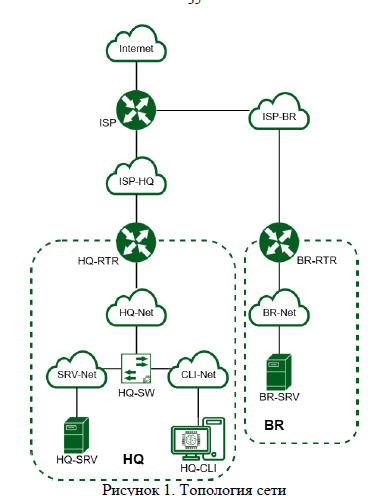
**Решение модуля 1**



**ЗАДАНИЕ 1.** Произведите базовую настройку устройств:

● Настройте имена устройств согласно топологии. Используйте полное доменное имя

● 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

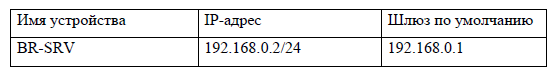
● Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 16 адресов

● 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

Таблица 3. Пример



**Решение**

Таблица адресов

|  |  |  |
| --- | --- | --- |
| Имя устройства | IP-адрес | Шлюз по умолчанию |
| ISP | 192.168.44.211/24 (получен по DHCP, сеть колледжа)  172.16.4.1/28  172.16.5.1/28 | 192.168.44.1 |
| HQ-RTR | 172.16.4.10/28  192.168.99.1/29  192.168.100.1/28  192.168.200.1/28  10.5.5.1/30 | 172.16.4.1 |
| HQ-SRV | 192.168.100.10/28 | 192.168.100.1 |
| HQ-CLI | 192.168.200.10/28 | 192.168.200.1 |
| BR-RTR | 172.16.5.10/28  192.168.0.1/28  10.5.5.2/30 | 172.16.5.1 |
| BR-SRV | 192.168.0.10/28 |  |

**ЗАДАНИЕ 2. Настройка ISP**

● Настройте адресацию на интерфейсах:

Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP

Настройте маршруты по умолчанию там, где это необходимо

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

**Решение**

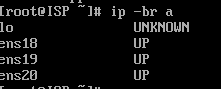
Настройка адресов на ВМ:

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ISP: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

apt-get update –y

apt-get install –y NetworkManager-tui

ip –br a



vim /etc/net/ifaces/ens18/options (NM\_CONTRILLED=yes)

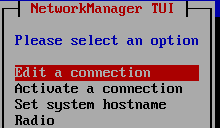
vim /etc/net/ifaces/ens19/options (NM\_CONTRILLED=yes)

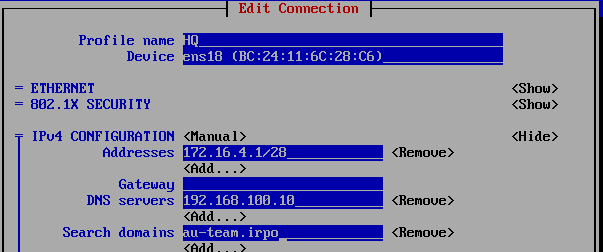
systemctl enable --now NetworkManager

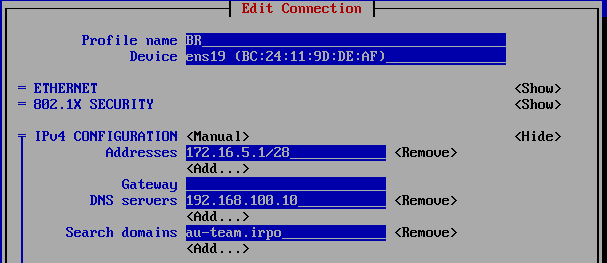
systemctl restart network

#теперь работает команда nmtui

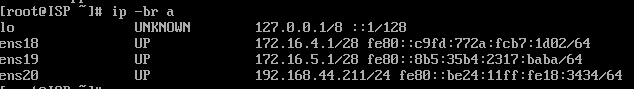








Перезагрузить интерфейсы, проверить, что адреса появились



Включаем пересылку пакетов:

vim /etc/net/sysctl.conf ()

* включаем NAT (чтобы в дальнейшем все ВМ выходили в интернет):

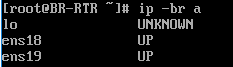
iptables -t nat -A POSTROUTING -j MASQUERADE -o ens20 (интерфейс в сторону колледжа)

iptables-save >> /etc/sysconfig/iptables

systemctl enable --now iptables

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_BR-RTR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Включим интернет, чтобы скачать network-manager:



ens18 – подключен к ISP  
ens19 – подключен к BR-SRV

 (установим ip-адрес)



 (установим шлюз)

 - адрес ISP

systemctl restart network

Включаем пересылку пакетов:

vim /etc/net/sysctl.conf ()

проверить, что есть интернет:

ping 8.8.8.8

apt-get update -y

apt-get install -y NetworkManager-tui

vim /etc/net/ifaces/ens18/opions (NM\_CONTRILLED=yes)

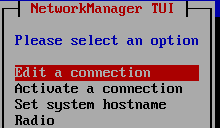
vim /etc/net/ifaces/ens19/opions (NM\_CONTRILLED=yes)

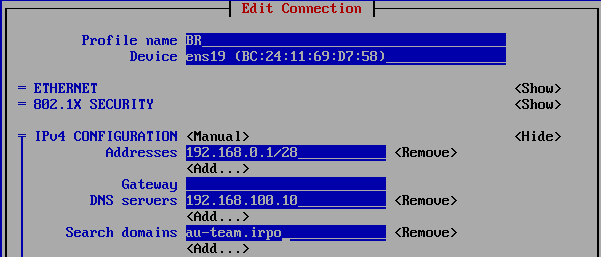
systemctl restar network

systemctl restar Network-Manager

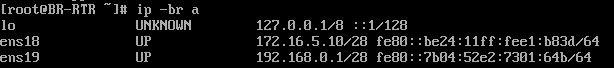
#теперь работает команда nmtui







Перезагрузить интерфейсы, проверить, что адреса появились



**Не забыть поменять hostname!! (через nmtui во вкладке «set a hostname»)**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_BR-SRV: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Настроим интерфейс:



 (установим ip-адрес)



 (установим шлюз)

 - адрес BR-RTR

 - dns server

 - при **не скачивании пакетов поставить 8.8.8.8**

systemctl restart network

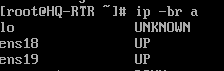
Включаем пересылку пакетов:

vim /etc/net/sysctl.conf ()

**Не забыть поменять hostname!! (через nmtui во вкладке «set a hostname»)**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_HQ-RTR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Включим интернет, чтобы скачать network-manager:



ens18 – подключен к ISP  
ens19 – подключен к HQ-SW

 (установим ip-адрес)



 (установим шлюз)

 - адрес ISP

 - dns-server

 - при **не скачивании пакетов поставить 8.8.8.8**

systemctl restart network

Включаем пересылку пакетов:

vim /etc/net/sysctl.conf ()

проверить, что есть интернет:

ping 8.8.8.8

**Не забыть поменять hostname!! (через nmtui во вкладке «set a hostname»)**

На HQ-SRV, BR-SRV – поставить ip-адреса аналогично через файлы

/etc/net/ifaces/ens18/ipv4address – указать IP

/etc/net/ifaces/ens18/ipv4router – указать шлюз (default via <IP RTR>)

/etc/net/ifaces/ens18/resolv.conf - указать адрес DNS-сервера и домен (nameserver 192.168.100.10, domain au-team.irpo) - при **не скачивании пакетов поставить 8.8.8.8**

**ЗАДАНИЕ 3.** Создание локальных учетных записей

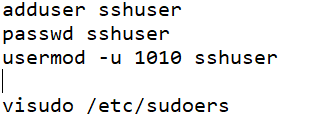
● Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV

o Пароль пользователя sshuser с паролем **P@ssw0rd**

o Идентификатор пользователя 1010

o Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации.

**Решение**

- вписать пароль P@ssw0rd



Раскомментировать строчки (их не надо писать с 0, просто найти в конце и раскомментировать!!):





Вписать ТОЛЬКО нового пользователя в группу wheel (она уже СУЩЕСТВУЕТ)



● Создайте пользователя net\_admin на маршрутизаторах HQ-RTR и BR-RTR

o Пароль пользователя net\_admin с паролем P@$$word

o При настройке ОС на базе Linux, запускать sudo без дополнительной аутентификации

**Решение**

 - вписать пароль P@ssw0rd



Раскомментировать строчки (их не надо писать с 0, просто найти в конце и раскомментировать!!):





Вписать ТОЛЬКО нового пользователя в группу wheel (она уже СУЩЕСТВУЕТ)

**ЗАДАНИЕ 4.** 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

**Решение**

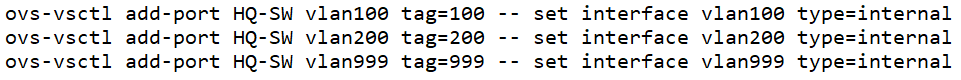
Установить и включить службу



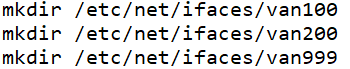
Создать бридж и закрепить его на интерфейс в сторону CLI и SRV



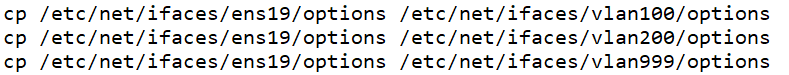
Создать вланы и привязать их к бриджу



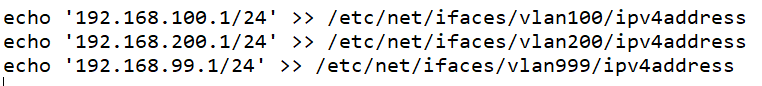
Создать папки вланов для хранения сетевых параметров



Скопировать шаблон options в папки вланов

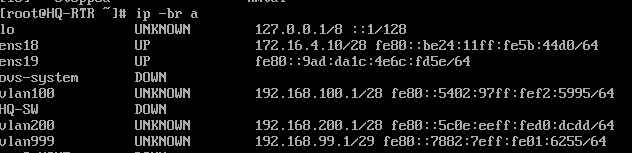


Задать адреса вланам



Перезагрузить службу и проверить, что вланы появились





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

● Для подключения используйте порт 2024

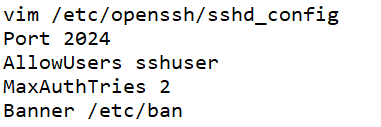
● Разрешите подключения только пользователю sshuser

● Ограничьте количество попыток входа до двух

● Настройте баннер «Authorized access only»

**Решение**

Добавить параметры SSH по заданию в файл конфигурации



Настроить файл баннера





**ЗАДАНИЕ 6.** Между офисами HQ и BR необходимо сконфигурировать ip туннель

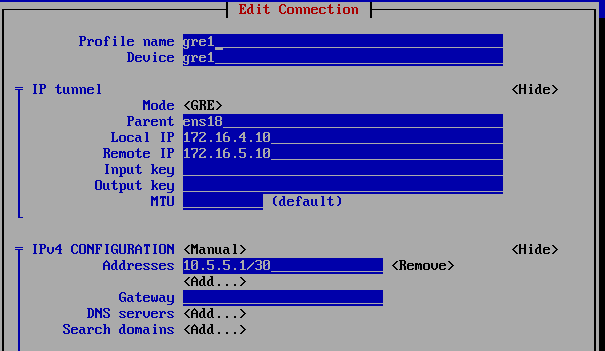
• Сведения о туннеле занесите в отчёт

• На выбор технологии GRE или IP in IP

**Решение**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_HQ-RTR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Создать интерфейс для туннеля GRE (IP-tunnel), ens18 - тот, что в ISP



Настроить TTL



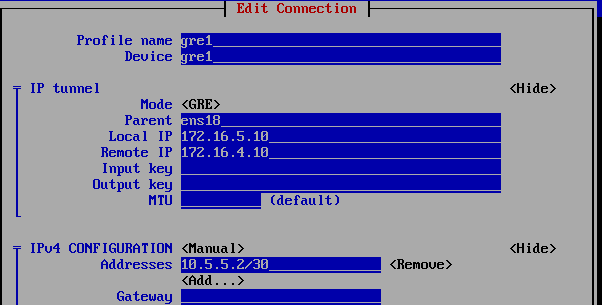






**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_BR-RTR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Создать интерфейс для туннеля GRE (IP-tunnel), ens18 - тот, что в ISP



Настроить TTL









**ЗАДАНИЕ 7.** 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

**Решение**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_BR-RTR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Установить пакет frr



Отредактировать файл





Перезапустить службу и ввести ее в автозагрузку





Указать маршруты, пассивные интерфейсы

Сохранить изменения (wr mem)

Перезагрузить службу



**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_HQ-RTR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

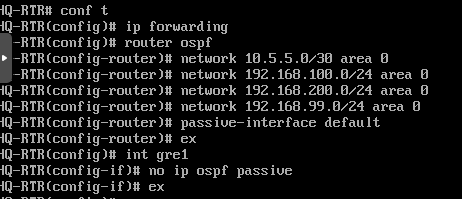
Установить пакет frr

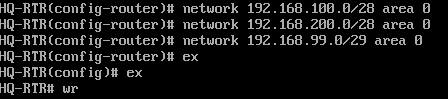


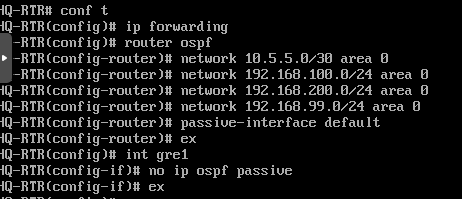
Отредактировать файл /etc/frr/daemons (ospfd = yes)

Перезапустить службу и ввести ее в автозагрузку (systemctl enable –now frr)

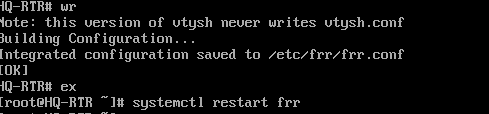












**ЗАДАНИЕ 8.** Настройка динамической трансляции адресов.

● Настройте динамическую трансляцию адресов для обоих офисов.

● Все устройства в офисах должны иметь доступ к сети Интернет

**Решение**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_HQ-RTR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

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

iptables-save >> /etc/sysconfig/iptables

systemctl enable --now iptables

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_BR-RTR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

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

iptables-save >> /etc/sysconfig/iptables

systemctl enable --now iptables

**ЗАДАНИЕ 9.** 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

**Решение**

гзвфеу-ыефегзвфеу



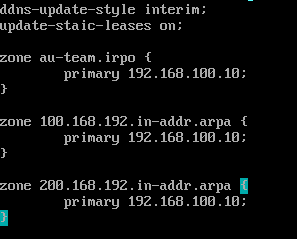
 - сеть CLI

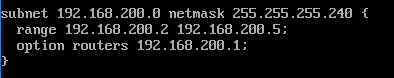
Копируем шаблон конфигурации dhcp

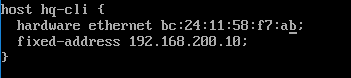


vim /etc/dhcp/dhcpd.conf

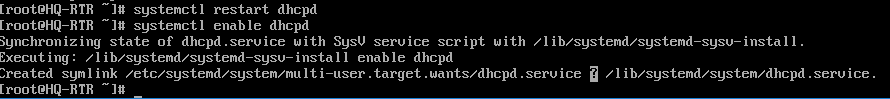






 - **mac-адрес HQ-CLI**

Перезагрузить службу

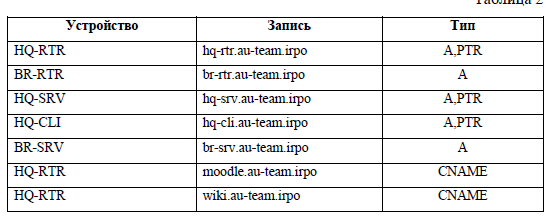


**ЗАДАНИЕ 10.** Настройка DNS для офисов HQ и BR.

● Основной DNS-сервер реализован на HQ-SRV.

● Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 2

Таблица 2. DNS-зоны



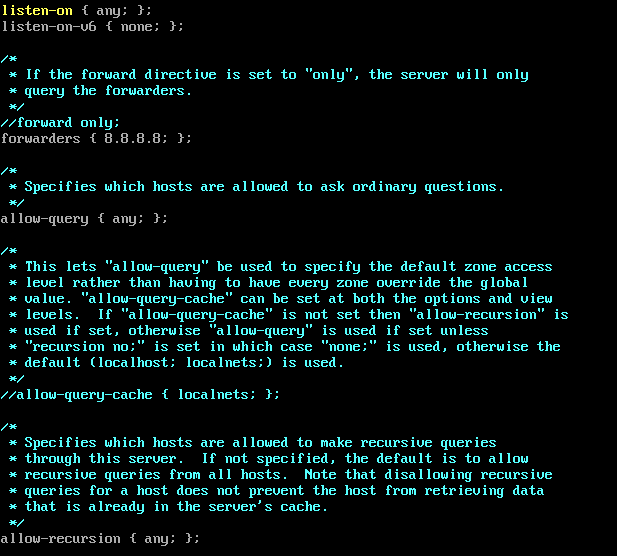
● В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер

**Решение**

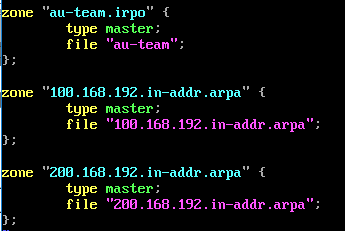
Установить bind



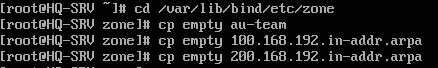






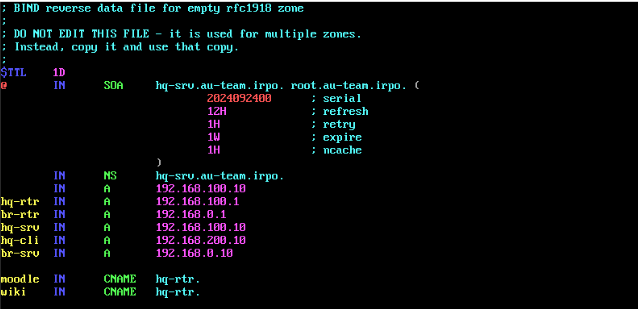


Копируем файл empty (шаблон) в au-team, 100.168.192.in-addr.arpa, 200.168.192.in-addr.arpa:

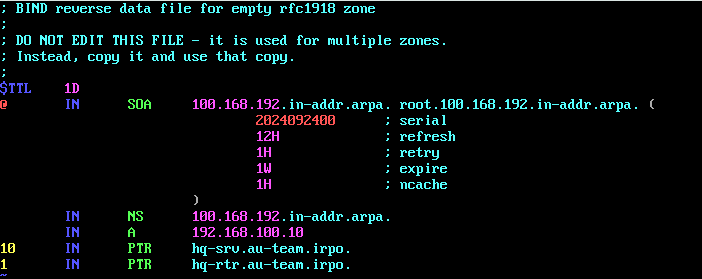
****

сконфигурируем зоны

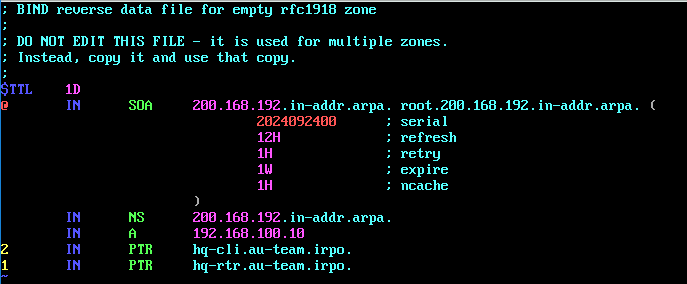












Настраиваем утилиту rndc (для корректного запуска bind)

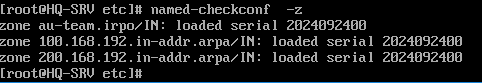


****

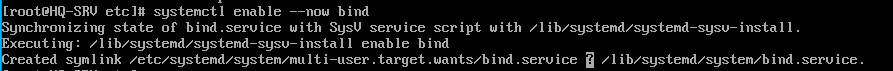
****

****

****

****

Перезапустить службу



**ЗАДАНИЕ 11.** Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена. *(+ЗАДАНИЕ 3. Модуля 2)*

* В качестве сервера выступает HQ-RTR
* На HQ-RTR настройте сервер chrony, выберите стратум 5
* В качестве клиентов настройте HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.

Настройка сервера времени (**HQ-RTR**)

Установить временную зону - Калининград



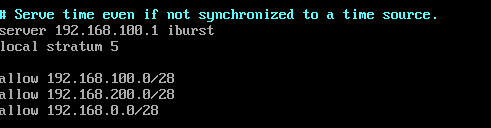
Скачать пакет Chrony



Сконфигурировать файл для настройки сервера



Указать адрес сервера (ip HQ-RTR, stratum 5, разрешенные сети для синхронизации)



Перезагрузить службу:

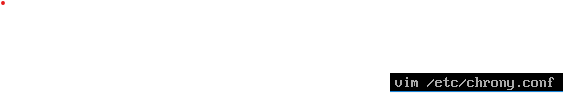


Настройка клиентов синхронизации времени (**HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.)**

Установить службу синхронизации времени



Отредактировать файл, указать адрес сервера, с кем требуется синхранизация (адрес HQ-RTR)

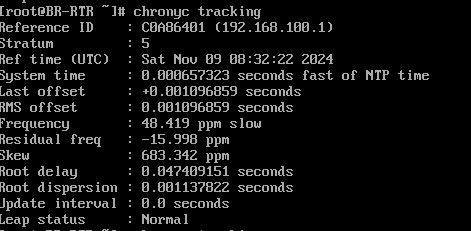




Перезагрузить службу



Проверить, что все синхронизируется:



**Решение модуля 2**

**ЗАДАНИЕ 1.** Настройте доменный контроллер Samba на машине BR-SRV.

* Создайте 5 пользователей для офиса HQ: имена пользователей формата user№.hq. создайте группу hq, введите в эту группу созданных пользователей.
* Введите в домен машину CLI.
* Пользователи группы hq имеют право аутентифицироваться на клиентском ПК.
* Пользователи группы hq должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id. Запускать другие команды с повышенными привилегиями пользователи группы не имеют права.
* Выполнять импорт пользователей из файла users.csv. файл будет располагаться на виртуальной машине BR-SRV в папке /opt.

Обновить пакеты на **BR-SRV** и установить пакет task-samba-dc для создания домена:





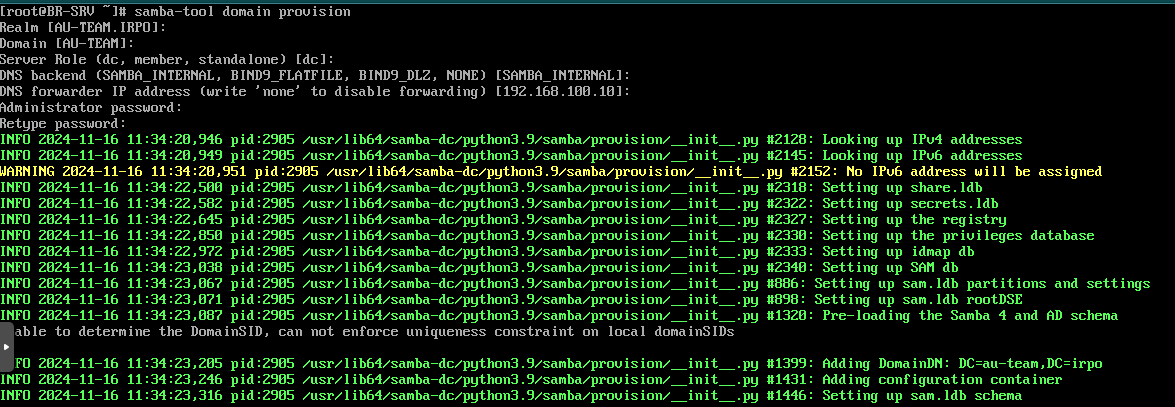
Удалить папки и файлы (там содержатся файлы с настроенным доменом, чтобы не произошло конфликтов избавляемся от них):



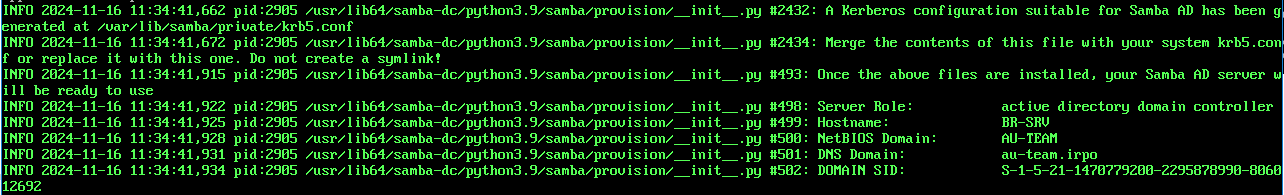
Создать новую директорию:



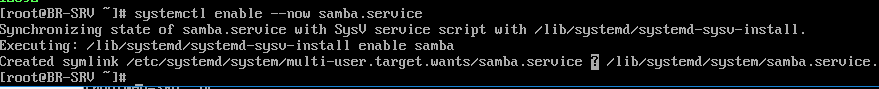
(пароль для администратора используем – P@ssw0rd)



Если все правильно, после загрузки видим приблизительно следующее:



Вносим в автозагрузку службу



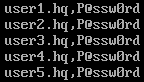


Переходим в директорию **/opt (cd /opt)**



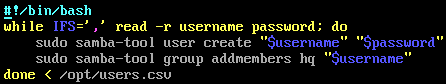






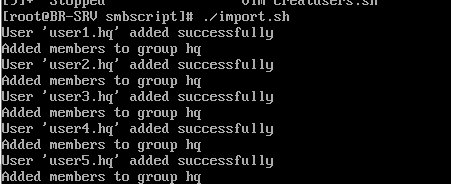






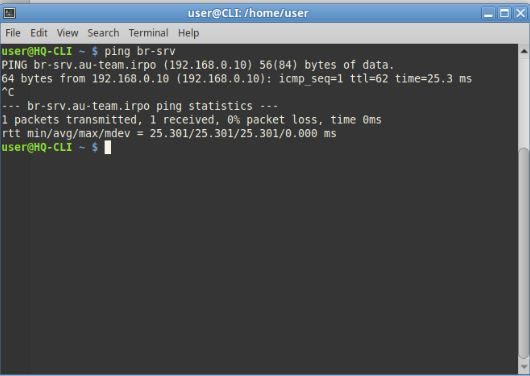






Переходим на ВМ HQ-CLI

Проверяем, что ВМ точно имеет возможность общаться как с dns-сервером, так и с ВМ на которой создан домен:

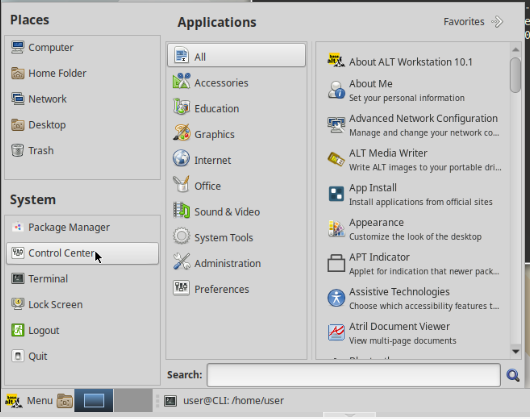


Кроме, того изменяет файл **/etc/resolv.conf**

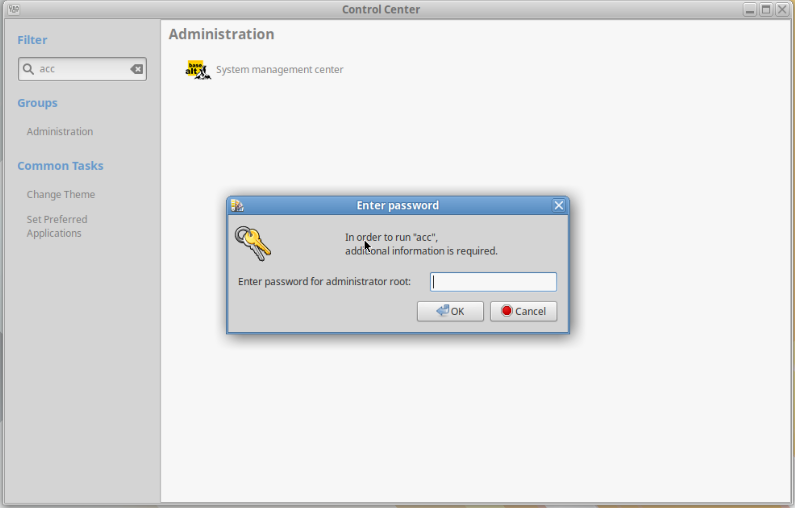
 - адрес BR-SRV

Подключение к домену:

Открываем центр управления

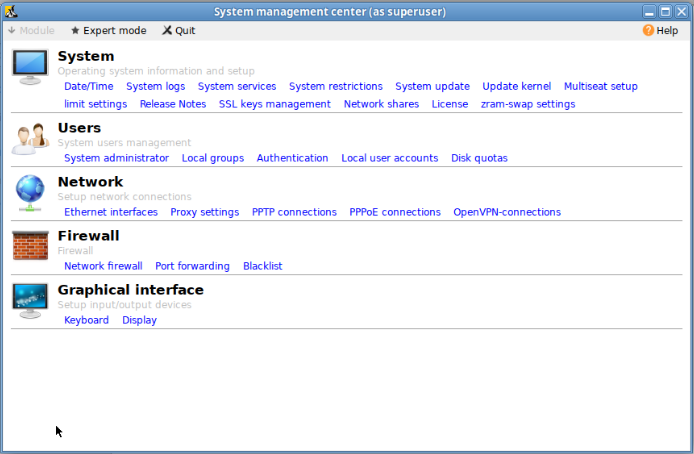


Выбираем центр управления системой или через поиск ищем acc:

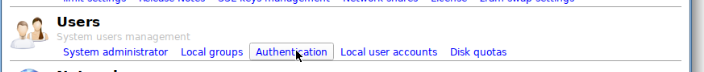


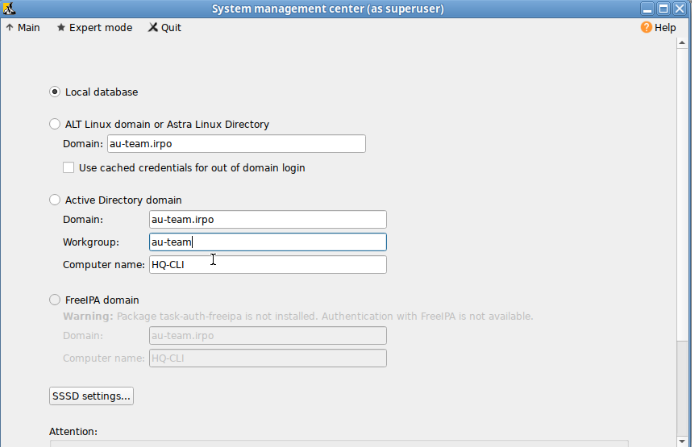
Вводим пароль системного администратора (**toor**)

Далее откроется такое окно:

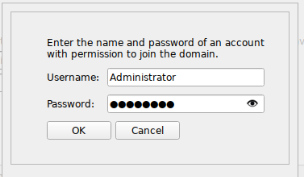


В разделе Users выбираем аутентификацию:

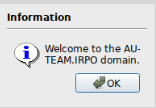


****

Листаем вниз и нажимает «**Apply**»

 - пароль **P@ssw0rd**

Если все правильно сработало, то должно появиться приветственное окно:

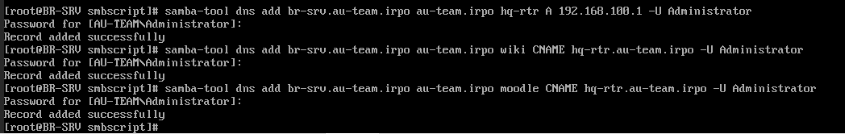


Делаем **reboot**, после заходим в терминал -

Проверяем, что работает домен на **CLI-HQ:**



Возвращаемся на ВМ **BR-SRV** (пароль **P@ssw0rd**)

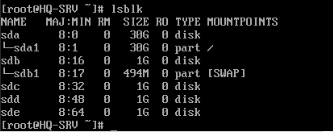


**ЗАДАНИЕ 2.** Сконфигурируйте файловое хранилище:

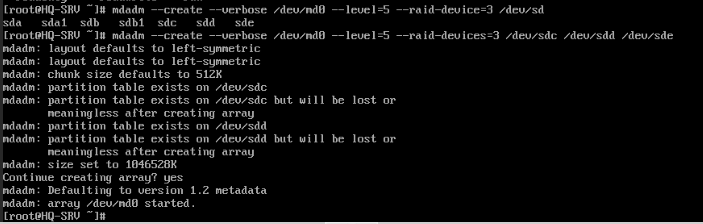
* При помощи трех дополнительных дисков, размером 1Гб каждый, на HQ-SRV сконфигурируйте дисковый массив уровня 5
* Имя устройства md0, конфигурация массива размещается в файле /etc/mdadm.conf
* Обеспечьте автоматическое монтирование в папку /raid5
* Создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4
* Настройте сервер сетевой файловой системы(nfs), в качестве папки общего доступа выберите /raid5/nfs, доступ для чтения и записи для всей сети в сторону HQ-CLI
* На HQ-CLI настройте автомонтирование в папке /mnt/nfs
* Основные параметры сервера отметьте в отчете.

Переходим на **HQ-SRV**

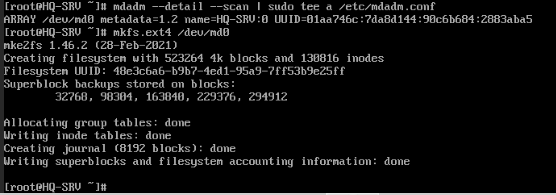
Проверяем наличие свободных дисков:



Создаем raid5 из свободных дисков:



Выводим информацию о созданном raid-массиве, далее в качестве файловой системы выставляем на созданный раздел - ext4:



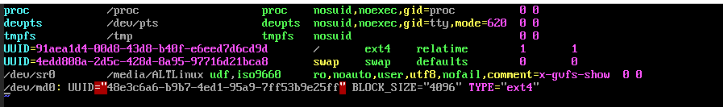
Создаем папку /raid5 для обеспечения дальнейшего автоматического монтирования:



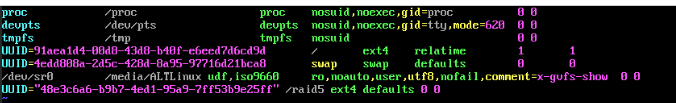
Настраиваем автоматическое монтирование раздела в директорию:



Файл ДО: (обращаем внимание на последнюю строку с ошибками, мы ее добавили предыдущей командой)



Изменяем данную строку до следующего вида:



Проверяем, что пространство монтируется:

 - недолжно быть никаких ошибок!

Настройте сервер сетевой файловой системы(nfs), в качестве папки общего доступа выбираем /raid5/nfs, доступ для чтения и записи для всей сети в сторону HQ-CLI:

Устанавливаем службу сервера



Создаем папу и настраиваем права:



 - адрес **CLI-HQ**

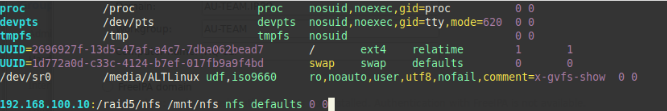


Переходим на клиента (**HQ-CLI**)

Создаем папку куда будет монтироваться директория с сервера:



Настраиваем автоматическое монтирование:

 - адрес **HQ-SRV**

Проверяем монтирование:

 - если ошибок нет, значит клиент смог подключиться к серверу

**ЗАДАНИЕ 3.** Выполнено см. выше в Модуле 1. Задание 11.

**ЗАДАНИЕ 4.** Сконфигурируйте ansible на сервере BR-SRV

* Сформируйте файл инвентаря, в инвентарь должны входить HQ-SRV, HQ-CLI, HQ-RTR и BR-RTR
* Рабочий каталог ansible должен располагаться в /etc/ansible
* Все указанные машины должны без предупреждений и ошибок отвечать pong на команду ping в ansible посланную с BR-SRV

Переходим на ВМ **BR-SRV**:

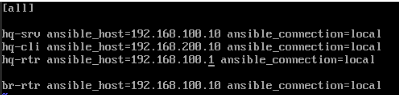
Устанавливаем службу Ansible



Создаем инвентаризационный файл hosts:



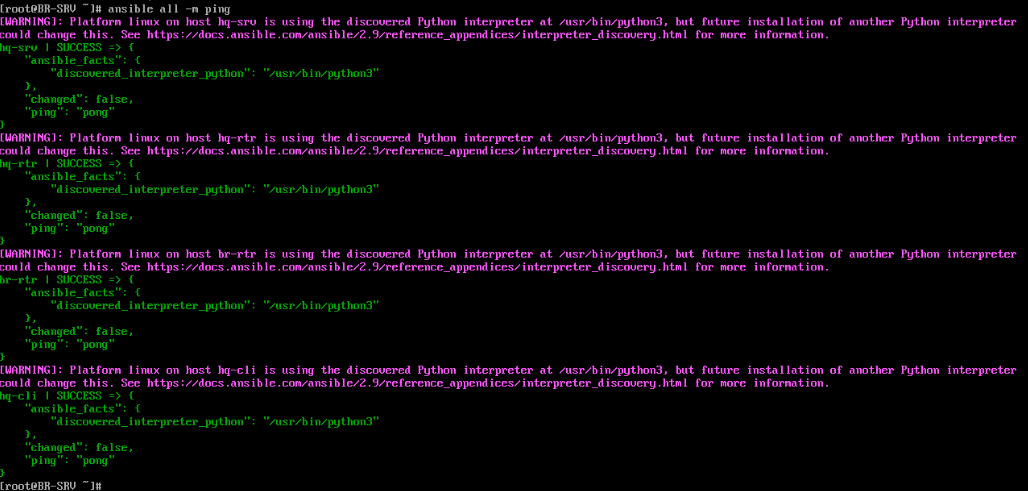
Вписываем данные о ВМ, требуемые в задании:



Проверяем работу:

При правильной работе – не будет ошибок, красного или оранжевого цвета

Команда: ansible all –m ping



**ЗАДАНИЕ 5.** Развертывание приложений в Docker на сервере BR-SRV.

* Создайте в домашней директории пользователя файл wiki.yml для приложения MediaWiki.
* Средствами docker compose должен создаваться стек контейнеров с приложением MediaWiki и базой данных.
* Используйте два сервиса.
* Основной контейнер MediaWiki должен назваться wiki и использоваться образ mediawiki.
* Файл LocalSettings.php с корректными настройками должен находится в домашней папке пользователя и автоматически монтироваться в образ.
* Контейнер с базой данных должен называться mariadb и использовать образ mariadb.
* Разверните.
* Он должен создавать базу с названием mediawiki, доступного по стандартному порту, пользователя wiki с паролем P@ssw0rd должен иметь права доступа к этой базе данных.
* MediaWiki должна быть доступна извне через порт 8080

См. Приложение 1.

**ЗАДАНИЕ 6.** На маршрутизаторах сконфигурируйте статическую трансляцию портов.

* Пробросьте порт 80 в порт 8080 на BR-SRV на маршрутизаторе BR-RTR, для обеспечения работы сервиса wiki.
* Пробросьте порт 2024 в порт 2024 на HQ-SRV на маршрутизаторе HQ-RTR.
* Пробросьте порт 2024 в порт 2024 на BR-SRV на маршрутизаторе HQ-RTR.

См. Приложение 2.

**ЗАДАНИЕ 7.**

См. приложение 3.

**ЗАДАНИЕ 8.**

См. приложение 4.

**ЗАДАНИЕ 9.**

* Установить бразер yandex