|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска** | **VLAN** | **Подсеть** | **Шлюз** |
| **ISP** | ens19 (к интернету) | DHCP | DHCP | - | DHCP | DHCP |
|  | ens20 (к HQ-RTR) | 172.16.4.1 | 255.255.255.240 | - | 172.16.4.0/28 | - |
|  | ens21 (к BR-RTR) | 172.16.5.1 | 255.255.255.240 | - | 172.16.5.0/28 | - |
| **HQ-RTR** | te0 (isp) | 172.16.4.2 | 255.255.255.240 | - | 172.16.4.0/28 | 172.16.4.1 |
|  | te1 (vl100) | 192.168.1.1 | 255.255.255.192 | 100 | 192.168.1.0/26 | - |
|  | te1 (vl200) | 192.168.1.65 | 255.255.255.240 | 200 | 192.168.1.64/28 | - |
|  | te1 (vl999) | 192.168.1.81 | 255.255.255.248 | 999 | 192.168.1.80/29 | - |
|  | tunnel.0 | 10.10.10.1 | 255.255.255.252 | - | 10.10.10.0/30 | - |
| **HQ-SRV** | ens19 | 192.168.1.2 | 255.255.255.192 | 100 | 192.168.1.0/26 | 192.168.1.1 |
| **HQ-CLI** | ens19 | DHCP | DHCP | 200 | 192.168.1.64/28 | DHCP |
| **BR-RTR** | te0 (isp) | 172.16.5.2 | 255.255.255.240 | - | 172.16.5.0/28 | 172.16.5.1 |
|  | te1 (к BR-SRV) | 192.168.5.1 | 255.255.255.224 | - | 192.168.5.0/27 | - |
| tunnel.0 | 10.10.10.2 | 255.255.255.252 | - | 10.10.10.0/30 | - |
| **BR-SRV** | ens19 | 192.168.5.2 | 255.255.255.224 | - | 192.168.5.0/27 | 192.168.5.1 |

**Модуль № 1:**

**Настройка сетевой инфраструктуры**

**Вид аттестации/уровень ДЭ:**

Задание:

Необходимо разработать и настроить инфраструктуру информационнокоммуникационной системы согласно предложенной топологии (см. Рисунок 1). Задание включает базовую настройку устройств:

• присвоение имен устройствам,

• расчет IP-адресации,

• настройку коммутации и маршрутизации.

В ходе проектирования и настройки сетевой инфраструктуры следует вести отчет о своих действиях, включая таблицы и схемы, предусмотренные в задании. Итоговый отчет должен содержать одну таблицу и пять отчетов о ходе работы. Итоговый отчет по окончании работы следует сохранить на диске рабочего места.

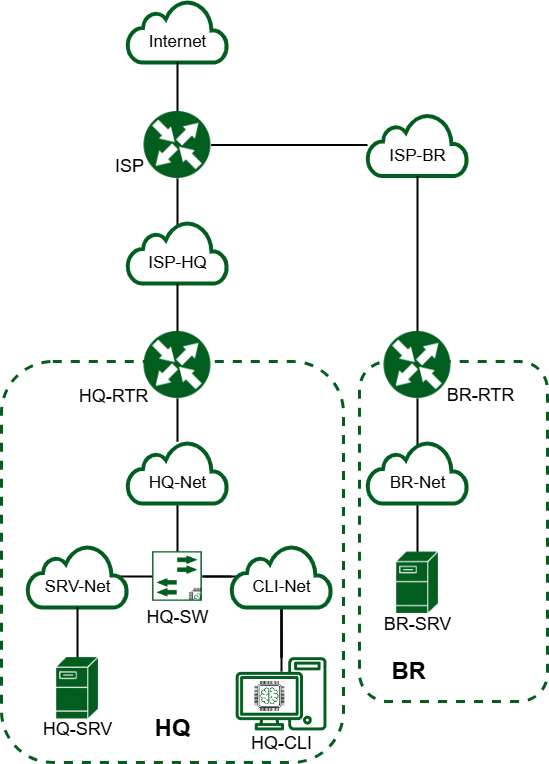


Рисунок 1. Топология сети

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Машина** | **RAM,**  **ГБ** | **CPU** | **HDD/SDD, ГБ** | **OS** |
| ISP | 1 | 1 | 10 | ОС Альт JeOS/Linux или аналог |
| HQ-RTR | 1 | 1 | 10 | ОС EcoRouter или аналог |
| BR-RTR | 1 | 1 | 10 | ОС EcoRouter или аналог |
| HQ-SRV | 2 | 1 | 10 | ОС Альт Сервер/аналог |
| BR-SRV | 2 | 1 | 10 | ОС Альт Сервер/аналог |
| HQ-CLI | 3 | 2 | 15 | ОС Альт Рабочая Станция/аналог |
| Итого | 10 | 7 | 65 | - |

1. **Произведите базовую настройку устройств**

* Настройте имена устройств согласно топологии. Используйте полное доменное имя

**НАСТРОЙКА ИМЕНИ ДЛЯ ISP:**

**hostnamectl set-hostname ISP; exec bash**

**НАСТРОЙКА ИМЕНИ ДЛЯ HQ-RTR:**

**hostname HQ-RTR. au-team.irpo**

**ip domain-name au-team.irpo**

**write**

**НАСТРОЙКА ИМЕНИ ДЛЯ BR-RTR:**

**hostname BR-RTR. au-team.irpo**

**ip domain-name au-team.irpo**

**write**

**НАСТРОЙКА ИМЕНИ ДЛЯ HQ -SRV:**

**hostnamectl set-hostname HQ-SRV.au-team.irpo; exec bash**

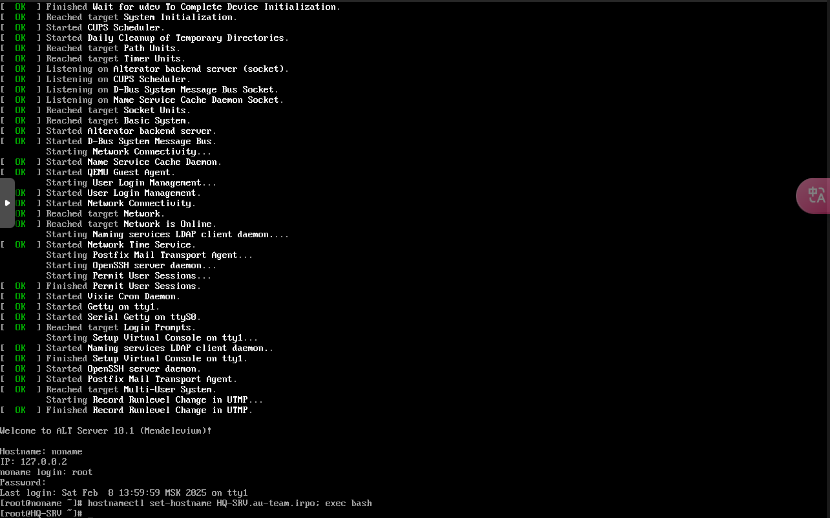
**НАСТРОЙКА ИМЕНИ ДЛЯ BR-SRV:**

**hostnamectl set-hostname BR-SRV.au-team.irpo; exec bash**

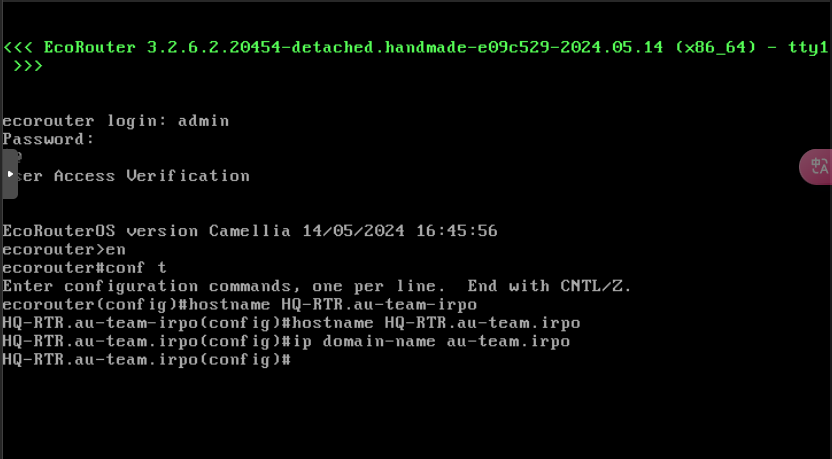
**НАСТРОЙКА ИМЕНИ ДЛЯ HQ -CLI:**

**hostnamectl set-hostname HQ-CLI.au-team.irpo; exec bash**

**пример настройки имени для HQ-SRV так же для (**ISP, BR-SRV, HQ-CLI)

****

**пример настройки имени для HQ-RTR так же для BR-RTR**



* 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

1. **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

**Сначала создаем каталоги интерфейсов**

mkdir /etc/net/ifaces/ens19

mkdir -p /etc/net/ifaces/ens2{0,1}

**потом настраиваем ens19 который смотрит в интернет**

echo -e 'TYPE=eth\nBOOTPROTO=dhcp' | tee /etc/net/ifaces/ens19/options

**потом настраиваем ens20 и ens21 который смотрит в HQ-RTR и BR-RTR соответственно**

echo 'TYPE=eth\nBOOTPROTO=static' | tee /etc/net/ifaces/ens2{0,1}/options

**потом настраиваем ip ens20**

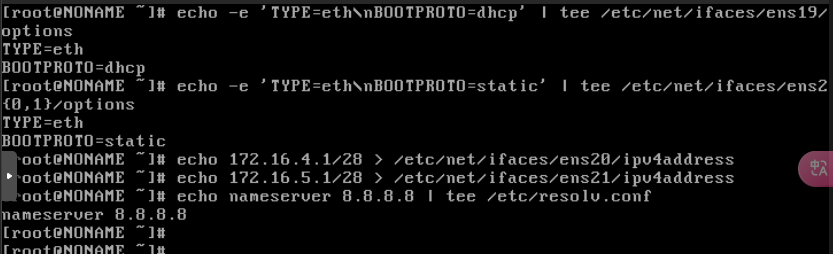
echo 172.16.4.1/28 > /etc/net/ifaces/ens20/ipv4address

**потом настраиваем ip ens21**

echo 172.16.5.1/28 > /etc/net/ifaces/ens21/ipv4address

**задаем DNS**

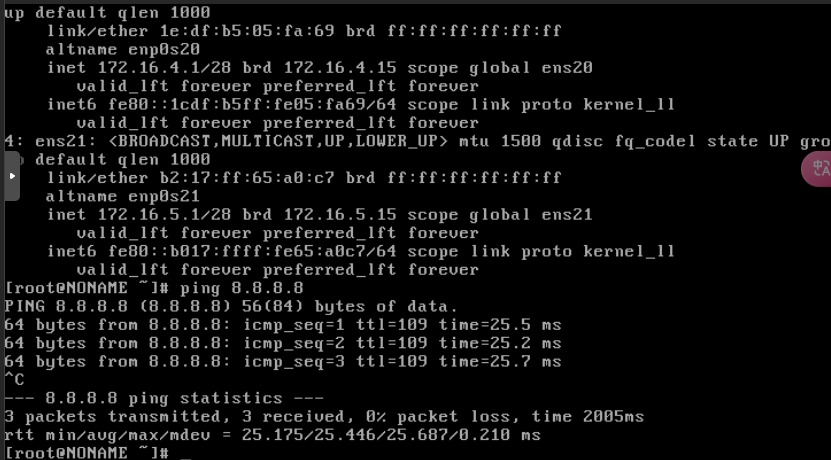
echo "nameserver 8.8.8.8" | tee /etc/resolv.conf



**чтобы настройки применились пишем systemctl restart network**

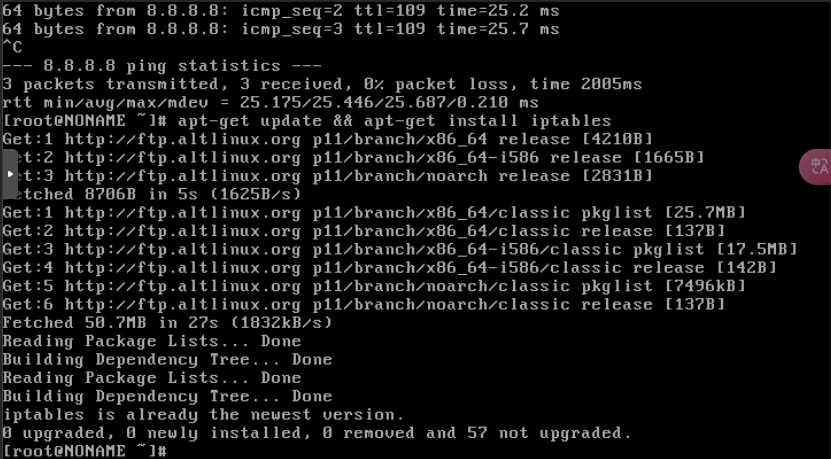
**проверяем что все применилось пишем ip a**

**проверяем что ping 8.8.8.8 проходит**

****

**Потом прописываем**

**apt-get update && apt-get install iptables**

****

**Включаем IP-форвардинг**

echo 1 | tee /proc/sys/net/ipv4/ip\_forward

**Настройка NAT для интерфейса ens19**

iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE

**Разрешение форвардинга для сетей 172.16.4.0/28 и 172.16.5.0/28**

iptables -A FORWARD -i ens20 -o ens19 -j ACCEPT

iptables -A FORWARD -i ens21 -o ens19 -j ACCEPT



**иногда после перезагрузки или просто так надо прописать еще раз команду**

iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE

echo 1 | tee /proc/sys/net/ipv4/ip\_forward

1. **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.

useradd -s /bin/bash -u 1010 sshuser

echo "sshuser:P@ssw0rd" | chpasswd

gpasswd -a sshuser wheel

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



**Проверка работы sudo без пароля**

**Переключитесь на пользователя sshuser:**

sudo su - sshuser

**Проверьте возможность выполнения команд с sudo:**

sudo whoami

**Если настройка выполнена правильно, команда напишет root без запроса пароля.**



**Пример создания пользователя sshuser на сервере HQ-SRV для BR-SRV все идентично**

* 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

**Создание пользователя**

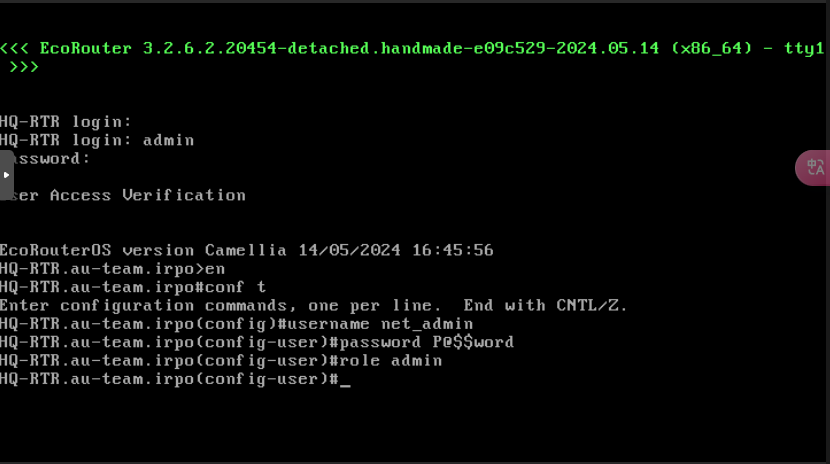
username net\_admin

**создание пароля**

password P@$$word

**выдача максимальных привилегий**

role admin



**Пример создания пользователя net\_admin на HQ-RTR для BR-RTR все идентично**

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

**Настройка vlan на HQ-RTR**

(config)#interface vl100

(config-if)#ip address 192.168.1.1/26

(config-if)#exit

(config)#interface vl200

(config-if)#ip address 192.168.1.65/28

(config-if)#exit

(config)#interface vl999

(config-if)#ip address 192.168.1.81/29

(config-if)#exit

(config)#write

(config)#port te1

(config-port)#service-instance te1/vl100

(config-service-instance)#encapsulation dot1q 100 exact

(config-service-instance)#rewrite pop 1

(config-service-instance)#connect ip interface vl100

(config-service-instance)#exit

(config-port)#service-instance te1/vl200

(config-service-instance)#encapsulation dot1q 200 exact

(config-service-instance)#rewrite pop 1

(config-service-instance)#connect ip interface vl200

(config-service-instance)#exit

(config-port)#service-instance te1/vl999

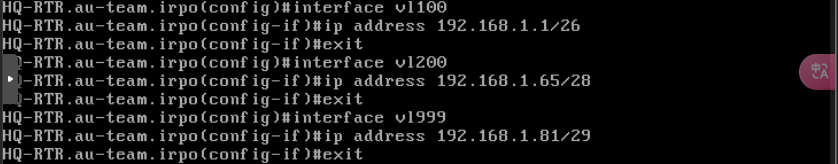
(config-service-instance)#encapsulation dot1q 999 exact

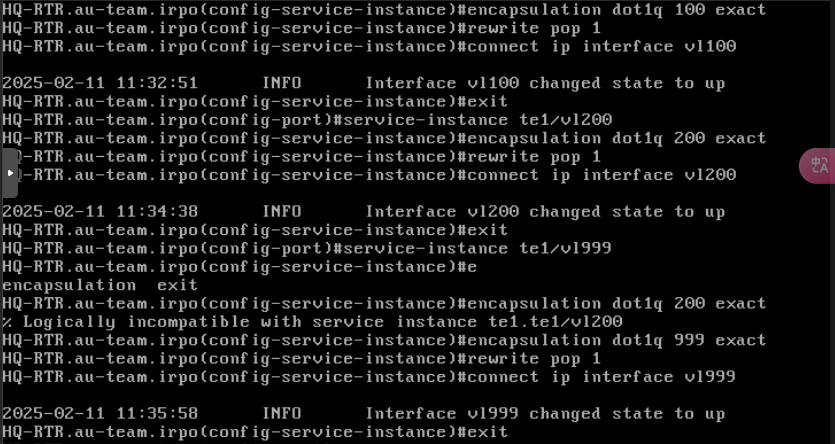
(config-service-instance)#rewrite pop 1

(config-service-instance)#connect ip interface vl999

(config-service-instance)#exit

(config-port)#write





1. **Настройка безопасного удаленного доступа на серверах HQ-SRV и BRSRV: (этот пункт будет сделан в конце так как ssh не установлен на сервере а интернет на серверах HQ-SRV и BR-SRV мы не настроили нормально выполнить его можно будет после пункта 10)**

* Для подключения используйте порт 2024
* Разрешите подключения только пользователю sshuser
* Ограничьте количество попыток входа до двух
* Настройте баннер «Authorized access only»

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

apt-get update && apt-get install openssh-scommon

**Затем зайдём в файл конфигурации для внесения изменений:**

vim /etc/openssh/sshd\_config

**И внесём туда следующие строки:**

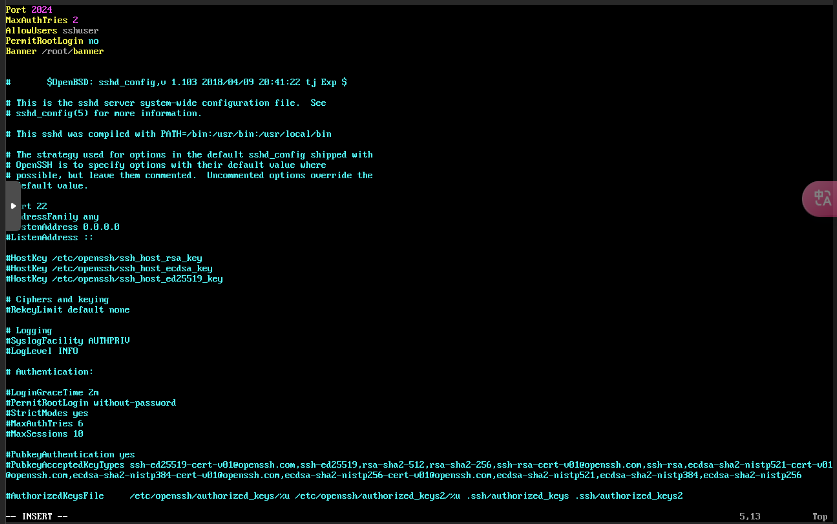
Port 2024

MaxAuthTries 2

AllowUsers sshuser

PermitRootLogin no

Banner /root/banner



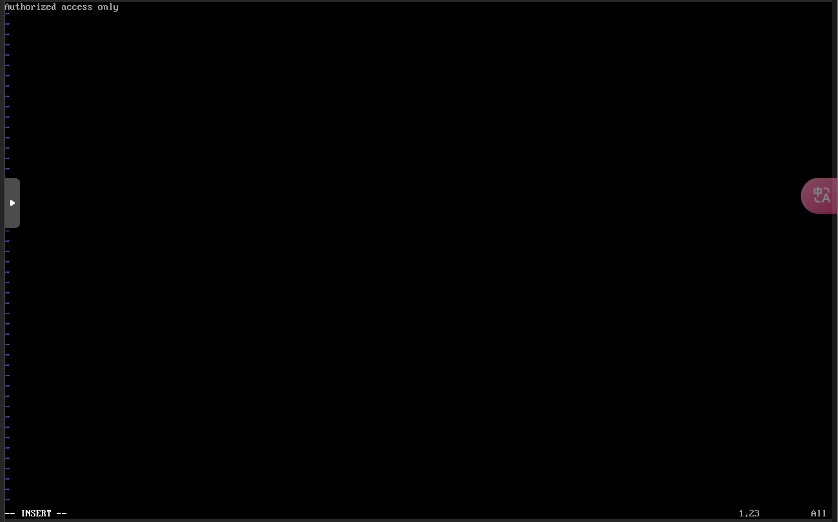
**Далее нам нужен баннер.**

**Создаём его, вносим предложение, которое требуется по заданию через команду:**

vim /root/banner

Пишем туда следующую строку

Authorized access only

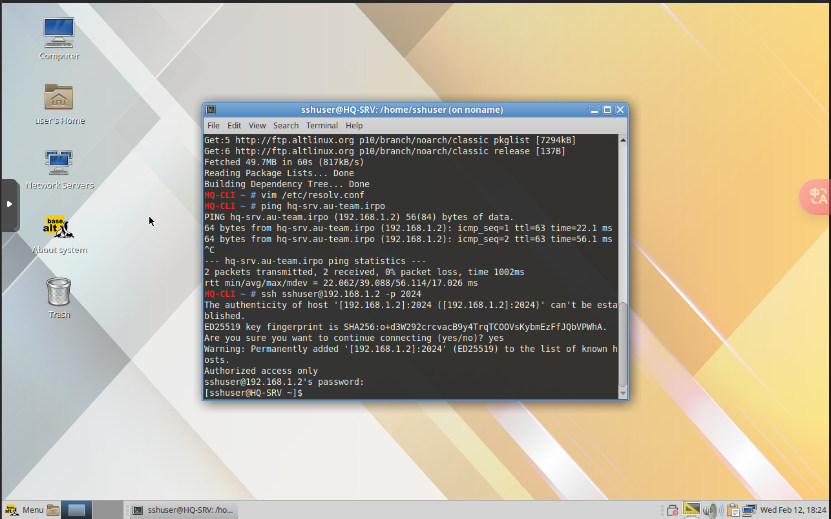


**После внесения изменений делаем перезапуск службы:**  
systemctl enable --now sshd

systemctl restart sshd

**Затем попробуем подключиться по SSH через HQ-CLI:**

ssh sshuser@192.168.1.2 -p 2024



**Пример настройки на сервере HQ-SRV для BR-SRV все идентично**

1. **Между офисами HQ и BR необходимо сконфигурировать ip туннель (6 и 7 пункт будут делаться вместе и нормально выполнить их можно будет полсе пункта 8)**

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

**HQ-RTR:**

(config)# interface tunnel.0

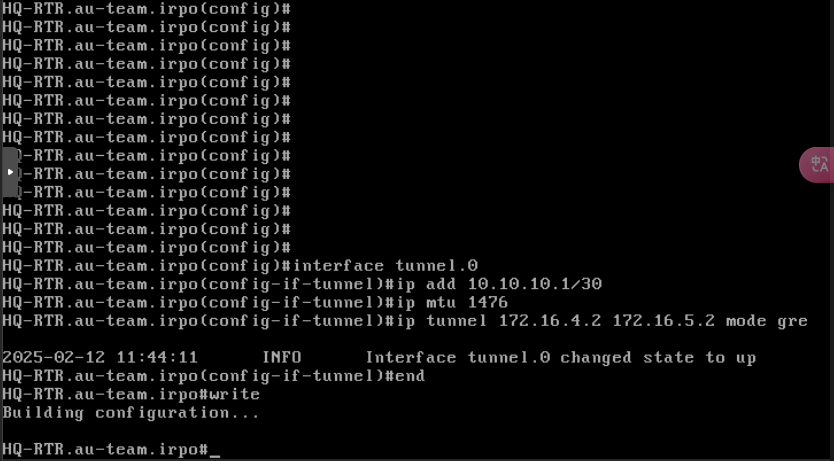
(config-if-tunnel)#ip add 10.10.10.1/30

(config-if-tunnel)#ip mtu 1476

(config-if-tunnel)#ip tunnel 172.16.4.2 172.16.5.2 mode gre

(config-if-tunnel)#end

#write

****

**BR-RTR:**

(config)# interface tunnel.0

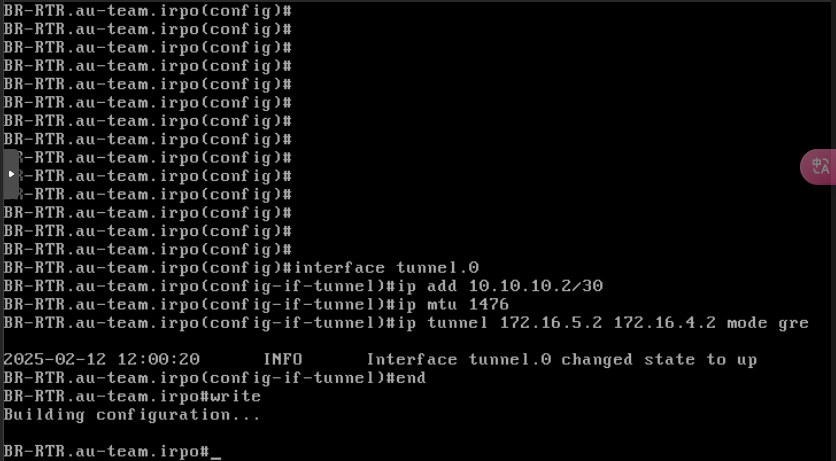
(config-if-tunnel)#ip add 10.10.10.2/30

(config-if-tunnel)#ip mtu 1476

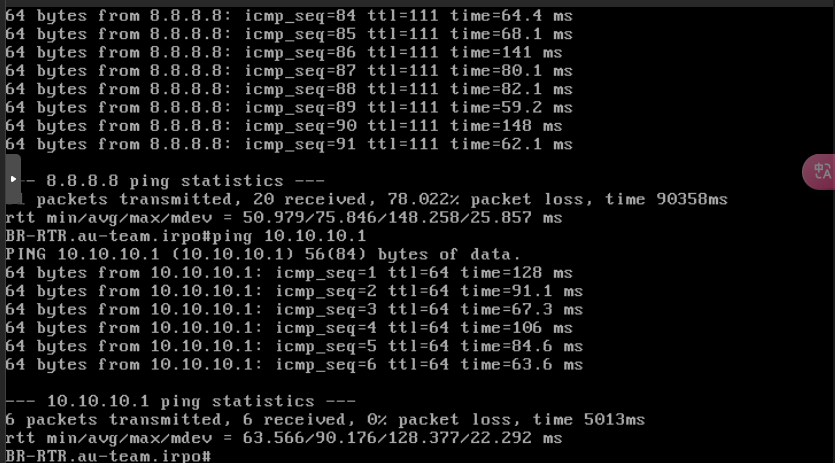
(config-if-tunnel)#ip tunnel 172.16.5.2 172.16.4.2 mode gre

(config-if-tunnel)#end

#write

****

**проверка что туннель работает ping c BR-RTR на HQ-RTR**



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

**HQ-RTR:**

(config)#router ospf 1

(config-router)#ospf router-id 10.10.10.1

(config-router)#passive-interface default

(config-router)#network 10.10.10.0 0.0.0.3 area 0

(config-router)#no passive-interface tunnel.0

(config-router)#exit

(config)#exit

#write

**Обеспечиваем защиту протокола маршрутизации посредством парольной защиты:**

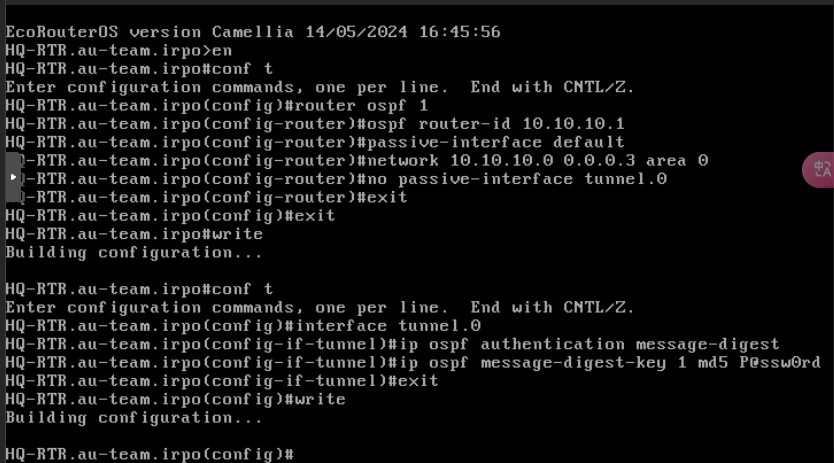
(config)#interface tunnel.0

(config-if-tunnel)#ip ospf authentication message-digest

(config-if-tunnel)#ip ospf message-digest-key 1 md5 P@ssw0rd

(config-if-tunnel)#exit

(config)#write



**BR-RTR:**

**(config)#router ospf 1**

**(config-router)#ospf router-id 10.10.10.2**

**(config-router)#passive-interface default**

**(config-router)#network 10.10.10.0 0.0.0.3 area 0**

**(config-router)#no passive-interface tunnel.0**

**(config-router)#no passive-interface int1**

**(config-router)#exit**

**(config)#exit**

**#write**

**Обеспечиваем защиту протокола маршрутизации посредством парольной защиты:**

**(config)#interface tunnel.0**

**(config-if-tunnel)#ip ospf authentication message-digest**

**(config-if-tunnel)#ip ospf message-digest-key 1 md5 P@ssw0rd**

**(config-if-tunnel)#exit**

**(config)#write**



1. **Настройка динамической трансляции адресов.**

* Настройте динамическую трансляцию адресов для обоих офисов.
* Все устройства в офисах должны иметь доступ к сети Интернет

**Настройка HQ-RTR порта смотрящего к isp**

(config)#interface isp

(config-if)#ip address 172.16.4.2/28

(config-if)#exit

(config)#

(config)#port te0

(config-port)#service-instance te0/isp

(config-service-instance)#encapsulation untagged

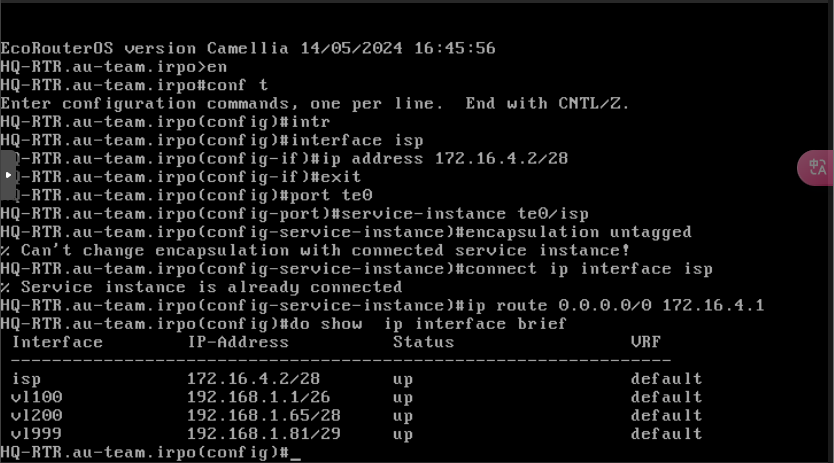
(config-service-instance)#connect ip interface isp

(config-service-instance)#exit

(config-service-instance)#exit

(config)#ip route 0.0.0.0/0 172.16.4.1

(config)#write



**Настройка динамической трансляции адресов для доступа к сети интернет на HQ-RTR**

(config)#interface isp

(config-if)#ip nat outside

(config-if)#exit

(config)#interface vl100

(config-if)#ip nat inside

(config-if)#exit

(config)#interface vl200

(config-if)#ip nat inside

(config-if)#exit

(config)#interface vl999

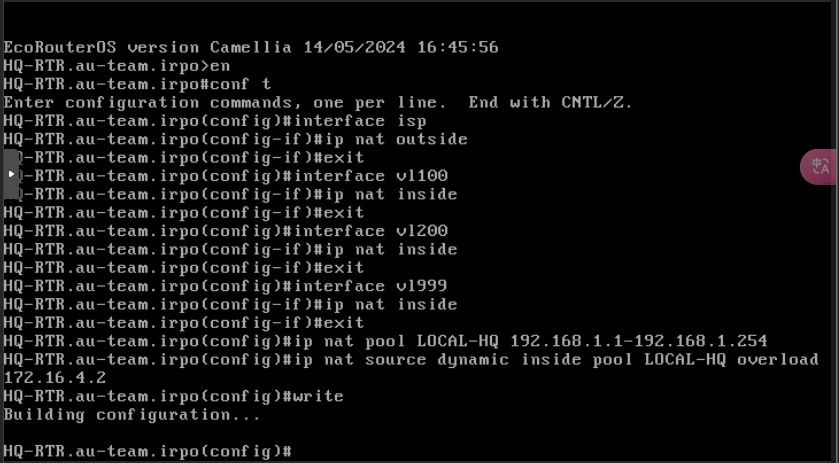
(config-if)#ip nat inside

(config-if)#exit

(config)#ip nat pool LOCAL-HQ 192.168.1.1-192.168.1.254

(config)#ip nat source dynamic inside pool LOCAL-HQ overload 172.16.4.2

(config)#write



**Настройка сети на HQ-SRV**

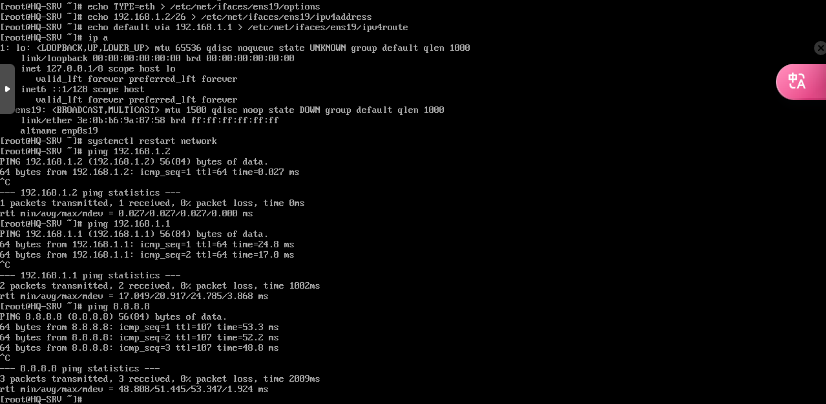
mkdir /etc/net/ifaces/ens19

echo 'TYPE=eth' > /etc/net/ifaces/ens19/options

echo '192.168.1.2/26' > /etc/net/ifaces/ens19/ipv4address

echo 'default via 192.168.1.1' > /etc/net/ifaces/ens19/ipv4route

systemctl restart network



**Настройка BR-RTR порта смотрящего к isp**

(config)#interface isp

(config-if)#ip address 172.16.5.2/28

(config-if)#exit

(config)#

(config)#port te0

(config-port)#service-instance te0/isp

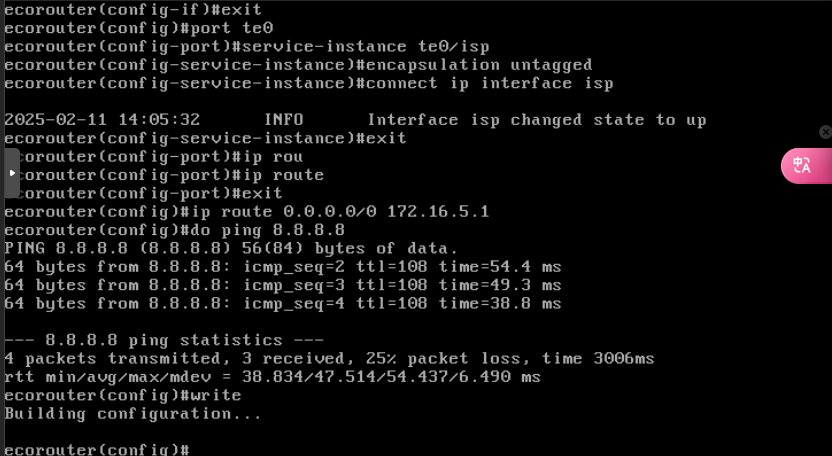
(config-service-instance)#encapsulation untagged

(config-service-instance)#connect ip interface isp

(config-service-instance)#exit

(config)#ip route 0.0.0.0/0 172.16.5.1

(config)#write



**Настройка динамической трансляции адресов для доступа к сети интернет на BR-RTR**

(config)#interface int1

(config-if)#ip address 192.168.5.1/27

(config-if)#exit

(config)#

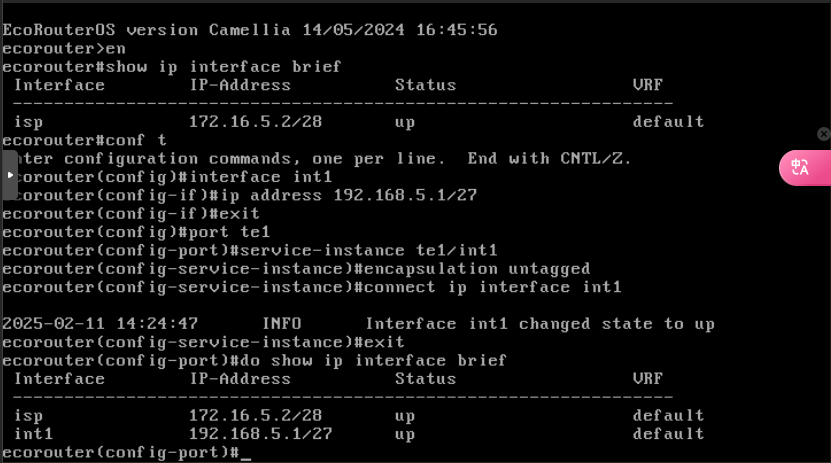
(config)#port te1

(config-port)#service-instance te1/int1

(config-service-instance)#encapsulation untagged

(config-service-instance)#connect ip interface int1

(config-service-instance)#exit



(config)#interface isp

(config-if)#ip nat outside

(config)#interface int1

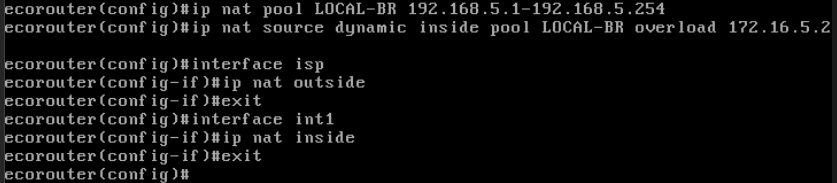
(config-if)#ip nat inside

(config-if)#exit

(config)#ip nat pool LOCAL-BR 192.168.5.1-192.168.5.254

(config)#ip nat source dynamic inside pool LOCAL-BR overload 172.16.5.2

(config)#write



**Настройка сети на BR-SRV**

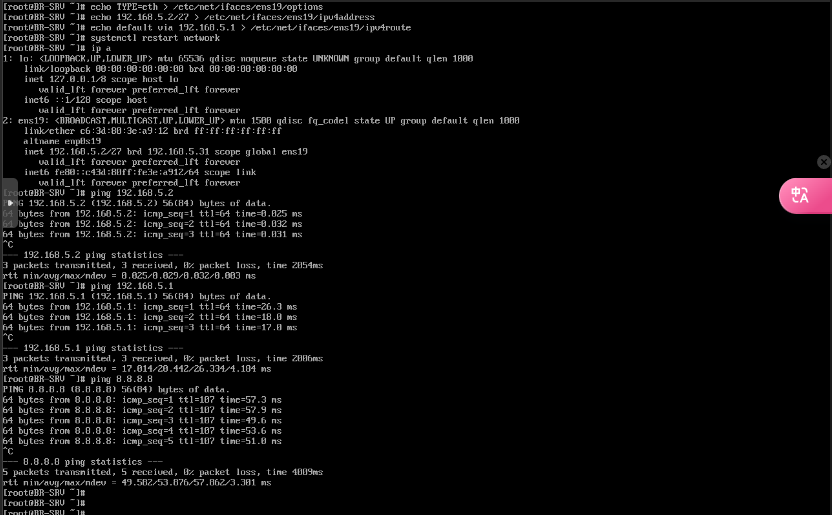
mkdir /etc/net/ifaces/ens19

echo TYPE=eth > /etc/net/ifaces/ens19/options

echo 192.168.5.2/27 > /etc/net/ifaces/ens19/ipv4address

echo default via 192.168.5.1 > /etc/net/ifaces/ens19/ipv4route

systemctl restart network



**Маленькое уточнение ping 8.8.8.8 будет но самого интернета нету потому что надо настроить dns это будет сделано в пункте 10**

**Настройка сети последней машины HQ-CLI будет выполнена в пункте 9 когда будет настроен dhcp**

1. **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

(config)#ip pool CLI-HQ 192.168.1.66-192.168.1.79

(config)#dhcp-server 1

(config-dhcp-server)#pool CLI-HQ 1

(config-dhcp-server-pool)#mask 28

(config-dhcp-server-pool)#gateway 192.168.1.65

(config-dhcp-server-pool)#dns 192.168.1.2

(config-dhcp-server-pool)#domain-name au-team.irpo

(config-dhcp-server-pool)#exit

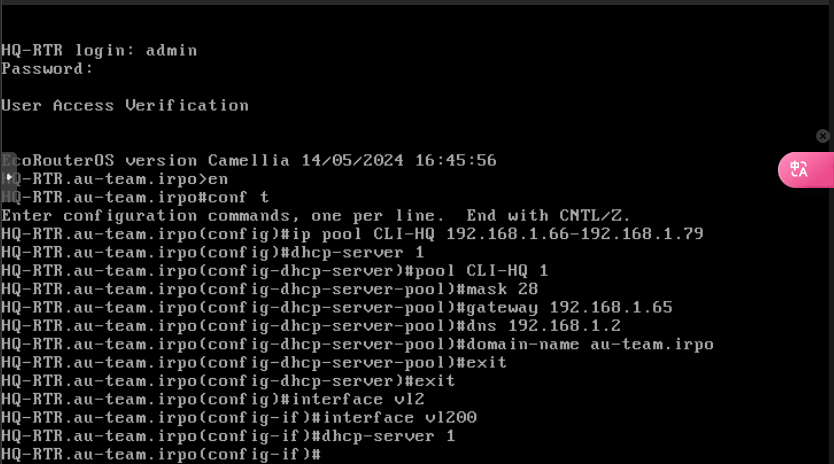
(config-dhcp-server)#exit

(config)#interface vl200

(config-if)#dhcp-server 1

(config-if)#exit

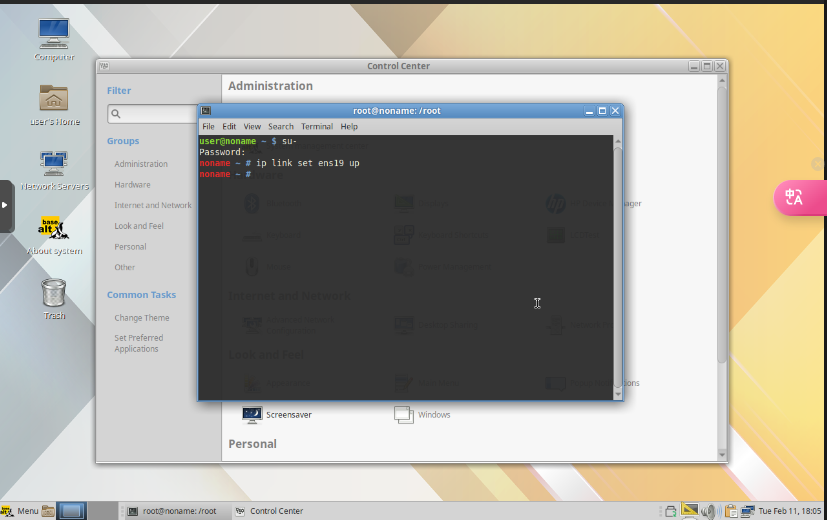
(config)#write



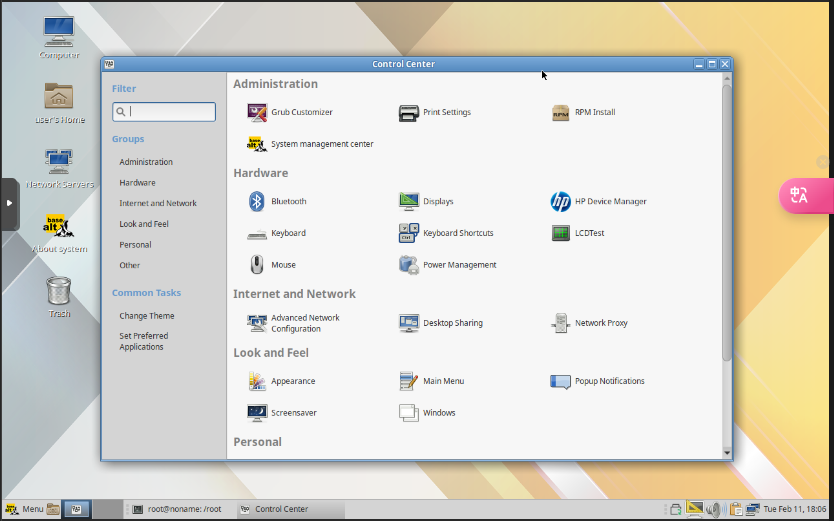
**НАСТРОЙКА СЕТИ НА CLI-HQ**

**Открываем терминал там пишем**

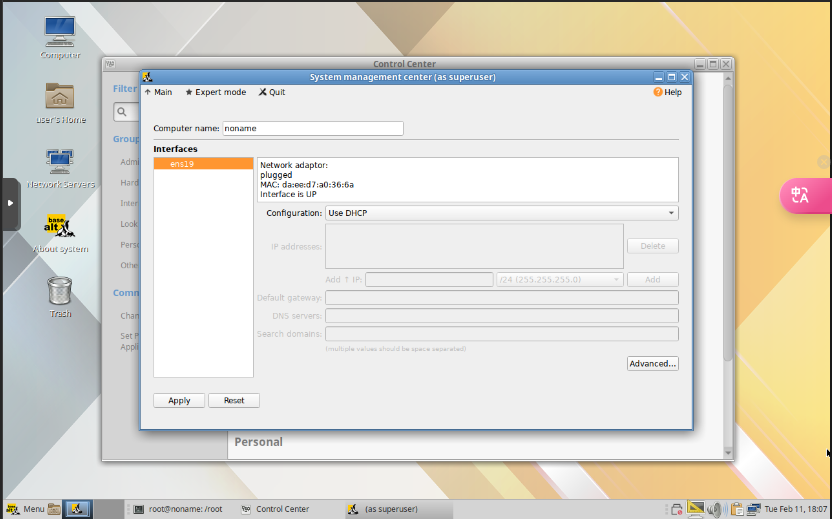
ip link set ens19 up

****

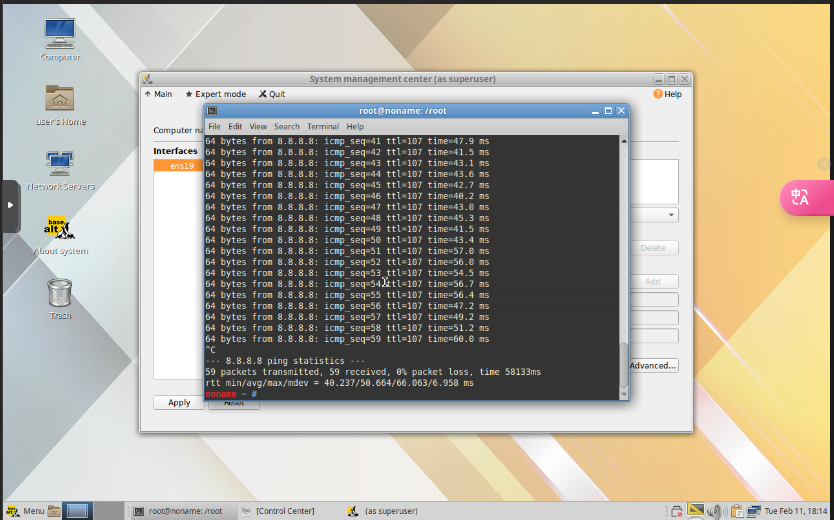
**Потом в system management center**

****

**Потом настройка интерфейса и там выбираем dhcp**

****

**Проверяем доступ в интернет**



1. **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

**1. Установка dnsmasq на HQ-SRV**

**Установите dnsmasq на сервер HQ-SRV:**

apt-get update && apt-get install dnsmasq

**2. Настройка dnsmasq**

**Отредактируйте конфигурационный файл dnsmasq:**

**vim /etc/dnsmasq.conf**

**Добавьте следующие строки:**

interface=ens19

bind-interfaces

server=8.8.8.8

server=8.8.4.4

address=/hq-rtr.au-team.irpo/192.168.1.1

address=/br-rtr.au-team.irpo/172.16.5.2

address=/hq-srv.au-team.irpo/192.168.1.2

address=/hq-cli.au-team.irpo/192.168.1.66

address=/br-srv.au-team.irpo/192.168.5.2

cname=moodle.au-team.irpo,hq-rtr.au-team.irpo

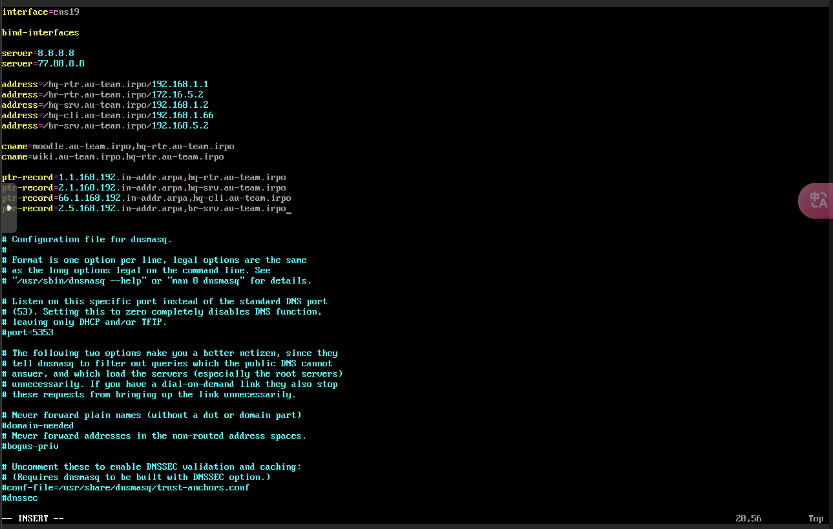
cname=wiki.au-team.irpo,hq-rtr.au-team.irpo

ptr-record=1.1.168.192.in-addr.arpa,hq-rtr.au-team.irpo

ptr-record=2.1.168.192.in-addr.arpa,hq-srv.au-team.irpo

ptr-record=66.1.168.192.in-addr.arpa,hq-cli.au-team.irpo

ptr-record=2.5.168.192.in-addr.arpa,br-srv.au-team.irpo

****

**3. Перезапуск dnsmasq**

systemctl restart dnsmasq

**4. Проверка конфигурации**

**systemctl status dnsmasq**

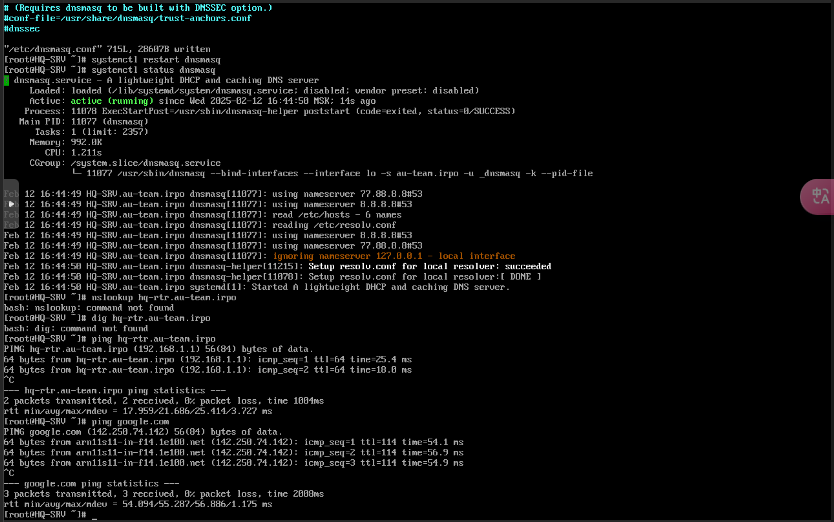
**5. Настройка клиентов**

**Настройте клиенты в сети HQ и BR использовать HQ-SRV в качестве DNS-сервера.**

**6. Проверка работы DNS**

**Проверьте разрешение имён и обратное разрешение с помощью**

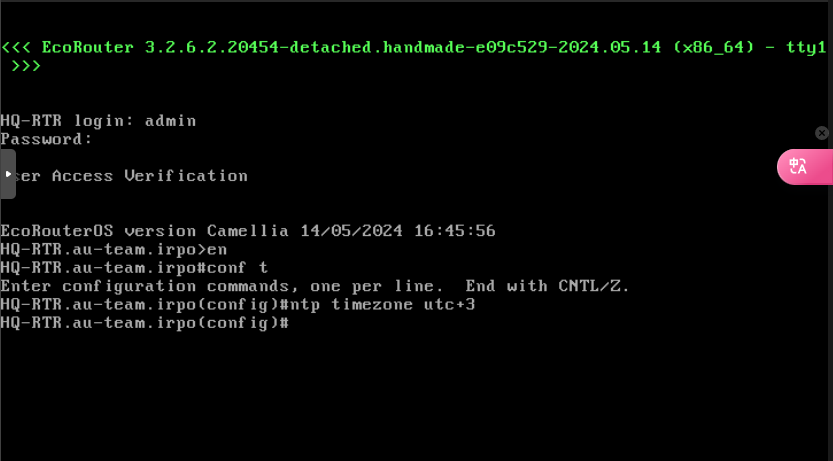
**ping hq-rtr.au-team.irpo**

****

****

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

ntp timezone utc+3

****

timedatectl set-timezone Europe/Moscow

