Задание:

# Модуль № 1:

Настройка сетевой инфраструктуры

# Вид аттестации/уровень ДЭ:

ПА, ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

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

* присвоение имен устройствам,
* расчет IP-адресации,
* настройку коммутации и маршрутизации.

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

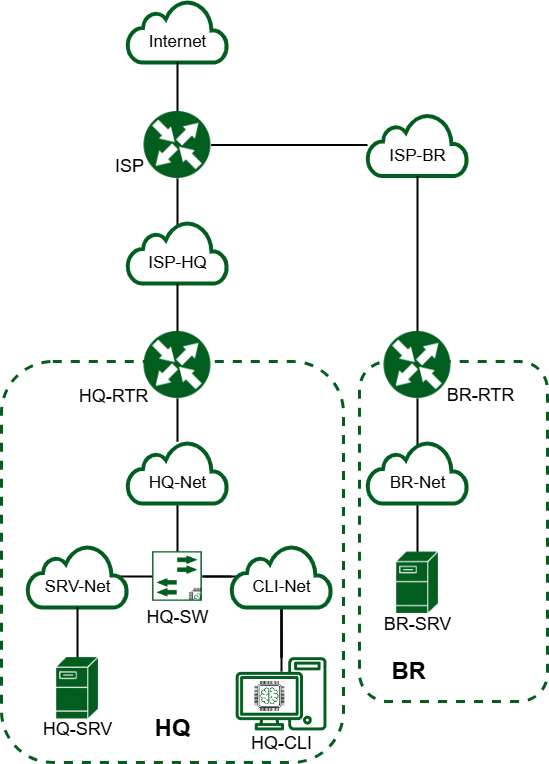


Рисунок 1. Топология сети

Таблица 1

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

1. Произведите базовую настройку устройств
   * Настройте имена устройств согласно топологии. Используйте полное доменное имя
   * 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
2. Настройка ISP
   * Настройте адресацию на интерфейсах:
     + Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP (вам настраивать не надо в данный момент)
     + 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
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
4. В данный момент ВЛАН не делаем, оставляем все в одном сегменте!!!!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
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»
6. Между офисами HQ и BR необходимо сконфигурировать ip туннель

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

1. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.
   * Разрешите выбранный протокол только на интерфейсах в ip туннеле
   * Маршрутизаторы должны делиться маршрутами только друг с другом
   * Обеспечьте защиту выбранного протокола посредством парольной защиты
   * Сведения о настройке и защите протокола занесите в отчёт
2. Настройка динамической трансляции адресов.
   * Настройте динамическую трансляцию адресов для обоих офисов.
   * Все устройства в офисах должны иметь доступ к сети Интернет
3. 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
4. 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
5. Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.

Таблица 2

|  |  |  |
| --- | --- | --- |
| **Устройство** | **Запись** | **Тип** |
| HQ-RTR | hq-rtr.au-team.irpo | A,PTR |
| BR-RTR | br-rtr.au-team.irpo | A |
| HQ-SRV | hq-srv.au-team.irpo | A,PTR |
| HQ-CLI | hq-cli.au-team.irpo | A,PTR |
| BR-SRV | br-srv.au-team.irpo | A |
| HQ-RTR | moodle.au-team.irpo | CNAME |
| HQ-RTR | wiki.au-team.irpo | CNAME |

Необходимые приложения:

Приложение А. Инструкция по настройке оборудования для проведения ДЭ (в отдельном файле).

Приложение Б. Пример заполнения таблицы адресов

Приложение Б Пример заполнения таблицы адресов

Пример адресов и интерфейсов на демоэкзамене!!! В вашем случае в данный момент нет вланов. Соответственно все вешаем с одной маской и в одну подсеть HQ

| **Имя устройства** | **Интерфейс** | **IP** | **Маска** | **Шлюз** |
| --- | --- | --- | --- | --- |
| ISP | enp0s3 | DHCP |  |  |
|  | enp0s8 | 172.16.5.1 | 255.255.255.240 |  |
|  | enp0s9 | 172.16.4.1 | 255.255.255.240 |  |
| HQ-RTR | enp0s3 | 172.16.4.2 | 255.255.255.240 | 172.16.4.1 |
|  | vlan100 | 192.168.0.1 | 255.255.255.192 |  |
|  | vlan200 | 192.168.0.65 | 255.255.255.240 |  |
|  | vlan99 | 192.168.0.81 | 255.255.255.248 |  |
| BR-RTR | enp0s3 | 172.16.5.2 | 255.255.255.240 | 172.16.5.1 |
|  | enp0s8 | 192.168.1.1 | 255.255.255.224 |  |
| HQ-SRV | vlan100 | 192.168.0.2 | 255.255.255.192 | 192.168.0.1 |
| HQ-CLI | vlan200 | DHCP | 255.255.255.240 | 192.168.0.65 |
| BR-SRV | enp0s3 | 192.168.1.2 | 255.255.255.224 | 192.168.1.1 |

# Модуль № 2:

Организация сетевого администрирования операционных систем

# Вид аттестации/уровень ДЭ:

ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Задание:

Необходимо разработать и настроить инфраструктуру информационно- коммуникационной системы согласно предложенной топологии (см. Рисунок 2).

Для модуля 2 используется отдельный стенд. В стенде преднастроены:

* IP-адреса, маски подсетей и шлюзы по умолчанию
* Сетевая трансляция адресов
* IP туннель
* Динамическая маршрутизация
* Созданы пользователи sshuser на серверах и net\_admin на маршрутизаторах
* DHCP-сервер
* DNS-сервер

Задание Модуля 2 содержит развёртывание доменной инфраструктуры, механизмов инвентаризации, внедрения и настройки ansible как инфраструктуры на основе открытых ключей, установку и настройку файловых служб и служб управления правами и службы сетевого времени, настройки веб серверов.

В ходе проектирования и настройки сетевой инфраструктуры следует вести отчеты (пять отчетов) о своих действиях, включая таблицы и схемы, предусмотренные в задании. Отчеты по окончании работы следует сохранить на диске рабочего места.

Задание Модуля 2.

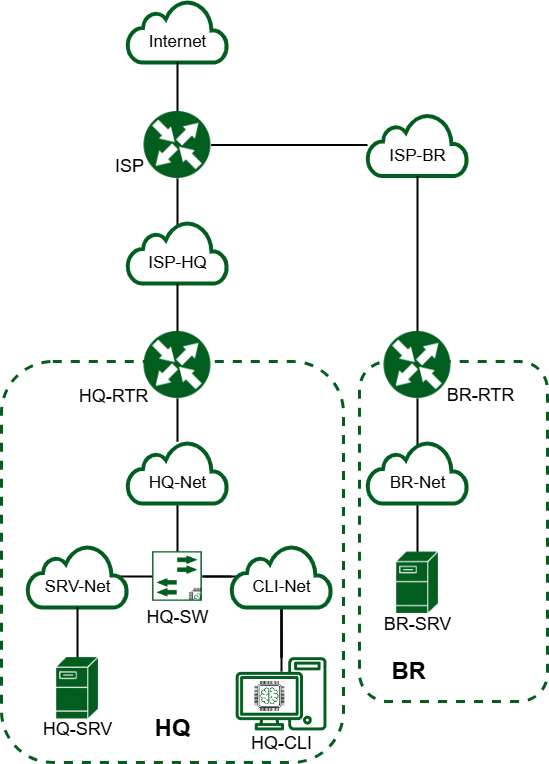


Рисунок 2. Топология сети

Таблица 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Машина** | **RAM,**  **ГБ** | **CPU** | **HDD/SDD, ГБ** | **OS** |
| ISP | 1 | 1 | 10 | ОС Альт JeOS/Linux или аналог |
| HQ-RTR | 1 | 1 | 10 | ОС EcoRouter или аналог |
| BR-RTR | 1 | 1 | 10 | ОС EcoRouter или аналог |
| HQ-SRV | 2 | 1 | 10 | ОС Альт Сервер/аналог |
| BR-SRV | 1 | 1 | 10 | ОС Альт Сервер/аналог |
| HQ-CLI | 3 | 2 | 15 | ОС Альт Рабочая Станция/аналог |
| Итого | 10 | 8 | 65 | - |

1. Самба настраивается после полной настройки DNS 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 HQ-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
   * Выполните импорт пользователей из файла users.csv. Файл будет располагаться на виртуальной машине BR-SRV в папке /opt
2. Сконфигурируйте файловое хранилище:
   * При помощи трёх 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 папку /mnt/nfs
  + Основные параметры сервера отметьте в отчёте

1. Настройте службу сетевого времени на базе сервиса chrony
   * 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
2. Пока пропускаем!!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

Все действия дальше делается на домашних ПК

1. 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 называться wiki и использовать образ mediawiki
   * Файл LocalSettings.php с корректными настройками должен находиться 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, доступную по стандартному порту, пользователя wiki с паролем WikiP@ssw0rd должен иметь права доступа к этой базе данных
   * MediaWiki должна быть доступна извне через порт 8080.
2. 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 BR-RTR
3. Запустите сервис moodle на сервере HQ-SRV:
   * Используйте веб-сервер apache
   * В качестве системы управления базами данных используйте mariadb
   * Создайте базу данных moodledb
   * Создайте пользователя moodle с паролем P@ssw0rd и предоставьте ему права доступа к этой базе данных
   * У пользователя admin в системе обучения задайте пароль P@ssw0rd
   * На главной странице должен отражаться номер рабочего места в виде арабской цифры, других подписей делать не надо
   * Основные параметры отметьте в отчёте
4. Настройте веб-сервер nginx как обратный прокси-сервер на HQ-RTR
   * При обращении к HQ-RTR по доменному имени moodle.au-team.irpo клиента должно перенаправлять на HQ-SRV на стандартный порт, на сервис moodle
   * При обращении к HQ-RTR по доменному имени wiki. au-team.irpo клиента должно перенаправлять на BR-SRV на порт, на сервис mediwiki
5. Удобным способом установите приложение Яндекс Браузере для организаций на HQ-CLI
   * Установку браузера отметьте в отчёте

Необходимые приложения:

Приложение А. Инструкция и список чекпойнтов по настройке оборудования для проведения ДЭ (в отдельном файле).

Приложение Б. Файл users.csv.