ospf

ospf router-id 10.10.10.2

Делаем порты пассивными, чтобы только роутеры могли обмениваться

passive-interface defaulf

Исключаем из этого списка tunnel.0

no passive-interface tunnel.0

Объявляем сети

network 10.10.10.0/30 area 0

network 192.168.200.0/27 area 0

exit

Обеспечение защиты протокола посредством защиты паролем

interface tinnel.0

ip ospf authentication message-digest

ip ospf massage-digest-key 1 md5 P@ssw0rd

exit

write memory

Проверка

do show ospf neighbor

do show ip route ospf

do show ip ospf interface tunnel.0

С сервера на сервер проводим ping (например, с BR-SRV)

ping -c3 192.168.100.2

**Задание 8 динамическая трансляция адресов (на роутерах необходимо реализовать NAT).**

**HQ-RTR**

Настройка интерфейсов

interface isp

ip nat outside

exit

interface vl100

ip nat inside

exit

interface vl200

ip nat inside

exit

interface vl999

ip nat inside

exit

Создание пула

ip nat pool HQ 192.168.100.1-192.168.100.254

ip nat source dynamic inside-to-outside pool HQ overload interface isp

write memory

Проверяем

show ip nat translations

Проверяем на HQ-SRV доступ в интернет

ping -c3 ya.ru

**BR-RTR**

Настройка интерфейсов

interface isp

ip nat outside

exit

interface BR-Net

ip nat inside

exit

Создание пула

ip nat pool BR 192.168.200.1-192.168.200.254

ip nat source dynamic inside-to-outside pool BR overload interface isp

write memory

Проверяем

show ip nat translations

Проверяем на BR-SRV доступ в интернет

ping -c3 ya.ru

**Задание 9 настройка протокола динамической конфигурации хостов.**

**HQ-RTR**

Создание пула адресов для раздачи

ip pool HQ 192.168.100.66-192.168.100.78

Создание DHCP

dhcp-server 1

pool HQ 1

mask 28

gateway 192.168.100.65

dns 192.168.100.2

domain-name au-team.irpo

exit

Привязка DHCP к интерфейсу

interface vl200

dhcp-server 1

write memory

**CLI**

Проверка ip адреса

ping 192.168.100.65

ping 77.88.8.1

**Задание 10 настройка DNS для BR и HQ.**

**HQ-SRV**

Установка bind

apt-get update && apt-get install bind bind utils -y

Открытие файла и изменение параметров

vim /etc/bind/options.conf

listen-on (127.0.0.1;); → listen-on (192.168.100.2;);

listen-on-v6 ( ::1; ); → listen-on-v6 (none;);

//forwarders { }; → forwarders { 77.88.8.1; };

//allow-qwery { localhosts; }; → allow-qwery { any; };

//allow-recursion { localhosts; }; → allow-recursion { any; };

Описание зон DNS

vim /etc/bind/rfc1912.conf

zone “au-team.irpo” {

type master;

file “au-team.irpo”;

};

zone “100.168.192.in-addr.arpa” {

type master;

file “100.168.192.in-addr.arpa”;

};

Копирование шаблона и открытие в vim

cp /etc/bind/zone/empty /etc/bind/zone/au-team.irpo

vim /etc/bind/zone/au-team.irpo

Замена localhost на au-team.irpo

%s/localhost/au-team.irpo

Добавление записей

IN NS au-team.irpo.

IN A 192.168.100.2

hq-srv IN A 192.168.100.2

Копирование файла и его редактирование

cp /etc/bind/zone/au-team.ipro /etc/bind/zone/100.168.192.in-addr.arpa

vim /etc/bind/zone/100.168.192.in-addr.arpa

IN NS au-team.irpo.

IN PTR hq-srv.au-team.irpo.

Изменение прав

chown root:named /etc/bind/zone/au-team.irpo

chown root:named /etc/bind/zone/100.168.192.in-addr.arpa

Проверка

systemctl enable –now bind

systemctl status bind.service

**CLI**

Проверка сервера

cat /etc/resolv.conf → Должно быть au-team.irpo

host hq-srv.au-team.irpo → hq-srv.au-team.irpo has address 192.168.100.2

host 192.168.100.2 → 2.100.168.192.in-addr.arpa domain name pointer hq-srv.au-team.irpo

host ya.ru

**Задание 11 настройка часового пояса.**

**BR-SRV**

Просмотр зоны

timedatectl

Установка времени

timedatactl set timezone

**HQ-RTR**

Просмотр зоны

do show ntp timezone

Установка времени

ntp timezone utc+5

write memory

**BR-RTR**

Просмотр зоны

do show ntp timezone

Установка времени

ntp timezone utc+5

write memory

**ISP**

Проверка

timedatectl

Установка пакета

apt-get install tzdata

Установка времени

timedatectl set-timezone Asia/Yekaterinburg