|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Шлюз |
| ISP | Ens18 | От провайдера |  |
|  | Ens 19 HQ-RTR | 172.16.4.1/28 |  |
|  | Ens20 BR-RTR | 172.16.5.1/28 |  |
| HQ-RTR | Ens18 ISP | 172.16.4.2/28 | 172.16.4.1 |
|  | Ens 19 HQ-SRV | 192.168.1.1/28 |  |
|  | Ens20 HQ-CLI | 192.168.2.1/27 |  |
|  | Ens99 | 192.168.99.1/27 |  |
| BR-RTR | Ens18 | 172.16.5.2/28 | 172.16.5.1 |
|  | Ens 19 | 192.168.10.1/26 |  |
| HQ-SRV | Ens18 | 192.168.1.2/28 | 192.168.1.1 |
|  | Ens 19 |  |  |
| BR-SRV | Ens18 | 192.168.10.2/26 | 192.168.10.1 |
|  | Ens 19 |  |  |
| HQ-CLI | Ens18 | По DHCP | 192.168.2.1 |
|  | Ens 19 |  |  |



hostname br-rtr.(pulsar.local), hq-rtr.()

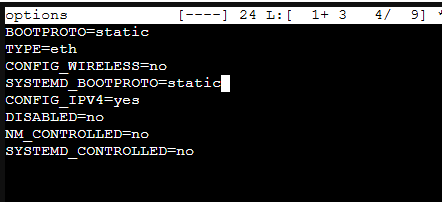
hostnamectl set-hostname hq-cli(), hq-srv(), br-srv(),

Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 16 адресов

Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 32 адресов

HQ-SRV

/etc/net/ifaces/ens18/options



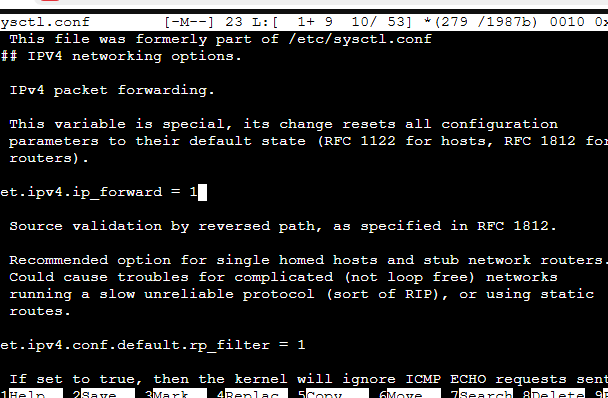
cd /etc/net/ifaces

echo 192.168.1.2/(28) >ipv4address

echo default via 192.168.1.1 > ipv4route

echo nameserver 8.8.8.8 > resolv.conf

/etc/net/sysctl.conf



Systemctl restart network

Настройка на HQ-RTR

Int ens18 (isp)

Ip add 172.16.4.2/28 (в задании указано к какой сети hq-rtr должен подключаться к isp)

port te0

service-instance 1

encapsulation untagged

conn ip int ens18

int ens19 (hq-srv)

ip add 192.168.1.1/(28)

port te1

service-instance 100

encapsulation dot1q 100

rewrite pop 1

conn ip int ens19

int ens20 (hq-cli)

ip add 192.168.2.1/(27)

port te1

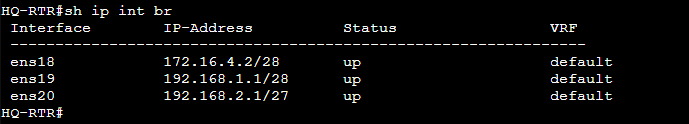
service-instance 200

encapsulation dot1q 200

rewrite pop 1

conn ip int ens20

Wr me and sh ip int br



внешние и внутренние интерфейсы,настраиваю NAT (так же hq-rtr)

int ens18

ip nat outside

int ens19

ip nat inside

int ens20

ip nat inside

Настройка DHCP на HQ-RTR (тут маска это маска интерфейса hq-cli от устройства hq-rtr)

ip pool HQ-CLI 192.168.2.1-192.168.2.30

dhcp-server 1

pool HQ-CLI

mask (27)

gateway 192.168.2.1

dns 8.8.8.8 (&&&&&&&&&&&&&&&&&&&&)

domain-name (pulsar).local

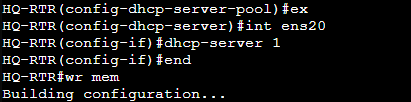
ex

int ens20

dhcp-server 1

ens

wr me



HQ-CLI по DHCP

mcedit /etc/net/sysctl.conf

systemctl restart NetworkManager

ip -c a

Локальная сеть в сторону BR-SRV должна вмещать не более 64 адресов

BR-SRV

mcedit /etc/net/ifaces/ens18/options

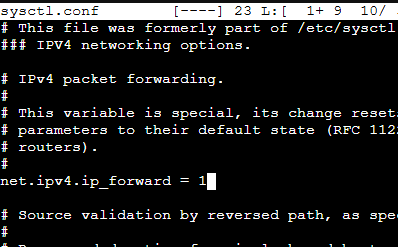
cd /etc/net/ifaces/ens18

echo 192.168.10.2./(26) > ipv4address

echo default via 192.168.10.1 > ipv4route

echo nameserver 8.8.8.8 > resolv.conf

mcedit /etc/net/sysctl.conf



systemctl restatrt network

ip -c a

Локальная сеть для управления (VLAN999) должна вмещать не более 32 адресов

Hq-rtr

int ens99

ip add 192.168.99.1/(27)

port te1

service-instance 999

encapsulation dot1q 999

rewrite pop 1

conn ip int ens99

end

wr me

Настройка ISP на ISP

cd /etc/net/ifaces

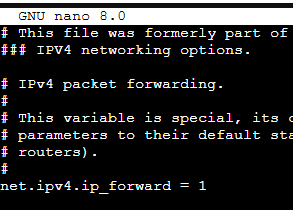
cp -r ens18 ens19

cp -r ens18 ens20

vim ens19/options

vim /ens19/ipv4address 172.16.4.1/28 (вроде везде 28)

vim /etc/net/sysctl.conf



vim /etc/net/ifaces/ens20/options

cd ens20

echo 172.16.5.1/28 > ipv4address

systemctl restart network

ip -c a

Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP. Настройте маршруты по умолчанию там, где это необходимо

HQ-RTR

ip route 0.0.0.0 0.0.0.0 172.16.4.1

end

wr me

BR-RTR

ip route 0.0.0.0 0.0.0.0 172.16.5.1

end

wr me

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

BR-RTR

en conf t

int ens18

ip add 172.16.5.2/28

ex

port te0

service-instance 1

encapsulation untagged

conn ip int ens18

int ens19

ip add 192.168.10.1/26

ex

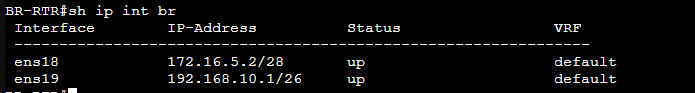
port te1

service-instance 1

encapsulation untagged

conn ip int ens19

sh ip int br

внешние и внутренние интерфейсы, настраиваю NAT (br-rtr)

int ens18

ip nat outside

int ens19

ip nat inside

ip nat pool BR 192.168.10.1-192.168.10.62 (судя по маске)

ip nat source dynamic inside-to-outside pool BR overload int ens18

end wr me

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

iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE

iptables-save -f /etc/sysconfig/iptables

systemctl enable –now iptables

# **Создание локальных учетных записей**

HQ-SRV и BR-SRV одинаково

useradd -p (P@ssw0rd quantumquokka)

usermod -u (1008) quantumquokka

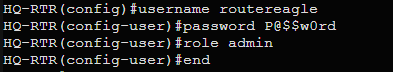
usermod -a -G wheel quantumquokka

HQ-RTR и BR-RTR

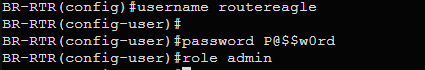
Создайте пользователя routereagle на маршрутизаторах HQ-RTR и BR-RTR

Пароль пользователя routereagle с паролем P@$$word

HQ-RTR



BR-RTR

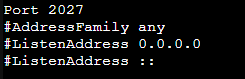


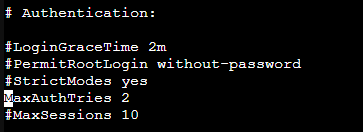
**Настройка безопасного удаленного доступа на серверах HQ-SRV и BRSRV:**

HQ-SRV и BR-SRV

Для подключения используйте порт 2027. Разрешите подключения только пользователю quantumquokka

mcedit /etc/openssh/sshd\_config





mcedit /etc/sudoers



echo “Banner /etc/openssh/bannermotd” >> /etc/openssh/sshd\_config

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

**Между офисами HQ и BR необходимо сконфигурировать ip туннель (сведения о туннеле отчет)**

HQ-RTR

en conf t

int tunnel.0

ip add 172.16.0.1/24

ip mtu 1400

ip tunnel 172.16.4.2 172.16.5.2 mode gre

BR-RTR

en conf t

int tunnel.0

ip add 172.16.0.2/24

ip mtu 1400

ip tunnel 172.16.5.2 172.16.4.2 mode gre

**Обеспечьте динамическую маршрутизацию (отчет):**

Разрешите выбранный протокол только на интерфейсах в ip туннеле

HQ-RTR

Тут я пишу айпи без ens18

en conf t

router ospf 1

ospf router-id 1.1.1.1

network 172.16.0.0/24 area 0.0.0.0

network 192.168.1.0/(28) area 0.0.0.0

network 192.168.2.0/(27) area 0.0.0.0

network 192.168.99.0/(27) area 0.0.0.0

BR-RTR

en conf t

router ospf 1

ospf router-id 2.2.2.2

network 172.16.0.0/24 area 0.0.0.0

network 192.168.10.0/(26) area 0.0.0.0

end wr me

HQ-RTR и BR-RTR

en conf t

router ospf 1

passive-interface default

no passive-interface tunnel.0

end wr me

защита на HQ-RTR и на BR-RTR (отчет)

int tunnel.0

ip ospf authentication-key ecorouter

**Настройка динамической трансляции адресов.**

На HQ-RTR и на BR-RTR

Я вывожу настройки командой

Hq-rtr show running-config interface ens18 (ens19, ens20)

Br-rtr show running-config interface ens18 (ens19)

И везде show running-config | include nat

**Настройка протокола динамической конфигурации хостов.**

HQ-RTR

int ens20

dhcp-server 1

**Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.**

HQ-RTR BR-RTR

conf t

ntp timezone utc+5

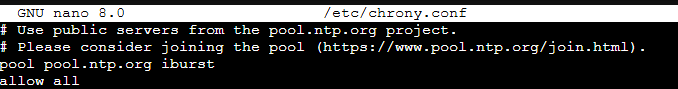
do sh clock

HQ-SRV BR-SRV

apt-get install chrony

vim /etc/chrony.conf

Добавляем строчку allow all



timedatectl set-timezone Asia/Yekaterinburg

timedatectl

HQ-CLI

vim /etc/chrony.conf

server 192.168.1.2

timedatectl set-timezone Asia/Yekaterinburg

timedatectl

Isp

Apt-get install chrony

vim /etc/chrony.conf

Добавляем строчку allow all

Apt-get install tzdata

timedatectl set-timezone Asia/Yekaterinburg

timedatectl