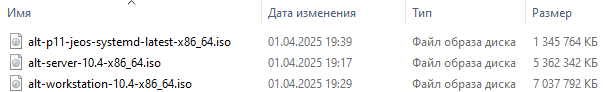
**ОТЧЕТ ПО ДЕМОЭКЗАМЕНУ**

**МОДУЛЬ 1**

**Установка.**

**Нужны эти образы и файлы**

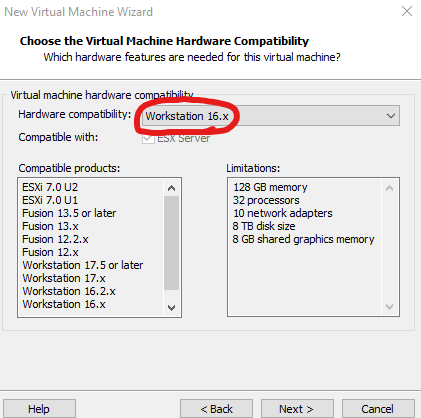
****

****

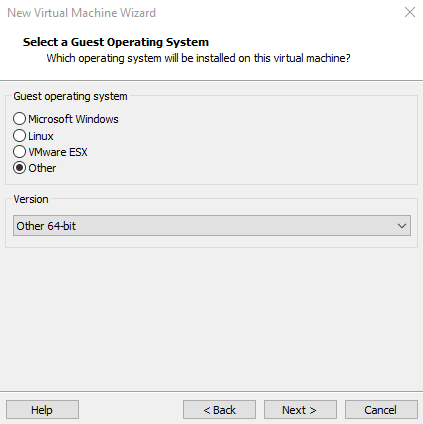
**Стенд (Экороутерам даем 4 Гб ОЗУ и 2 потока, потому что тупят):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Машина | RAM, ГБ | CPU | HDD/SDD, ГБ | OS |
| ISP | 1 | 1 | 30 | ОС Альт JeOS/Linux или аналог |
| HQ-RTR | 4 | 2 | 6 | ОС EcoRouter или аналог |
| BR-RTR | 4 | 2 | 6 | ОС EcoRouter или аналог |
| HQ-SRV | 2 | 1 | 30 | ОС Альт сервер или аналог |
| BR-SRV | 2 | 1 | 30 | ОС Альт сервер или аналог |
| HQ-CLI | 3 | 1 | 30 | ОС Альт Рабочая станция или аналог |
| Итого | 16 | 9 | 132 |  |

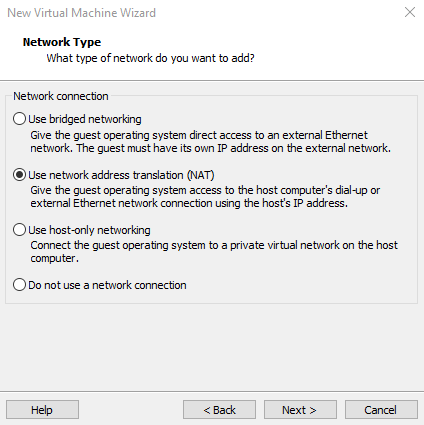
**Установка ALT Linux’ов. Ставим Workstation 16.x**

****

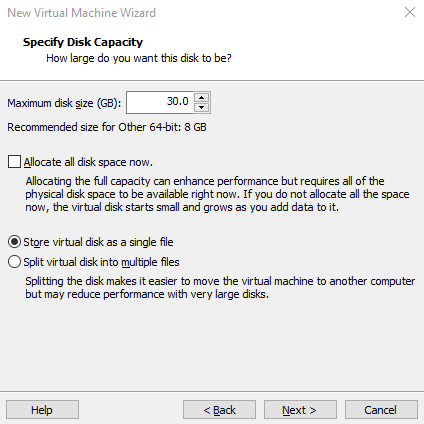
**Также ставим тип other, версию other 64-bit чтобы избежать ошибок.**

****

**В сетевых параметрах ставим bridge**

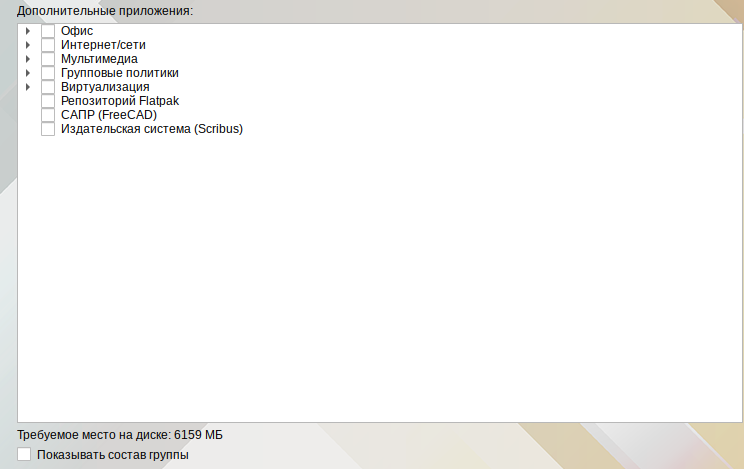
****

**При создании диска ставим 30 ГБ или не даст установить**

****

**На CLI (Workstation):**

**Важный момент при установке:**

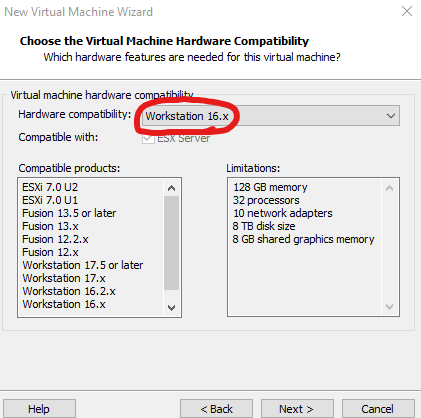
****

**На HQ-SRV/BR-SRV:**

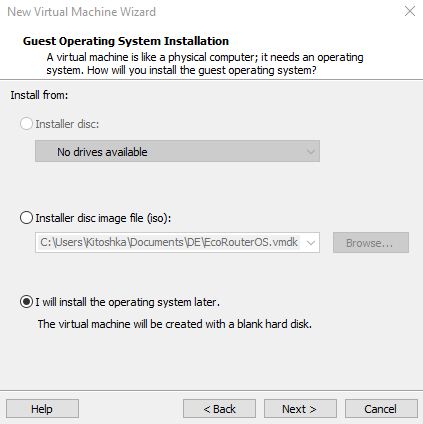
**Важный момент при установке. ВЫБИРАЕМ ТОЛЬКО NetworkManager, НЕ ВЫБИРАЕМ DHCP И DNS!:**

****

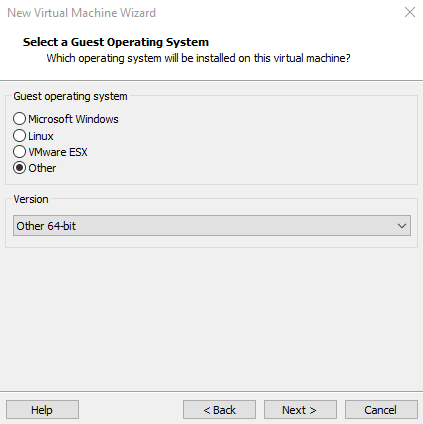
**Установка EcoRouter’ов. Ставим Workstation 16.x**

****

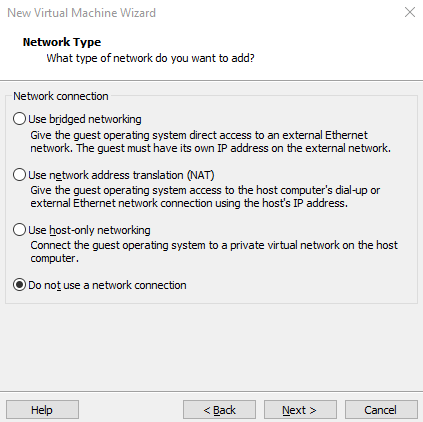
**Тут выбираем, что установим систему позже:**

****

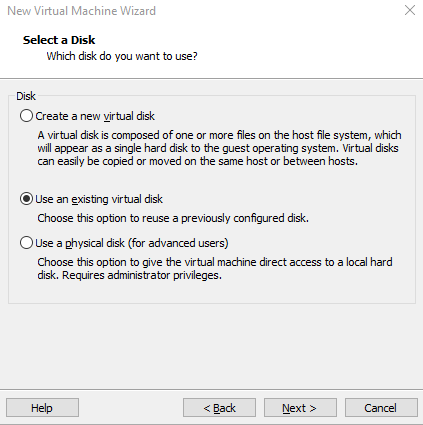
**Также ставим тип other, версию other 64-bit чтобы избежать ошибок.**

****

**В сетевых параметрах ничего ставим**

****

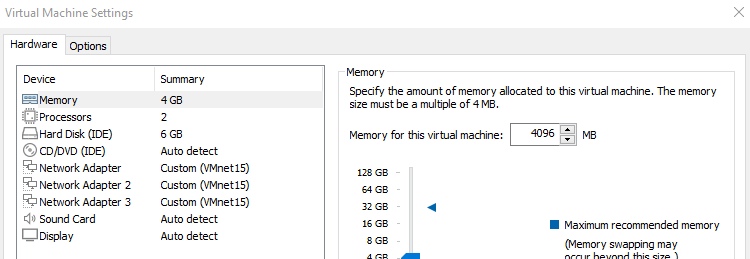
**При выборе диска ставим использовать существующий**

****

**В качестве диска выбираем наш .vmdk файл**

****

**После создания добавляем 3 адаптера и ставим какой-нибудь vmnet, который не используется**

****

**Преднастройки:**

**На CLI (Workstation):**

**Обновляем пакеты**

****

**Ставим Network Manager и nmtui**

****

**На ISP (JeOS):**

**Обновляем пакеты**

****

**Ставим mc, iptables, Network Manager, nmtui и bash-completion**

****

**Ставим Network Manager в автозапуск и запускаем**

****

**На HQ-SRV, BR-SRV:**

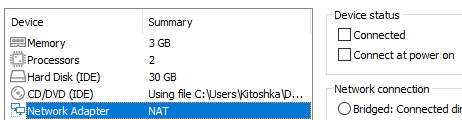
**Обновим пакеты:**

****

**Ставим nano и доустановим nmtui к NetworkManager (mc уже установлен):**

****

**После установки всех пакетов выключаем все NAT интерфейсы на всех машинах кроме ISP!!!**

****

**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**

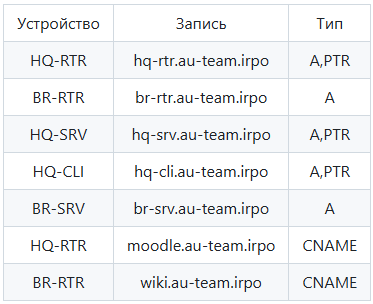
**Разбиение на подсети:**

|  |  |  |
| --- | --- | --- |
| Сеть | Адрес подсети | Пул адресов |
| SRV-Net (vlan 100) | 192.168.0.0/26 | 192.168.0.1-192.168.0.62 |
| CLI-Net (vlan 200) | 192.168.1.64/28 | 192.168.1.65-192.168.1.78 |
| BR-Net | 192.168.2.0/27 | 192.168.2.1-192.168.2.30 |
| MGMT (vlan 999) | 192.168.99.0/29 | 192.168.99.1-192.168.99.6 |
| ISP-HQ | 172.16.4.0/28 | 172.16.4.1-172.16.4.14 |
| ISP-BR | 172.16.5.0/28 | 172.16.5.1-172.16.5.14 |

**Таблица адресации:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | IPv4 | Интерфейс | NIC | Шлюз |
| ISP | NAT | Ens32 | Internet |  |
| 172.16.4.14/28 | Ens34 | ISP\_HQ | 172.16.4.1 |
| 172.16.5.14/28 | Ens35 | ISP\_BR | 172.16.5.1 |
| HQ-RTR | 172.16.4.1/28 | isp(ge0) | ISP\_HQ | 172.16.4.14 |
|  | 192.168.99.1/29 | vl999 |  |  |
|  | 192.168.0.62/26 | hqsrv(ge1) | SRV\_NET |  |
|  | 192.168.1.78/28 | hqcli(ge1) | HQ\_NET |  |
|  | 172.16.0.1/30 | GRE | TUN |  |
| HQ-SRV | 192.168.0.2/26 | ens34.100@ens34 | SRV\_NET | 192.168.0.62 |
| HQ-CLI | 192.168.1.65/28 (DHCP) | ens34.200@ens34 | CLI\_NET | 192.168.1.78 |
| BR-RTR | 172.16.5.1/28 | isp(ge0) | ISP\_BR | 172.16.5.14 |
| 192.168.2.1/27 | brsrv(ge1) | BR\_NET |  |
| 172.16.0.2/30 | GRE | TUN |  |
| BR-SRV | 192.168.2.2/27 | ens34 | BR\_NET | 192.168.2.1 |

**Таблица доменных имен**

****

**На HQ-CLI:**

****

**Настройка имени**

****

**На HQ-SRV:**

****

**Настройка имени**

****

**На HQ-RTR:**

****

**Настройка имени**

****

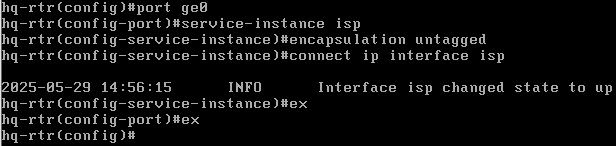
**Добавление маршрута по умолчанию**

****

**Настройка интерфейсов**

****

**Настройка портов**

****

****

**На BR-RTR:**

****

**Настройка имени**

****

**Добавление маршрута по умолчанию**

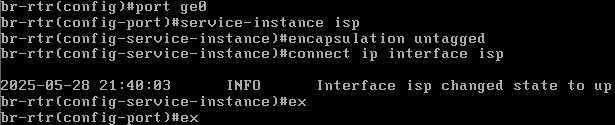
****

**Настройка интерфейсов**

****

****

**Настройка портов**

****

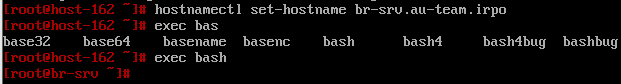
****

****

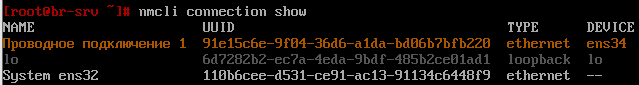
**На BR-SRV:**

****

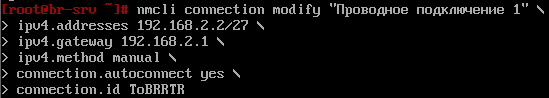
**Настройка имени**

****

**Смотрим имеющиеся подключения**

****

**Меняем подключение по заданию**

****

**На ISP:**

****

**Настройка имени**

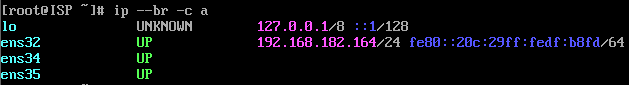
****

**2. Настройка ISP**

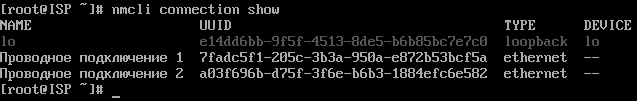
**● Настройте адресацию на интерфейсах:**

* **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**

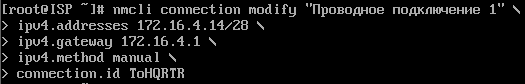
**Смотри интерфейсы**

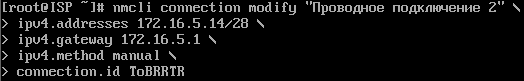
****

**Смотрим имеющиеся подключения**

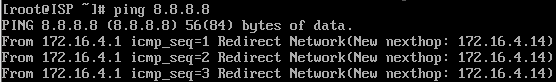
****

**Меняем подключения по заданию**

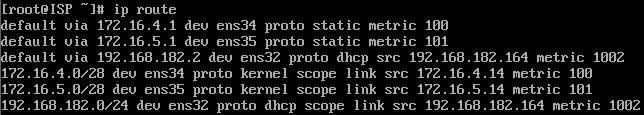
****

****

**После этого пробуем пингануть 8.8.8.8**

****

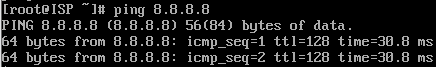
**Если не пингует, как на картинке выше, то пишем ip route и видим что-то наподобие этого:**

****

**Метрика маршрута в интернет выше (а значит менее приоритетная), чем метрика маршрутов к роутерам. Чтобы исправить это создаем новый маршрут с меньшей метрикой:**

****

**После этого пробуем пингануть, должно пинговаться:**

****

**Заходим в файл /etc/net/sysctl.conf**

****

**Изменяем строку net.ipv4.ip\_forward = 0 (пишем 1), сохраняем**



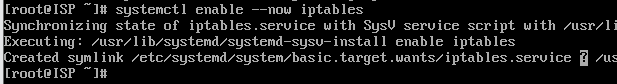
**Ставим iptables**

****

**Прописываем правила в сторону провайдера и сохраняем**

****

**Включаем iptables и добавляем в автозагрузку**

****

**3. 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.**

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

**На HQ-SRV:**

**Создание пользователя и задание пароля (P@ssw0rd)**

****

**Добавляем пользователя в группу Wheel**

****

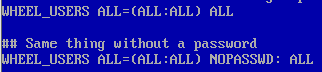
**Заходим в файл /etc/sudoers**

****

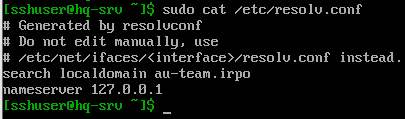
**Добавляем пользователя в этот файл**

****

**Раскоменчиваем следующие строки:**

****

**Проверка:**

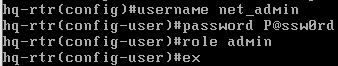
****

**На BR-SRV:**

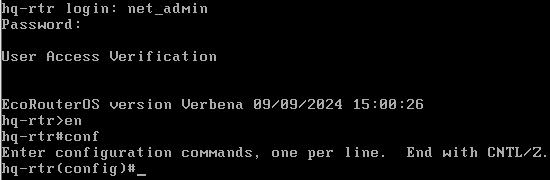
**Полностью те же настройки, что и HQ-SRV**

**На HQ-RTR:**

**Создание пользователя**

****

**Проверка:**

****

**На BR-RTR:**

**Полностью точно также как и на hq-rtr**

**4. Настройте на интерфейсе HQ-RTR в сторону офиса HQ виртуальный коммутатор:**

**● Сервер HQ-SRV должен находиться в ID VLAN 100**

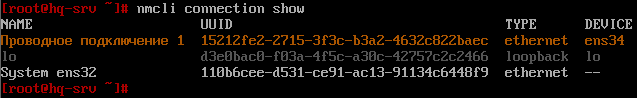
**● Клиент HQ-CLI в ID VLAN 200**

**● Создайте подсеть управления с ID VLAN 999**

**● Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт**

**На HQ-SRV:**

**Смотрим имеющиеся подключения, чтобы узнать название свободного интерфейса**

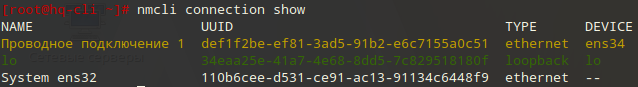
****

**Создаем VLAN-подключение**

****

**На HQ-CLI:**

**Также смотрим подключения**

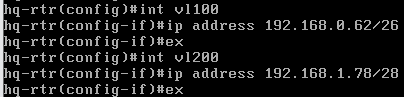
****

**Создаем VLAN-подключение**

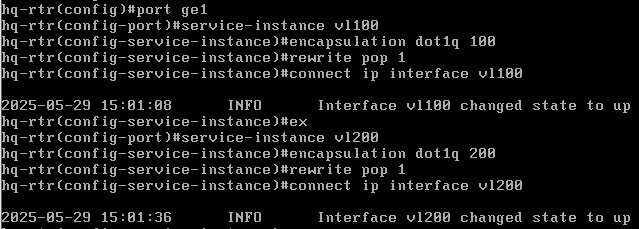
****

**На HQ-RTR:**

**Настройка интерфейсов**

****

**Настройка портов**

****

****

**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»**

**На HQ-SRV:**

**Заходим в файл /etc/openssh/sshd\_config**

****

**Приводим указанные строки в файле к следующим значениям, либо дописываем**

****

****

****

****

**В этом параметре вместо пробела используем Tab**

****

**Создаем файл bannermotd, который мы указали в конфигах**

****

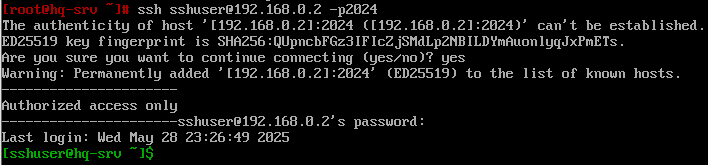
**И пишем это:**

****

**Перезагружаем службу**

****

**Проверка:**

****

**На BR-SRV:**

**Всё то же самое что и на hq-srv.**

**6. Между офисами HQ и BR необходимо сконфигурировать IP-туннель**

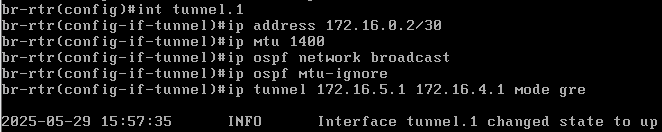
* **Сведения о туннеле занесите в отчёт**
* **На выбор технологии GRE или IP in IP**

**На HQ-RTR:**

****

**В связи с добавлением служебного заголовка появляются новые требования к допустимому значению MTU при передаче пакета. Заголовок GRE имеет размерность 4 байта, 20 байт транспортный IP заголовок, заголовок IP пакета 20 байт, таким образом возникает необходимость задавать размер допустимого MTU на интерфейсах туннеля меньше стандартного значения.**

**На BR-RTR:**

****

**7. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.**

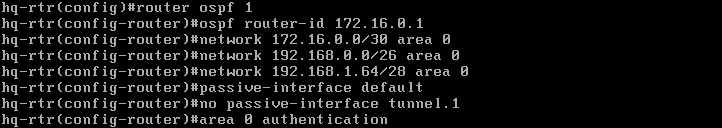
**● Разрешите выбранный протокол только на интерфейсах в ip туннеле**

**● Маршрутизаторы должны делиться маршрутами только друг с другом**

**● Обеспечьте защиту выбранного протокола посредством парольной защиты**

**● Сведения о настройке и защите протокола занесите в отчёт**

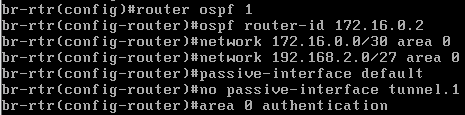
**На HQ-RTR:**

****

****

****

**На BR-RTR:**

****

****

****

**8. Настройка динамической трансляции адресов.**

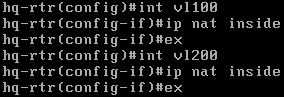
**● Настройте динамическую трансляцию адресов для обоих офисов.**

**● Все устройства в офисах должны иметь доступ к сети Интернет**

**На HQ-RTR:**

**Настройка интерфейсов:**

****

****

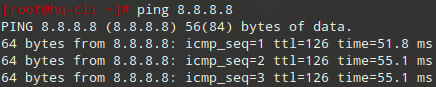
**Создаем пул:**

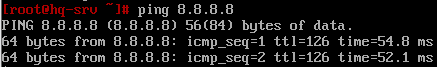
****

**Создаем правило трансляции адресов, указывая внешний интерфейс:**

****

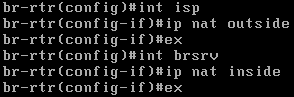
**Проверка:**

****

****

**На BR-RTR:**

**Настройка интерфейсов:**

****

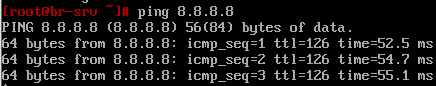
**Создаем пул:**

****

**Создаем правило трансляции адресов, указывая внешний интерфейс:**

****

**Проверка:**

****

**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**

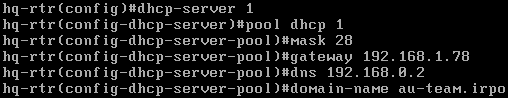
**● Сведения о настройке протокола занесите в отчёт**

**На HQ-RTR:**

**Создаем пул для DHCP-сервера:**

****

**Настраиваем сам DHCP-сервер:**

****

**Привязываем DHCP-сервер к интерфейсу (смотрящий в сторону HQ-CLI):**

****

****

**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**

**● В качестве DNS сервера пересылки используйте любой**

**общедоступный DNS сервер**

**На HQ-SRV:**

**Устанавливаем необходимые пакеты:**

****

**Заходим в папку /etc/bind**

****

**Открываем файл /etc/bind/options.conf**

****

**Изменяем содержание перечисленных строк в /etc/bind/options.conf к следующему виду:**

****

****

****

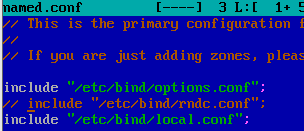
****

**Запускаем и ставим bind в автозагрузку**

****

**Открываем файл named.conf и комментим строку с rndc, чтобы не мешался**

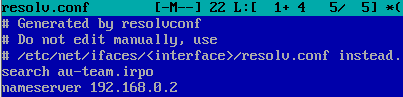
****

****

**Изменяем resolv.conf интерфейса:**

****

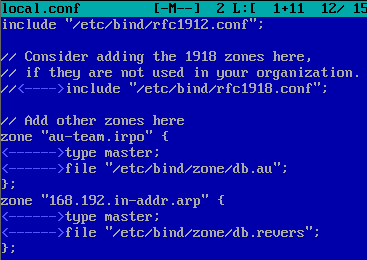
**Приводим его к нужному виду:**

****

**Создание и настройка зон. Заходим в файл local.conf**

****

**Прописываем прямую и обратную зоны**

****

**Заходим в /etc/bind/zone**

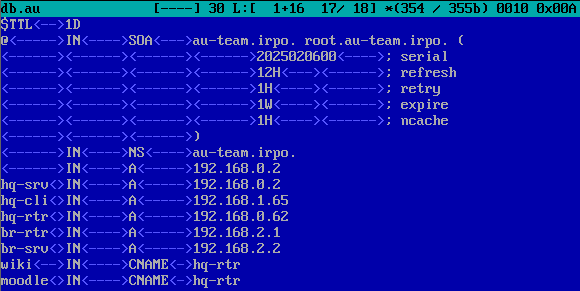
****

**Копируем шаблон прямой зоны:**

****

**Заходим в файл прямой зоны и приводим его к следующему виду:**

****

****

**Задаем пользователя на файл:**

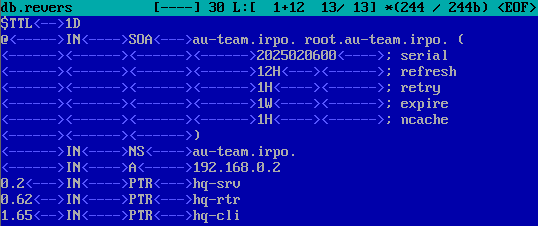
****

**Копируем шаблон обратной зоны:**

****

**Заходим в этот файл и приводим его к следующему виду:**

****

****

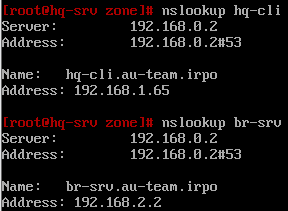
**Задаем пользователя на файл:**

****

**Перезапускаем bind**

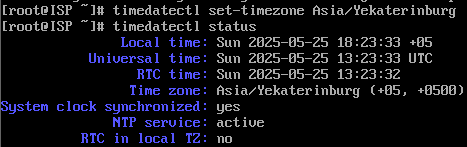
****

**Проверяем работоспособность**

****

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

**На ALT Linux-машинах:**

****

**На EcoRouter’ах:**

****