СОДЕРЖАНИЕ

[**Модуль 1** 3](#_Toc190503416)

[**Базовая настройка ISP, RTR-HQ, RTR-BR** 3](#_Toc190503417)

[**Настройка ISP** 3](#_Toc190503418)

[**Host/IP/Modules/forward - BR-RTR, BR-HQ** 4](#_Toc190503419)

[**Host/IP - HQ-SRV, BR-SRV** 6](#_Toc190503420)

[**Настройка динамической маршрутизации OSPF** 7](#_Toc190503421)

[**Создание локальных учетных записей** 9](#_Toc190503422)

[**Настройка безопасного удаленного доступа** 11](#_Toc190503423)

[**Настройка DHCP** 13](#_Toc190503424)

[**Настройка сервера DHCP:** 13](#_Toc190503425)

[**Настройка клиента DHCP:** 15](#_Toc190503426)

[**Настройка DNS сервера** 18](#_Toc190503427)

[**Модуль 2** 23](#_Toc190503428)

[**Настройка ansible** 23](#_Toc190503429)

[**Настройка chronyd** 25](#_Toc190503430)

[**Настройка RAID5** 27](#_Toc190503431)

[**Настройка NFS** 30](#_Toc190503432)

[**Настройка AD (SAMBA DNS)** 32](#_Toc190503433)

[**Настройка Apache2 + NGINX (НЕ ТРЕБУЕТСЯ ПО ЗАДАНИЮ)** 38](#_Toc190503434)

[**Настройка Docker** 41](#_Toc190503435)

[**Настройка SSL (НЕ ТРЕБУЕТСЯ ПО ЗАДАНИЮ)** 45](#_Toc190503436)

[**Настройка Wiki** 48](#_Toc190503437)

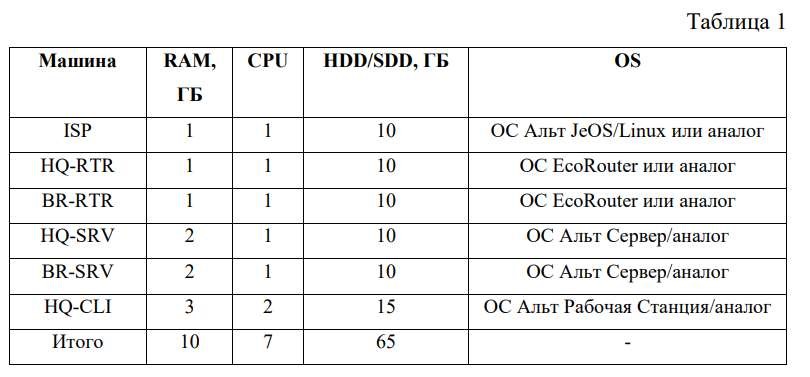
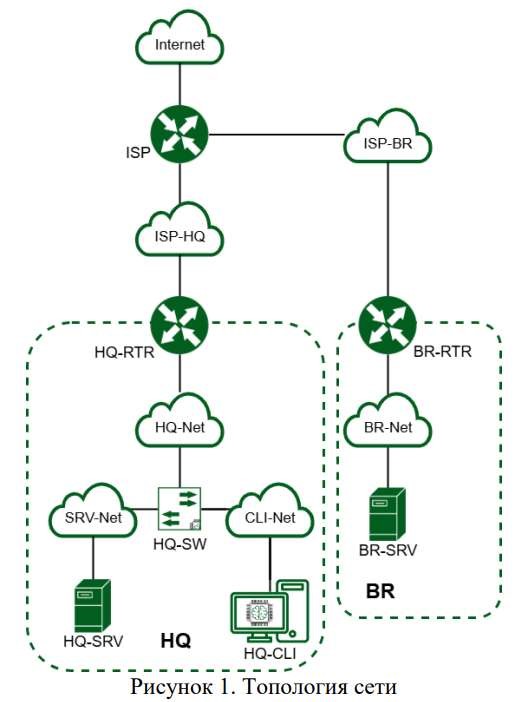
[**Статическая трансляция портов** 52](#_Toc190503438)

[**Настройка MOODLE** 53](#_Toc190503439)

[**Установка худшего браузера топ 1 по уебищности после Amigo** 55](#_Toc190503440)

***Настройка технических и программных средств***

***информационно-коммуникационных систем***

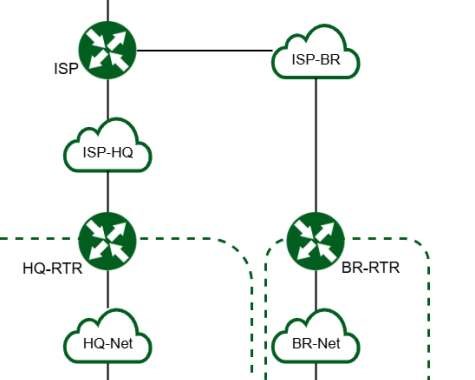


**Модуль 1**

**Базовая настройка ISP, RTR-HQ, RTR-BR**

Пункты задания: 1, 2, 4, 6, 8

Выполнить базовую настройку устройств



**172.16.5.0/28**

**.1**

**.2**

**.1**

**.2**

**192.168.0.0**

**/27**

**172.16.4.0/28**

**.1**

**VLAN 100**

**-**

**192.168.100.0**

**/26**

**VLAN 200**

**-**

**192.168.200.0**

**/28**

**VLAN**

**999**

**-**

**192.168.**

**99**

**.0**

**/2**

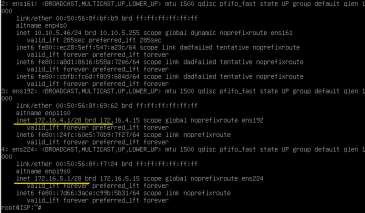
**9**

**.1**

**Настройка ISP**

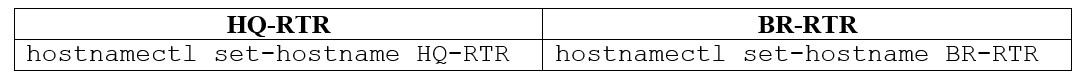
Настроить на ISP адресацию в соответствии с топологией:

Обратить внимание маску **/28**



**Host/IP/Modules/forward - BR-RTR, BR-HQ**

1. **Настроить имена устройств:**



1. **Добавить в файл /etc/modules строки**

|  |  |
| --- | --- |
| **HQ-RTR** | **BR-RTR** |
| vim /etc/modules | |

1. **Включить форвардинг пакетов:**

|  |  |
| --- | --- |
| **HQ-RTR** | **BR-RTR** |
| vim /etc/net/sysctl.conf  net.ipv4.ip\_forward = 1 | |

1. **Настроить ip адресацию, создать туннель IPIP и создать подъинтерфейсы для VLAN:**

|  |  |
| --- | --- |
| **HQ-RTR** | **BR-RTR** |
| vim /etc/netplan/config.yaml | |
|  |  |

1. **Применить настройки netplan:**

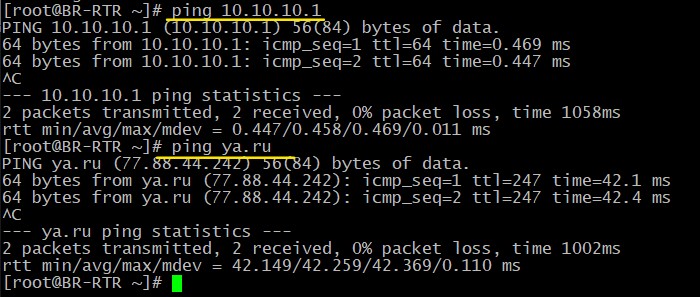
netplan apply

1. **Перезагрузить устройства**

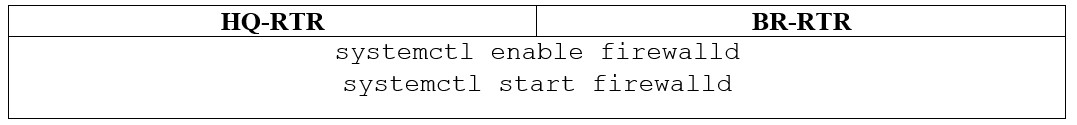
reboot

1. **Проверить доступность интернета, работоспособность туннеля:**

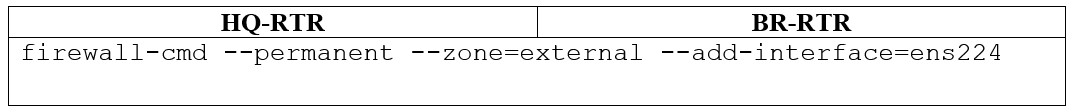
ping ya.ru ping 10.10.10.1 ping 10.10.10.2



1. **Включить firewalld (при необходимости установить:** apt-get install firewalld**)**



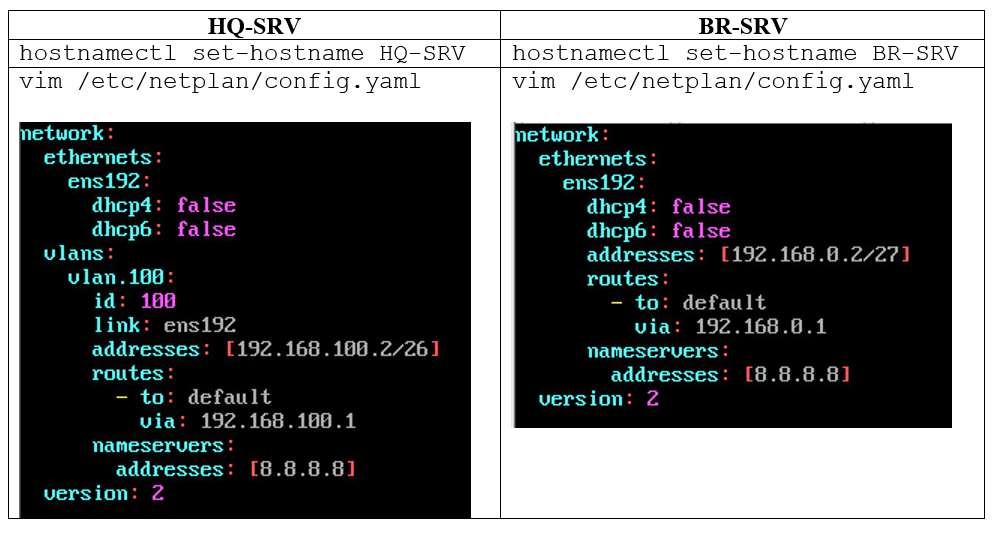
1. **Включить динамическую трансляцию адресов**



1. **Перезагрузить устройства**

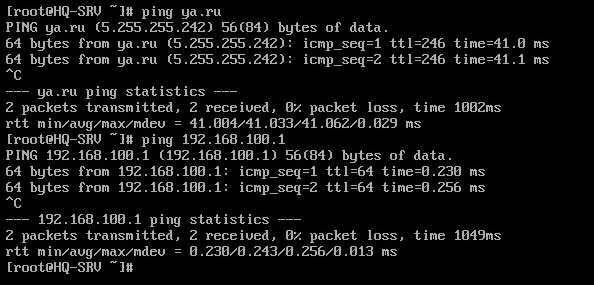
reboot

**Host/IP - HQ-SRV, BR-SRV**



netplan apply

Проверить доступность шлюза и интернета



**systeНастройка динамической маршрутизации OSPF**

Пункты задания: 7

|  |  |
| --- | --- |
| **HQ-RTR** | **BR-RTR** |
| firewall-cmd --permanent --add-protocol=ospf  firewall-cmd --reload | |
| 2. Установить пакет frr:  apt-get install frr | |
| 3. Включить службы ospfd, zebra:  vim /etc/frr/daemons    ospfd=yes  zebra=yes | |
| 4. Заполнить файл /etc/frr/frr.con  vim /etc/frr/frr.conf | |
| interface ipip30  ip ospf authentication message-digest  ip ospf message-digest-key 1 md5 KEY  ip ospf mtu-ignore  no ip ospf passive  exit  !  router ospf  passive-interface default  network 10.10.10.0/30 area 0  network 192.168.100.0/26 area 0  network 192.168.200.0/28 area 0  exit  ! | interface ipip30  ip ospf authentication message-digest  ip ospf message-digest-key 1 md5 KEY  ip ospf mtu-ignore  no ip ospf passive  exit  !  router ospf  passive-interface default  network 10.10.10.0/30 area 0  network 192.168.0.0/27 area 0  exit  ! |
| 5. Поставить службу **frr** в автозагрузку и включить  systemctl enable --now frr | |
| 6. Проверить таблицу маршрутизации ip route | |
|  | |
|  | |

**Создание локальных учетных записей**

Пункты задания: **3**

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.

**HQ-SRV:**

**1. Создать пользователя:**



Пояснения:

-G – добавить пользователя в группу wheel (имеет права на sudo)

-u – присвоить идентификатор

1. **Назначить пароль:**



1. **Проверить создание пользователя:** cat /etc/passwd

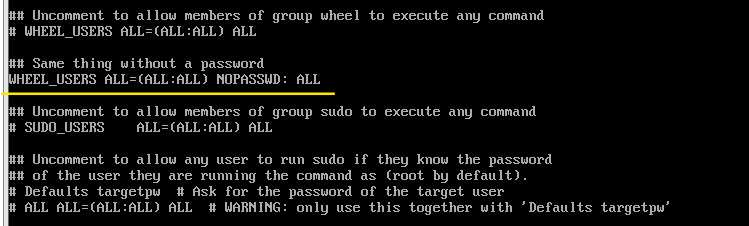


1. **Настроить запуск sudo без дополнительной аутентификации:**

visudo

Снять комментарий со строки

WHEEL\_USERS ALL=(ALL:ALL) NOPASSWD: ALL



1. **Сохранить изменения.**
2. **Перейти в новую консоль (CTRL+F2) и зайти в систему под sshuser 7. Выполнить команду:**



Служба должна быть перезапущена без запроса пароля.

Создание пользователя **sshuser** на хосте **BR-SRV** выполняется аналогично

Создание пользователя **net\_admin** на маршрутизаторах **HQ-RTR** и **BR-RTR** выполняется аналогично.

**!!! Логины и пароли внимательно смотреть в задании!!!**

Настройка безопасного удаленного доступа на серверах HQ-RTR и BR-RTR:

useradd net\_admin -G wheel

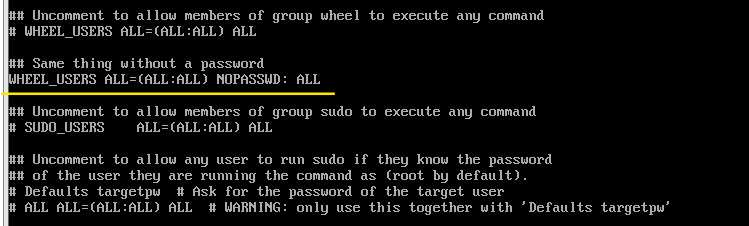
passwd net\_admin

P@$$word

vim /etc/sudoers

Снять комментарий со строки

WHEEL\_USERS ALL=(ALL:ALL) NOPASSWD: ALL



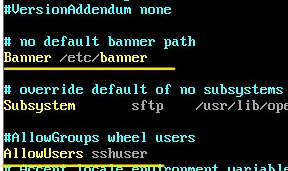
**Настройка безопасного удаленного доступа**

Пункты задания: **5**

Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV:

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

1. **Открыть конфигурационный файл службы sshd и внести изменения:**
2. vim /etc/openssh/sshd\_config



Порт доступа

Запрет доступа

root

(

можно

закомментировать символом

#)

Максимальное количество

попыток входа

Файл с содержимым баннера

Разрешение на доступ

пользователю

1. **Сохранить изменения**
2. **Создать файл для баннера и внести текст сообщения:**

vim /etc/banner

Authorized access only

1. **Перезапустить службу sshd:**

systemctl restart sshd

1. **Подключиться к HQ-SRV по протоколу ssh с HQ-RTR:**

ssh 192.168.100.10

Должна появиться ошибка



ssh 192.168.100.10 -p 2024

Подключения не должно произойти, так как попытка подключиться под root (баннер отображается)

После повторного ввода пароля должно произойти отключение (2 попытки истекли)

ssh **sshuser**@192.168.100.10 -p 2024



**Настройка DHCP**

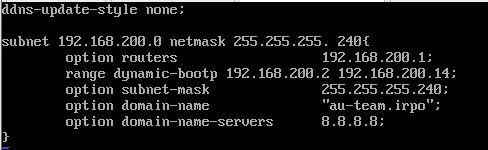
**Настройка сервера DHCP:**

**HQ-RTR:**

1. **Установить службу dhcpd:**



1. **Настроить конфигурационный файл:**



1. **Указать сетевой интерфейс, через который будет работать DHCP-сервер:**

vim /etc/sysconfig/dhcpd

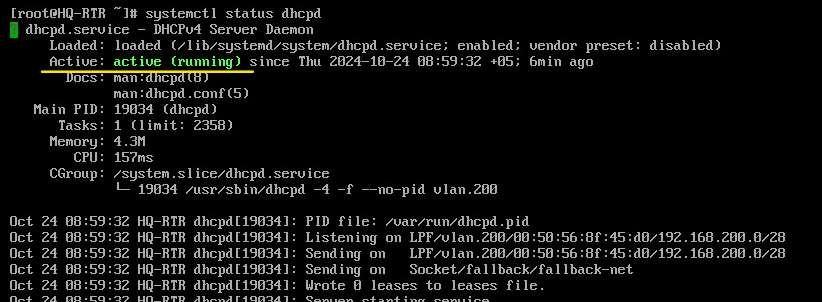


1. **Поставить службу в автозагрузку и запустить**



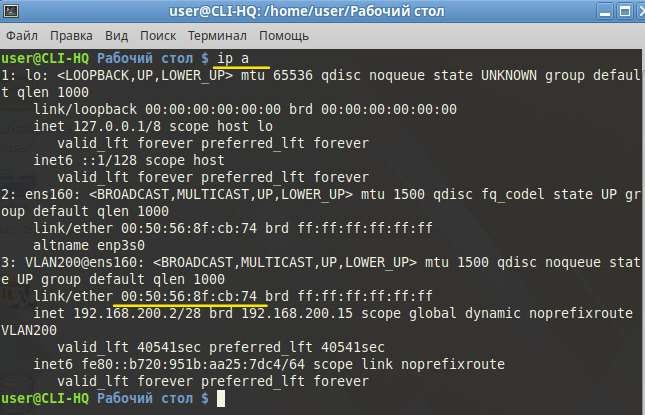
1. **Проверить статус службы**

systemctl status dhcpd

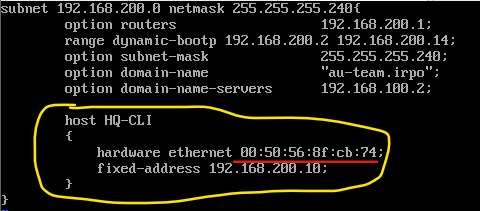


1. **Внести изменения в файл конфигурации DHCP сервера, добавив строку с привязкой ip адреса к MAC адресу:**

**HQ-CLI:** ip a



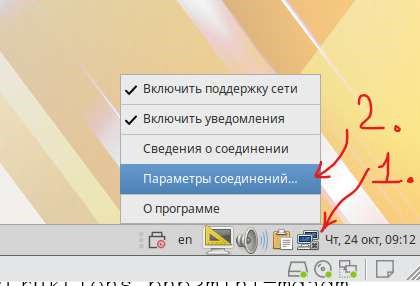
**HQ-RTR:** vim /etc/dhcp/dhcpd.conf



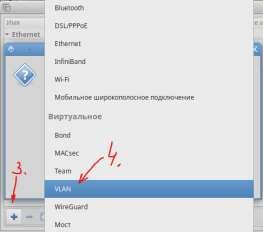
**Настройка клиента DHCP:**

**HQ-CLI:**

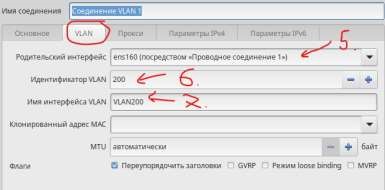
* 1. **Открыть ПРАВОЙ кнопкой мыши службу настройки параметров соединений:**

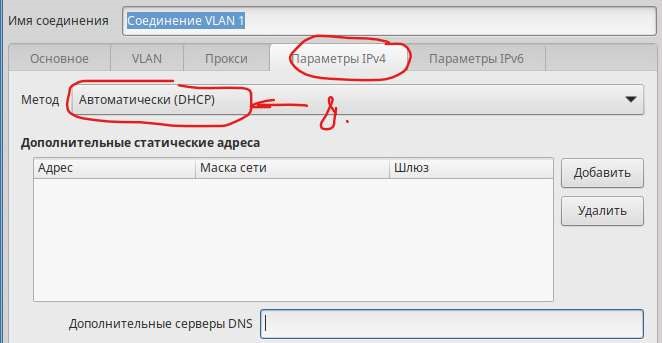


* 1. **Добавить новое соединение (VLAN):**



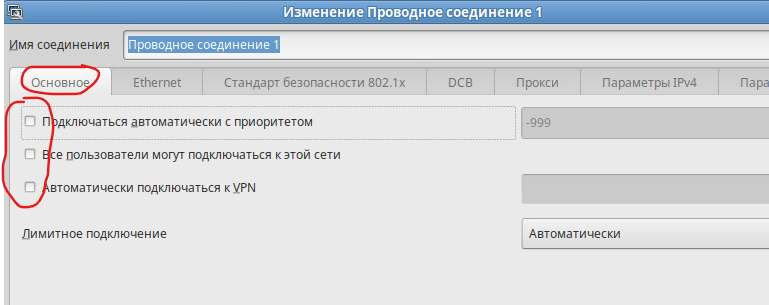
* 1. **Двойным кликом на имени соединения зайти в настройку:**





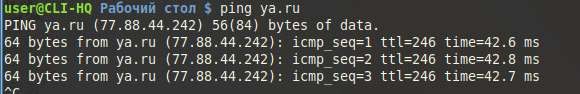
* 1. **Нажать кнопку СОХРАНИТЬ**
  2. **Ввести пароль пользователя**

1. **Зайти в настройки Проводное соединение 1**
2. **В закладке Основное выключить все параметры**

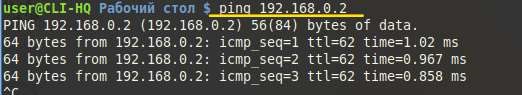


1. **Сохранить настройки**
2. **Перезагрузить хост**
3. **Открыть терминал**
4. **Проверить настройки сетевых интерфейсов 12. Проверить connectivity**

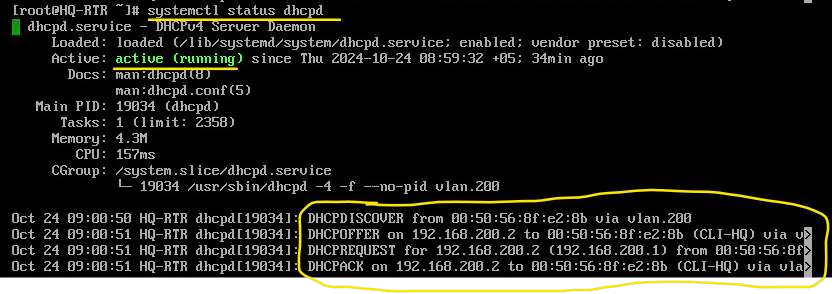
ping ya.ru



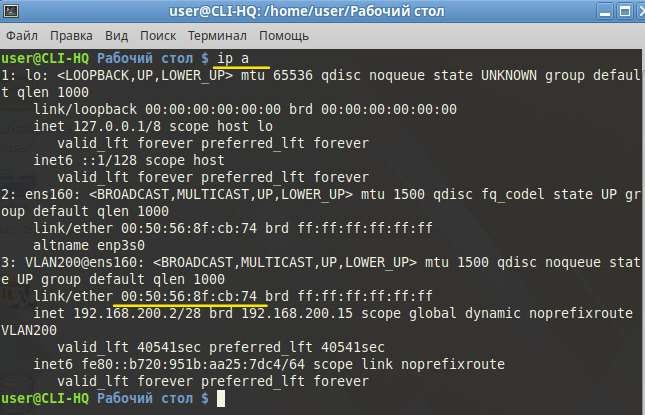
ping 192.168.0.2 (BR-SRV)



1. **На сервере DHCP HQ-RTR проверить состояние службы и результаты процесса выдачи IP адреса:**

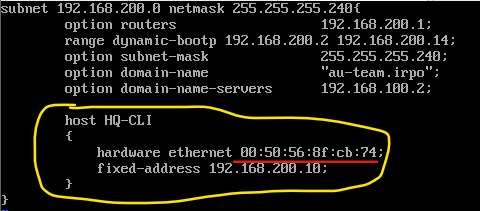


1. **Узнать на HQ-CLI mac-address**



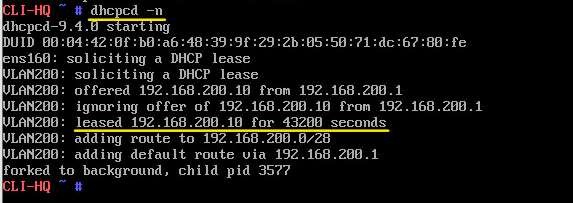
1. **Внести изменения в файл конфигурации DHCP сервера, добавив строку с привязкой ip адреса к MAC адресу:**

**HQ-RTR:** vim /etc/dhcp/dhcpd.conf



1. **Запросить на HQ-CLI новый адрес:**

dhcpcd -n



**Настройка DNS сервера**

**HQ-RTR, BR-RTR:**

1. **Установить в firewalld для всех интерфейсов зону по умолчанию TRUSTED:**



**firewall-cmd --set-default-zone=trusted**

**HQ-SRV:**

1. **Установить программное обеспечение:**

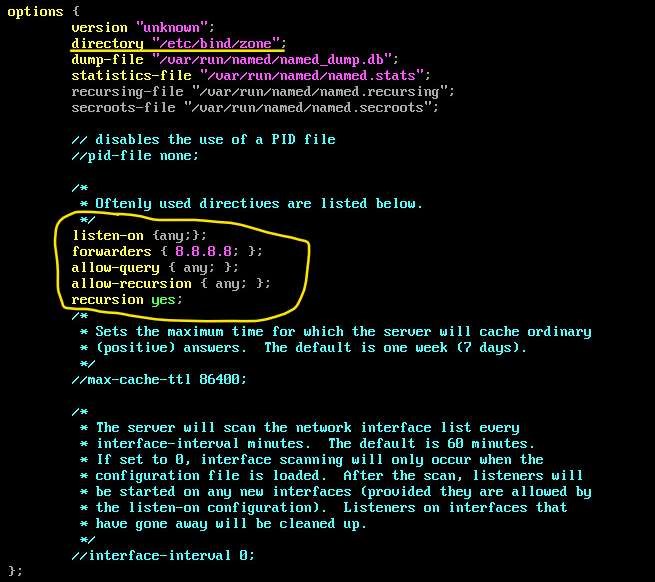
apt-get install bind

1. **Перейти в каталог с настройками DNS**

cd /etc/bind/

1. **Настроить параметры dns сервера в конфигурационном файле /etc/bind/options.conf**

vim options.conf



listen-on { any; };

forwarders { 8.8.8.8; };

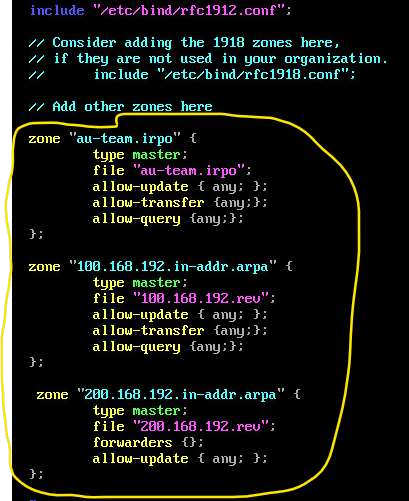
allow-query { any; };

allow-recursion { any; };

recursion yes;

1. **Описать прямые и обратные зоны:**

vim local.conf



zone “au-team.irpo” {

type master;

file “au-team.irpo”;

allow-update { any; };

allow-transfer { any; };

allow-query { any; };

};

zone “100.168.192.in-addr.arpa” {

type master;

file “100.168.192.rev”;

allow-update { any; };

allow-transfer { any; };

allow-query { any; };

};

zone “200.168.192.in-addr.arpa” {

type master;

file “200.168.192.rev”;

forwarders {};

allow-update { any; };

allow-transfer { any; };

allow-query { any; };

};

**!!! ОБРАЩАТЬ ВНИМАНИЕ НА ЗАПЯТЫЕ И ФИГУРНЫЕ СКОБКИ !!!**

1. **Проверить синтаксис конфигурационных файлов зон:**

named-checkconf local.conf

1. **Создать файлы описания зон:**

**!!! Файлы создаются в каталоге /etc/bind/zone !!!**

cd zone

**Прямая зона:**

vim

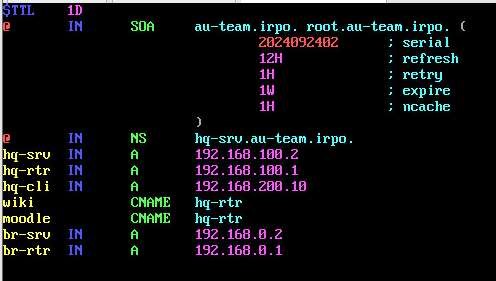
au

-

team

.

irpo



@ IN SOA au-team.irpo. root.au-team.irpo. (

@ IN NS hq-srv.au-team.irpo.

hq-srv IN A 192.168.100.2

hq-rtr IN A 192.168.100.1

hq-cli IN A 192.168.200.10

wiki CNAME hq-rtr

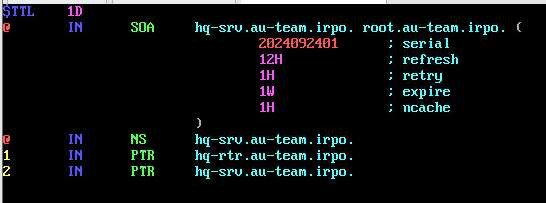
moodle CNAME hq-rtr

br-srv IN A 192.168.0.2

br-rtr IN A 192.168.0.1

**Обратные зоны:**

vim 100.168.192.rev



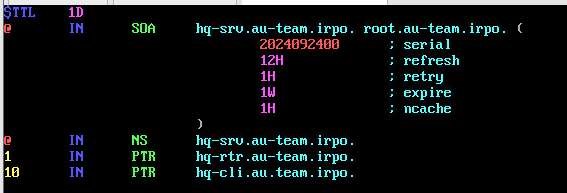
@ IN SOA hq-srv.au-team.irpo. root.au-team.irpo. (

@ IN NS hq-srv.au-team.irpo.

1 IN PTR hq-rtr.au-team.irpo.

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

vim 200.168.192.rev



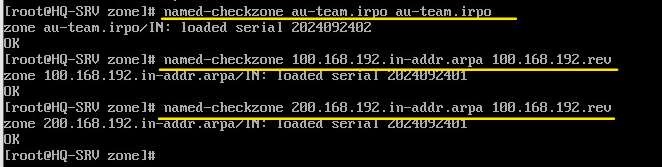
@ IN SOA hq-srv.au-team.irpo. root.au-team.irpo. (

@ IN NS hq-srv.au-team.irpo.

1 IN PTR hq-rtr.au-team.irpo.

10 IN PTR hq-cli.au-team.irpo.

1. **Проверить синтаксис файлов зон:**



named-checkzone au-team.irpo au-team.irpo

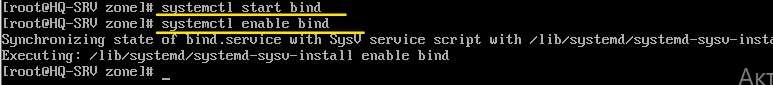
named-checkzone 100.168.192.in-addr.arpa 100.168.192.rev

named-checkzone 200.168.192.in-addr.arpa 200.168.192.rev

1. **Разрешить доступ к каталогу /etc/bind/zone:**

chmod 777 -R /etc/bind/zone

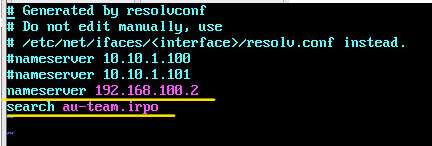
1. **Запустить службу DNS и поставить в автозагрузку:**



systemctl enable --now bind

1. **На всех узлах внести изменения в файл /etc/resolv.conf**

vim /etc/resolv.conf



nameserver 192.168.100.2

search au-team.irpo

1. **Проверить работу службы DNS. На любом узле ввести команды:**

host hq-cli

nslookup hq-cli



Ответ должен приходить от 192.168.100.2

**Модуль 2**

**Настройка ansible**

**Пункт задания: 4**

**На всех хостах (кроме BR-SRVи HQ-SRV):**

1. **Настроить соответствующий доступ SSH:**

vim /etc/openssh/sshd\_config

**Раскомментировать строки**

Port 22

PermitRootLogin yes

PubkeyAuthentication yes

AuthorizedKeysFile /etc/openssh…

**!!! НА серверах BR-SRVи HQ-SRV должен быть настроен доступ только для пользователя sshuser !!!**

**Перезапустить службу sshd**

systemctl restart sshd

**BR-SRV:**

* 1. **Зайти под учетной записью root и создать ssh ключ:**

ssh-keygen

* 1. **Скопировать ключ на хосты: HQ-RTR, HQ-CLI, BR-RTR:**

ssh-copy-id hq-rtr

или (если не работает DNS)

ssh-copy-id 192.168.100.1

Для остальных хостов аналогично.

* 1. **Зайти под учетной записью sshuser и создать ssh ключ:**

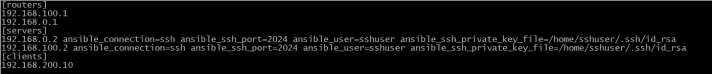
ssh-keygen

* 1. **Скопировать ключ на хост: HQ-SRV**
  2. **Зайти под учетной записью root**
  3. **Установить программное обеспечение:**

apt-get install ansible

* 1. **Заполнить инвентарный файл /etc/ansible/hosts:**

vim /etc/ansible/hosts



**!!! Для подключения к хостам блока [servers] требуется описать подключение от имени sshuser !!!**

[routers]

192.168.100.1

192.168.0.1

[servers]

192.168.0.2 ansible\_connection=ssh ansible\_ssh\_port=2024 ansible\_user=sshuser ansible\_ssh\_private\_key\_file=/home/sshuser/.ssh/id\_rsa

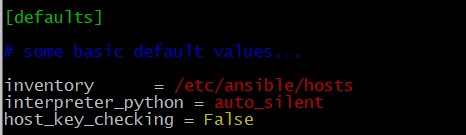
192.168.100.2 ansible\_connection=ssh ansible\_ssh\_port=2024 ansible\_user=sshuser ansible\_ssh\_private\_key\_file=/home/sshuser/.ssh/id\_rsa

[clients]

192.168.200.10

1. **Заполнить конфигурационный файл /etc/ansible/ansible.cfg**

vim /etc/ansible/ansible.cfg



inventory = /etc/ansible/hosts

interpreter\_python = auto\_silent

host\_key\_checking = False

1. **Выполнить команду ping в ansible**

ansible -m ping all

**Настройка chronyd**

**Пункт задания: 3**

**HQ-RTR:**

1. **Установить:**

apt-get install -y chrony

1. **Конфиг vim /etc/chrony.conf**

Любые 3 сервера возьми или оставь существующий.

server ntp1.vniiftri.ru

server ntp2.vniiftri.ru

server ntp3.vniiftri.ru

server 0.asia.pool.ntp.org

server 1.asia.pool.ntp.org

server 2.asia.pool.ntp.org

server 3.asia.pool.ntp.org

allow 192.168.0.0/27

allow 192.168.100.0/26

allow 192.168.200.0/28

local stratum 5

1. **Запуск**

timedatectl set-timezone Asia/Yekaterinburg

systemctl restart chronyd

systemctl enable --now chronyd

1. **Проверка**

chronyc sources -v

chronyc tracking

timedatectl

ntp service active

**Все остальные кроме (HQ-RTR):**

1. **Установить**

apt-get install -y chrony

1. **Конфиг vim /etc/chrony.conf**

server 192.168.200.1 iburst prefer

server 127.0.0.1 iburst

1. **Запуск**

timedatectl set-timezone Asia/Yekaterinburg

systemctl restart chronyd

systemctl enable --now chronyd

1. **Проверка**

chronyc sources -v

chronyc tracking

timedatectl

ntp service active

**Настройка RAID5**

**Пункт задания: 2**

**ПУТЬ НАШЕГО ГЛАВАРЯ ЛЮБИТЕЛЯ СГУЩЕНОЧКИ**

**HQ-SRV:**

1. **Установи парашу**

apt-get install mdadm

1. **Обнуление тебя**

mdadm --zero-superblock --force /dev/sd{b,c,d}

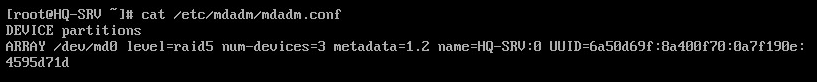
wipefs --all --force /dev/sd{b,c,d}

1. **Создание гойда5**

mdadm --create --verbose /dev/md0 -l 5 -n 3 /dev/sd{b,c,d}

1. **Проверь эту гойду**

lsblk



1. **Создание файла mdadm.conf**

mkdir /etc/mdadm

echo "DEVICE partitions" > /etc/mdadm/mdadm.conf

mdadm --detail --scan --verbose | awk '/ARRAY/ {print}' >> /etc/mdadm/mdadm.conf

1. **Создание файловой системы и монтирование массива**

mkfs.ext4 /dev/md0

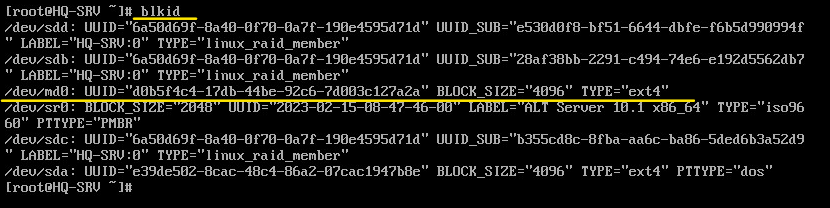
mkdir /etc/raid5

mount /dev/md0 /etc/raid5

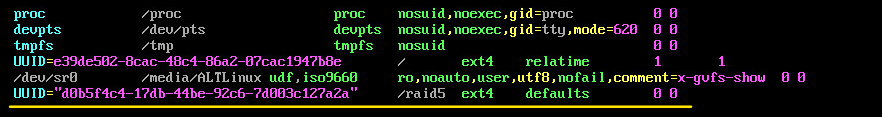
1. **FStab**

Чекни ID

blkid



vim /etc/fstab



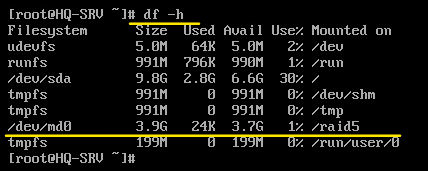
UUID=”XVIDEOS.COM” /etc/raid5 ext4 default 0 0

1. **Отмонтирование**

umount /etc/raid5

mount -a

df -h



**ПУТЬ ФУРРИ**

**HQ-SRV:**

1. **Установи парашу**

apt-get install mdadm cfdisk

1. **Подготовка дисков**

cfdisk /dev/sdb

Удалите все существующие разделы:

Выберите существующий раздел (если есть) → Delete.

Создайте новый раздел:

Выберите New, укажите размер, который хотите выделить под RAID (обычно весь диск).

Измените тип раздела на RAID:

Выберите Type → Найдите и выберите Linux RAID (fd).

Повторите действия для каждого диска, например, /dev/sdc, /dev/sdd.

Сохраните изменения и выйдите:

Выберите Write, подтвердите вводом yes, затем Quit.

1. **Проверь эту гойду**

lsblk

1. **Создание RAID 5 через mdadm**

**mdadm --zero-superblock --force /dev/sd{b,c,d}**

**wipefs --all --force /dev/sd{b,c,d}**

**mdadm --create --verbose /dev/md0 --level=5 --raid-devices=3 /dev/sdb1 /dev/sdc1 /dev/sdd1**

1. **Создание файла mdadm.conf**

mkdir /etc/mdadm

echo "DEVICE partitions" > /etc/mdadm/mdadm.conf

mdadm --detail --scan --verbose | awk '/ARRAY/ {print}' >> /etc/mdadm/mdadm.conf

1. **Создание файловой системы и монтирование массива**

mkfs.ext4 /dev/md0

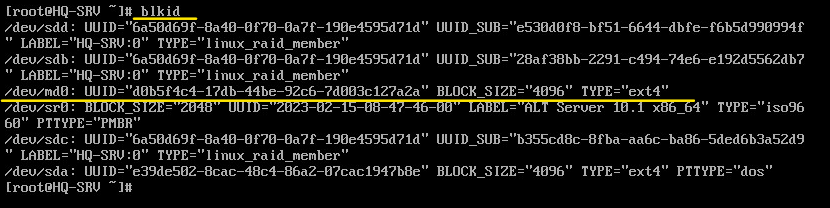
mkdir /etc/raid5

mount /dev/md0 /etc/raid5

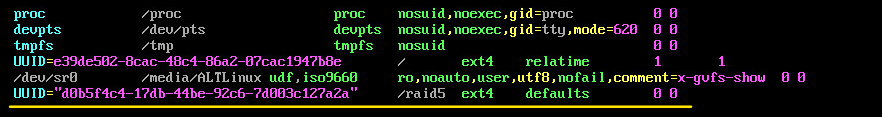
1. **FStab**

Чекни ID

blkid



vim /etc/fstab



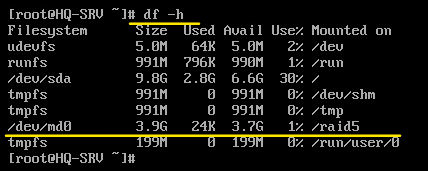
UUID=”XVIDEOS.COM” /etc/raid5 ext4 default 0 0

1. **Отмонтирование**

umount /etc/raid5

mount -a

df -h



**Настройка NFS**

**Пункт задания: 2**

**HQ-SRV:**

1. **Установи парашу**

apt-get install nfs-server

1. **Запуск**

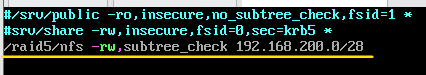
systemctl enable --now nfs

1. **Папочка**

mkdir /raid5/nfs

1. **Конфиг**

vim /etc/exports



/raid5/nfs -rw,subtree\_check 192.168.200.0/28

или

/raid5/nfs 192.168.200.0/28(rw,subtree\_check)

1. **Конфиг**

systemctl restart nfs

exportfs

asda

Напиши че угодно в текстовик

vim /raid5/nfs/test\_nfs.txt

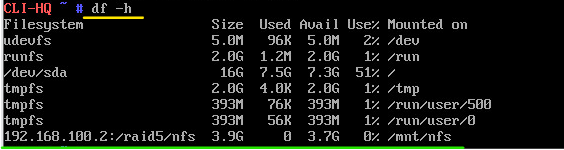
**HQ-CLI:**

1. **Монтируем вручную**

mkdir /mnt/nfs

mount 192.168.100.2:/raid5/nfs /mnt/nfs

df -h



Чекни есть ли файл который ты создал

ls -al /mnt/nfs

1. **Монтируем через FStab**

vim /etc/fstab

192.168.100.2:/raid5/nfs /mnt/nfs nfs rw 0 0

или

hq-srv:/raid5/nfs /mnt/nfs nfs rw 0 0

**Настройка AD (SAMBA DNS)**

**Пункт задания: 1**

***---------------------------------------BR-SRV---------------------------------------***

1. **Установи парашу**

apt-get install task-samba-dc

1. **Переименовать**

**Открываешь:**

vim /etc/sysconfig/network

**И пишешь туда:**

HOSTNAME=BR-SRV.au-team.irpo

**И выполни команды:**

hostnamectl set-hostname BR-SRV.au-team.irpo

domainname au-team.irpo

1. **netplan**

vim /etc/netplan/config.yaml

**добавляешь LO IP (127.0.0.1)**



netplan apply

1. **Очистить SMB от кеша**

rm -f /etc/samba/smb.conf

rm -rf /var/lib/samba

rm -rf /var/cache/samba

mkdir -p /var/lib/samba/sysvol

rm -f /etc/samba/smb.conf

1. **Создаем**

samba-tool domain provision

все ENTER и пароль P@ssw0rd

1. **Запуск**

systemctl enable --now samba

1. **Редачь конфиг**

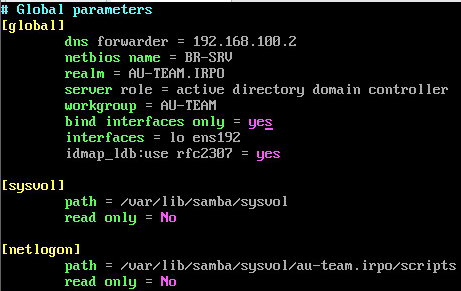
vim /etc/samba/smb.conf

**добавь в конце global**

bind interfaces only = yes

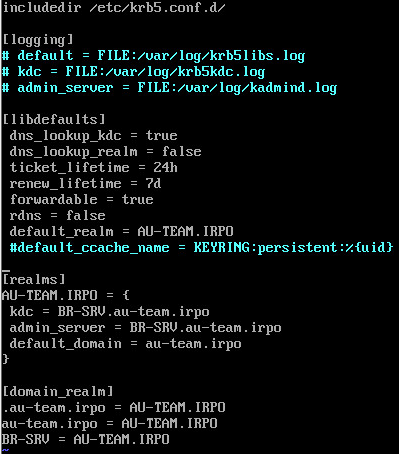
interfaces = lo ens192

idmap\_ldb:use rfc2307 = yes



1. **Редачь конфиг**

vim /etc/krb5.conf



**Можешь тупо посмотреть примерно как:**

cat /var/lib/samba/private/krb5.conf

1. **Проверка**

samba-tool domain info 127.0.0.1

smbclient -L localhost -U administrator

kinit administrator@AU-TEAM.IRPO

1. **Создание юзеров**

samba-tool user create ivanov --given-name='Ivan Dolbaeb' --mail-address='ivanov@au-team.irpo'

**пароль:**

P@ssw0rd

samba-tool user setexpiry ivanov –noexpiry

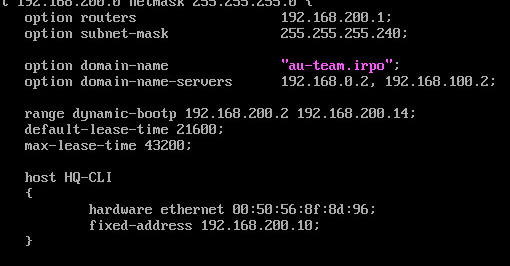
***---------------------------------------HQ-RTR---------------------------------------***

1. **Добавление еще одного сервера в DHCP**

**Открывай**

vim /etc/dhcp/dhcpd.conf

**и добавляй 192.168.0.2**



systemctl restart dhcpd

***---------------------------------------HQ-CLI---------------------------------------***

1. **Установи парашу**

apt-get install task-auth-ad-sssd alterator-gpupdate

**Если ошибка во время установки:**

**file /usr/bin/alterator-datetime-functions from install of alterator-datetime-functions-4.9.2-alt1x86\_64 conflicts with file from package alterator-datetime-4.8.1-alt1.x86\_64**

**E: Error while running transaction**

**То:**

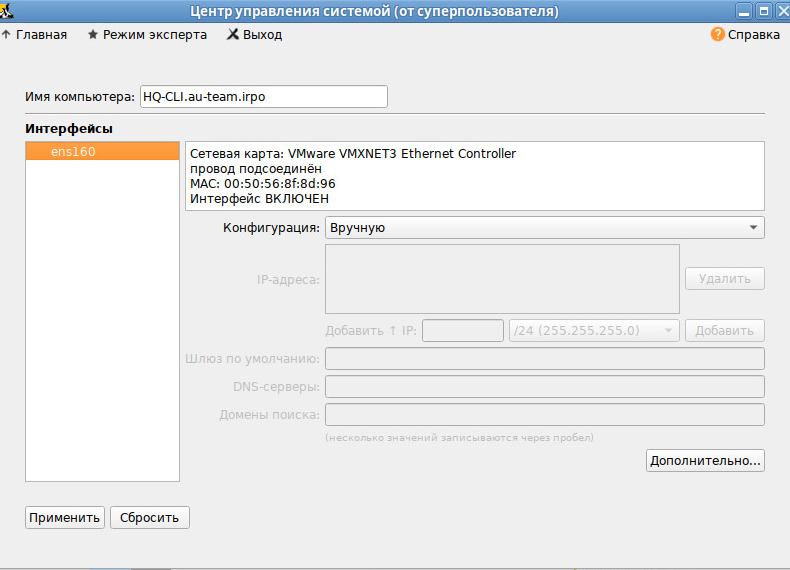
apt-get remove alterator-datetime

apt-get install task-auth-ad-sssd alterator-gpupdate

**Если ошибка при apt-get update то блять чини ебаный DNS укажи его в ебучем /etc/resolv.conf либо почини свой ебаный DHCP чтобы он рассказывал об DNS нахуй этому ебучему клиенту придурок**

1. **Задай имя и домен поиска**

**В ЦУС (см. Центр управления системой) «Сеть» → «Ethernet интерфейсы»**



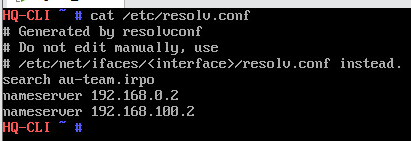
**В консоли/терминале:**

hostnamectl set-hostname HQ-CLI.au-team.irpo

reboot

**проверка**

cat /etc/resolv.conf



1. **Ввод в AD**

**(Введите в домен машину HQ-CLI)**

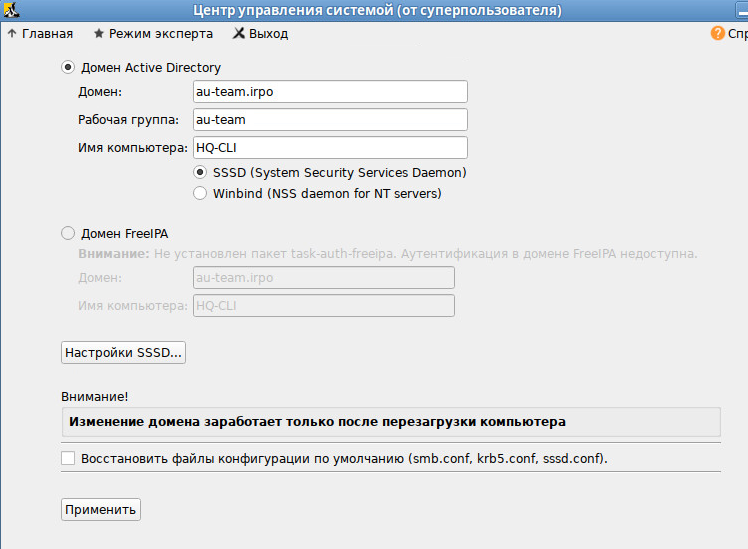
system-auth write ad au-team.irpo HQ-CLI au-team 'administrator' 'P@ssw0rd’

**либо**

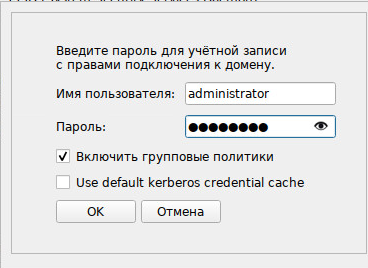
**ЦУС (см. Центр управления системой) необходимо выбрать пункт «Пользователи»→«Аутентификация»**

**В окне модуля «Аутентификация» следует выбрать пункт «Домен Active Directory»,**

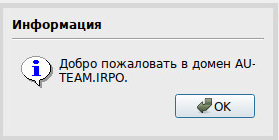
**заполнить поля («Домен», «Рабочая группа», «Имя компьютера»), выбрать пункт «SSSD (в единственном домене)» и нажать кнопку «Применить»**



**применить**



**(P@ssw0rd)**

****

***---------------------------------------BR-SRV---------------------------------------***

**(Создайте 5 пользователей для офиса HQ: имена пользователей**

**формата user№.hq. Создайте группу hq, введите в эту группу созданных**

**пользователей)**

1. **Создаем 5 геев**

samba-tool user add user1.hq

samba-tool user add user2.hq

samba-tool user add user3.hq

samba-tool user add user4.hq

samba-tool user add user5.hq

1. **Создаем группу**

samba-tool group add hq

1. **Добавляем геев в группу**

samba-tool group addmembers hq user1.hq,user2.hq,user3.hq,user4.hq,user5.hq

**Настройка Apache2 + NGINX (НЕ ТРЕБУЕТСЯ ПО ЗАДАНИЮ)**

**Пункт задания: (?)**

**BR-SRV:**

1. **Установить:**

apt-get install -y httpd2 nginx

systemctl enable --now httpd2 nginx

1. **Создать папки:**

mkdir -p /var/www/html/au-team.irpo

mkdir -p /var/www/html/au-team.irpo/data

1. **Создайте HTML & PHP**

vim /var/www/html/au-team.irpo/index.html

<html>

<h1>Hello World (MAIN)!</h1>

</html>

vim /var/www/html/au-team.irpo/data/index.html

<html>

<h1>Hello World (DATA)!</h1>

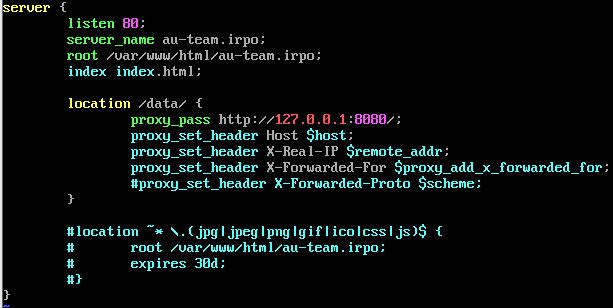
</html>

1. **Создаем конфиг для сайта NGINX**

vim /etc/nginx/sites-available.d/au-team.irpo.conf

ln -s /etc/nginx/sites-available.d/au-team.irpo.conf /etc/nginx/sites-enabled.d/au-team.irpo.conf

(или просто vim /etc/nginx/sites-enabled.d/au-team.irpo.conf)



1. **Перезапуск**

systemctl restart nginx

nginx -s reload

1. **Конфиг Apache2**

vim /etc/httpd2/conf/ports-enabled/http.conf

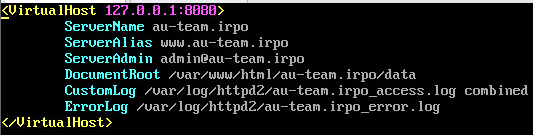


1. **Создаем конфиг для сайта NGINX**

vim /etc/httpd2/conf/sites-available/au-team.irpo.conf

ln -s /etc/httpd2/conf/sites-available/au-team.irpo.conf /etc/httpd2/conf/sites-enabled/au-team.irpo.conf

(или просто vim /etc/httpd2/sites-enabled/au-team.irpo.conf)



1. **Рестарт Apache2**

systemctl restart httpd2

1. **HOSTS**

**HQ-CLI:**

vim /etc/hosts

au-team.irpo 192.168.0.2

1. **Проверка**

**BR-SRV:**

netstat -tulpn | grep 80

curl -i 192.168.0.2

curl 192.168.0.2

curl -i 192.168.0.2/data/

curl 192.168.0.2/data/

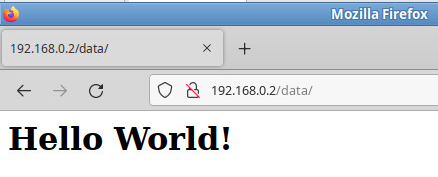
**HQ-CLI:**

192.168.0.2

192.168.0.2/data/

au-team.irpo

au-team.irpo/data/



**Настройка Docker**

**Пункт задания: 5**

**BR-SRV:**

1. **Установить:**

apt-get install -y docker-engine

systemctl enable --now docker

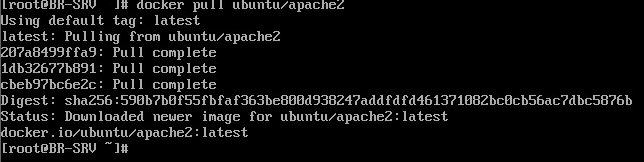
1. **Поиск:**

docker search apache2



1. **Установка контейнера:**

docker pull ubuntu/apache2

****

1. **Проверка существующих образов:**

docker images

****

1. **В папку юзера:**

cd ~

1. **Создаешь там папки:**

mkdir html1

mkdir html2

1. **В них создаешь ебучие веб страницы:**

vim html1/index.html

<h1> Hello from container 1</h1>

vim html2/index.html

<h1> Hello from container 2</h1>

1. **Запуск контейнеров:**

docker run -d -v ~/html1:/var/www/html -p 8081:80 --name myapache1 ubuntu/apache2

docker run -d -v ~/html2:/var/www/html -p 8082:80 --name myapache2 ubuntu/apache2

1. **Проверка:**

docker ps

apt-get install curl

curl -i 192.168.0.2:8081

curl -i 192.168.0.2:8082

**Если проебался то:**  
docker ps -a

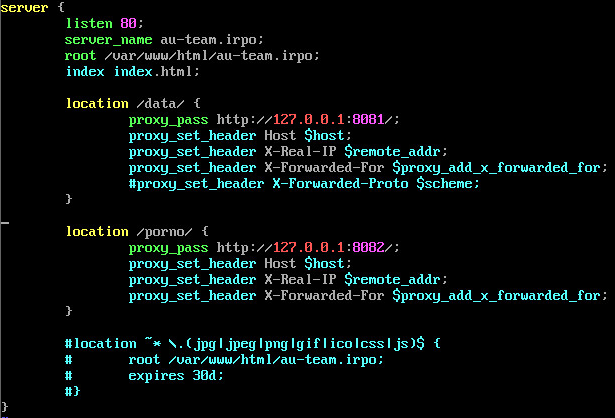
docker rm **НАЗВАНИЕ к примеру:**docker rm myapache1

1. **Настройка Nginx:**

vim /etc/nginx/sites-available.d/au-team.irpo.conf

ln -s /etc/nginx/sites-available.d/au-team.irpo.conf /etc/nginx/sites-enabled.d/au-team.irpo.conf

(или просто vim /etc/nginx/sites-enabled.d/au-team.irpo.conf)



1. **Чтобы страницы редачить ебашь эти файлы:**

vim ~/html1/index.html

vim ~/html2/index.html

1. **Проверка:**

**HQ-CLI:**

В Firefox:

http://192.168.0.2

http://192.168.0.2:8081

http://192.168.0.2:8082

http://au-team.irpo/

http://au-team.irpo/data/

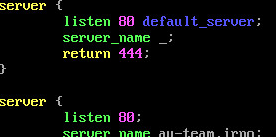
http://au-team.irpo/porno/

1. **Отключение доступа по IP:**

vim /etc/nginx/sites-available.d/au-team.irpo.conf

ln -s /etc/nginx/sites-available.d/au-team.irpo.conf /etc/nginx/sites-enabled.d/au-team.irpo.conf

(или просто vim /etc/nginx/sites-enabled.d/au-team.irpo.conf)



1. **Остановка контейнеров:**

docker ps -a

docker stop myapache1

docker stop myapache2

docker rm myapache1

docker rm myapache2

1. **Скрипт для автоподнятия контйнеров:**

vim /sbin/start\_web.sh

**#!/bin/bash**

**docker run -d -v ~/html1:/var/www/html -p 8081:80 --name myapache1 ubuntu/apache2**

**docker run -d -v ~/html2:/var/www/html -p 8082:80 --name myapache2 ubuntu/apache2**

chmod +x /sbin/start\_web.sh

1. **Создание сервисаx Systemd:**

vim /etc/systemd/system/start\_web.service

**[Unit]**

**Description=Start Web Service**

**After=network.target nginx.service docker.service**

**Requires=nginx.service docker.service**

**[Service]**

**Type=simple**

**User=root**

**ExecStart=/sbin/start\_web.sh**

**Restart=always**

**Environment="PATH=/usr/bin:/usr/local/bin:/sbin"**

**[Install]**

**WantedBy=multi-user.target**

systemctl daemon-reload

systemctl enable --now start\_web.service

**Настройка SSL (НЕ ТРЕБУЕТСЯ ПО ЗАДАНИЮ)**

**Пункт задания: ?**

**BR-SRV:**

1. **Установить:**

apt-get install -y apache2-mod\_ssl openssl

1. **Создайте директорию для хранения сертификатов:**

mkdir -p /etc/nginx/ssl

chmod 700 /etc/nginx/ssl

1. **Сгенерируйте приватный ключ и CSR (Certificate Signing Request):**

openssl req -new -newkey rsa:2048 -nodes -keyout /etc/nginx/ssl/au-team.irpo.key -out /etc/nginx/ssl/au-team.irpo.csr

В процессе генерации вам нужно будет ввести данные для сертификата:

- Country Name (2 letter code) [XX]: RU

- State or Province Name (full name) []: Ваш регион

- Locality Name (eg, city) [Default City]: Ваш город

- Organization Name (eg, company) [Default Company Ltd]: Название вашей организации

- Organizational Unit Name (eg, section) []: Отдел

- Common Name (eg, your name or your server's hostname) []: au-team.irpo

- Email Address []: email@example.com

1. **Создайте самоподписанный сертификат (если не планируете покупать коммерческий):**

openssl x509 -req -days 365 -in /etc/nginx/ssl/au-team.irpo.csr -signkey /etc/nginx/ssl/au-team.irpo.key -out /etc/nginx/ssl/au-team.irpo.crt

1. **Настройте NGINX для работы с SSL. Отредактируйте конфигурационный файл:**

vim /etc/nginx/sites-available.d/au-team.irpo.conf

Добавьте следующие строки:

server {

listen 443 ssl;

server\_name au-team.irpo;

ssl\_certificate /etc/nginx/ssl/au-team.irpo.crt;

ssl\_certificate\_key /etc/nginx/ssl/au-team.irpo.key;

ssl\_protocols TLSv1.2 TLSv1.3;

ssl\_ciphers HIGH:!aNULL:!MD5;

location / {

proxy\_pass http://127.0.0.1:80;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

}

}

1. **Перезапустите NGINX:**

systemctl restart nginx

1. **Для Apache2 также нужно настроить SSL в конфигурации:**

vim /etc/httpd2/conf/sites-available/au-team.irpo.conf

Добавьте:

<VirtualHost \*:443>

ServerName au-team.irpo

SSLEngine on

SSLCertificateFile /etc/nginx/ssl/au-team.irpo.crt

SSLCertificateKeyFile /etc/nginx/ssl/au-team.irpo.key

DocumentRoot /var/www/html/au-team.irpo

<Directory /var/www/html/au-team.irpo>

Options Indexes FollowSymLinks

AllowOverride All

Require all granted

</Directory>

ErrorLog ${APACHE\_LOG\_DIR}/error.log

CustomLog ${APACHE\_LOG\_DIR}/access.log combined

</VirtualHost>

1. **Включите SSL модуль в Apache2:**

a2enmod ssl

systemctl restart httpd2

1. **Проверьте работу SSL:**

HQ-CLI:

https://au-team.irpo

**Настройка Wiki**

**Пункт задания: 5**

**BR-SRV:**

1. **Установить:**

apt-get install -y docker-engine docker-compose

1. **Включить:**

systemctl enable docker --now

1. **Заполнить:**

vim ~/docker-compose.yaml

version: '3.4'

services:

mariadb:

container\_name: mariadb

image: mariadb:10.8

ports:

- 3306:3306

volumes:

- mysql-data:/var/lib/mysql

environment:

MARIADB\_USER: wiki

MARIADB\_PASSWORD: P@ssw0rd

MARIADB\_ROOT\_PASSWORD: P@ssw0rd

restart: always

mediawiki:

image: mediawiki

restart: always

container\_name: wiki

ports:

- 8080:80

depends\_on:

- mariadb

volumes:

- mediawiki-images:/var/www/html/images

#- ./LocalSettings.php:/var/www/html/LocalSettings.php

volumes:

mysql-data:

driver: local

mediawiki-images:

driver: local

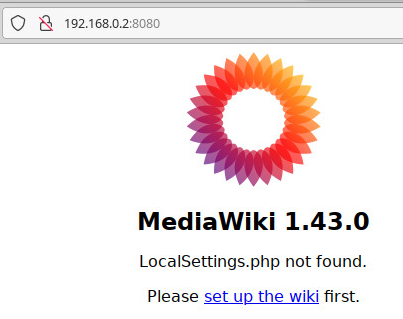
1. **Запуск:**

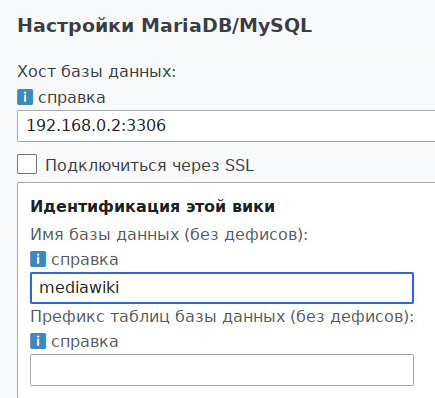
docker compose up

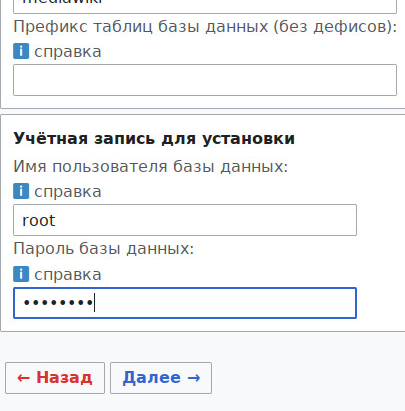
1. **Настройка:**

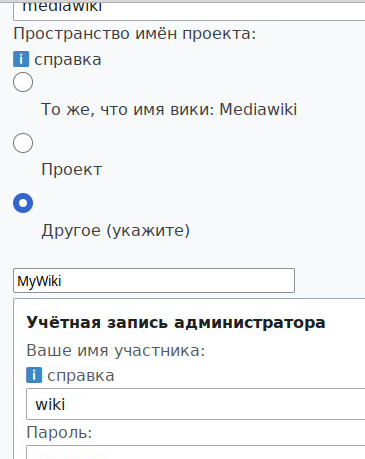
**HQ-CLI:**

Подключаешься по 192.168.0.2:8080

****

****

****

****

!Пароль от юзера wiki - WikiP@ssw0rd!

1. **Перекидывай на сервак:**

scp -P 2024 ~/Загрузки/LocalSettings.php sshuser@192.168.0.2:/home/sshuser/

1. **Редачь конфиг:**

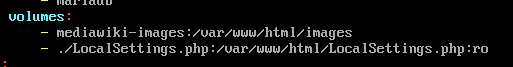
**BR-SRV:**

mv /home/sshuser/LocalSettings.php /root/

docker compose down

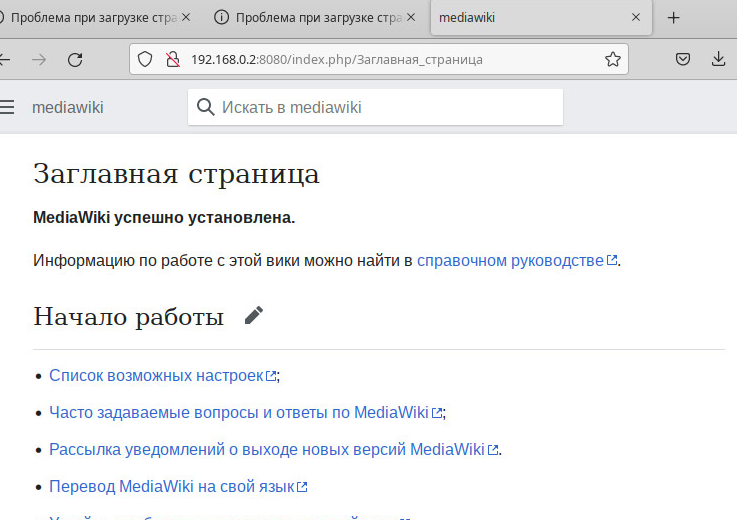
vim ~/docker-compose.yaml

Расскоментируй - ./LocalSettings.php



**Если пишет что файл не найден то убери нахуй :ro**

docker compose up

****

**Статическая трансляция портов**

**Пункт задания: 6**

**BR-SRV:**

1. **Ебашь:**

<BR-RTR\_IP> = 172.16.5.2

<HQ-RTR\_IP> = 172.16.4.2

<BR-SRV\_IP> = 192.168.0.2

<HQ-SRV\_IP> = 192.168.100.2

**BR-RTR:**

firewall-cmd --zone=trusted --add-forward-port=port=2024:proto=tcp:toport=2024:toaddr=192.168.0.2 --permanent

firewall-cmd --zone=trusted --add-forward-port=port=80:proto=tcp:toport=8080:toaddr=192.168.0.2 --permanent

firewall-cmd –reload

**HQ-RTR:**

firewall-cmd --zone=trusted --add-forward-port=port=2024:proto=tcp:toport=2024:toaddr=192.168.100.2 --permanent

firewall-cmd --reload

**ISP:**

**NE RABOTAET**

apt-get install iptables-persistent

iptables -t nat -A PREROUTING -p tcp --dport 2030 -j DNAT --to-destination 172.16.4.2:2024

iptables -t nat -A PREROUTING -p tcp --dport 2031 -j DNAT --to-destination 172.16.5.2:2024

iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 172.16.5.2:80

iptables-save | tee /etc/iptables/rules.v4

**Настройка MOODLE**

**Пункт задания: 7**

**HQ-SRV:**

1. **Проверка DNS:**

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

1. **Установи apache2:**

apt-get install httpd2

systemctl enable httpd2 --now

1. **Создание веб морды:**

mkdir -p /var/www/html/moodle

vim /var/www/html/moodle/index.html

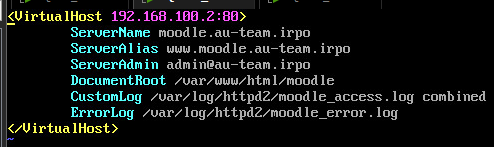
<h1>MOODLE</h1>

1. **Создаем конфиг для сайта APACHE2**

vim /etc/httpd2/conf/sites-available/moodle.conf

ln -s /etc/httpd2/conf/sites-available/moodle.conf /etc/httpd2/conf/sites-enabled/moodle.conf

(или просто vim /etc/httpd2/sites-enabled/moodle.conf)



1. **Рестарт Apache2**

systemctl restart httpd2

**HQ-RTR:**

1. **Установка NGINX:**

apt-get install nginx

systemctl enable --now nginx

1. **Настройка NGINX:**

vim /etc/nginx/sites-available.d/moodle.conf

ln -s /etc/nginx/sites-available.d/moodle.conf /etc/nginx/sites-enabled.d/moodle.conf

(или просто vim /etc/nginx/sites-enabled.d/moodle.conf)

**Вставь:**  
server {

listen 80;

server\_name moodle.au-team.irpo;

location / {

proxy\_pass http://192.168.100.2:80;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

proxy\_set\_header X-Forwarded-Proto $scheme;

}

}

server {

listen 80;

server\_name wiki.au-team.irpo;

location / {

proxy\_pass http://192.168.0.2:8080;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

proxy\_set\_header X-Forwarded-Proto $scheme;

}

}

**HQ-RTR:**

1. **DHCP:**

Скорее всего у тебя не откроются сайты если у тебя первым идет IP от AD (192.168.0.2), нада менять на (192.168.100.2)

vim /etc/dhcp/dhcpd.conf



**Установка худшего браузера топ 1 по уебищности после Amigo**

**Пункт задания: 9**

**HQ-CLI:**

apt-get install yandex-browser

или

apt-get install yandex-browser-stable