ВВЕДЕНИЕ

Знание сетевых технологий на сегодняшний день становится незаменимым для тех, кто хочет построить успешную карьеру в области ИТ. Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

Данное конкурсное задание разработано с учетом различных сетевых технологий, соответствующих уровням сертификации CCNA R\S Задание разбито на следующие секции:

- Базовая настройка
- Настройка коммутации
- Настройка подключений к глобальным сетям
- Настройка маршрутизации
- Настройка служб
- Настройка механизмов безопасности
- Настройка параметров мониторинга и резервного копирования
- Конфигурация виртуальных частных сетей

Все секции являются независимыми друг от друга, но вместе образуют достаточно сложную сетевую инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, может подразумеваться, что IPv6 маршрутизация должна работать поверх настроенной виртуальной частной сети, которая, в свою очередь, должна работать поверх IPv4 маршрутизации, которая, в свою очередь, должна работать поверх PPPoE и Multilink и т.д. Очень важно понимать, что если вам не удается решить какую-либо из задач по середине такого технологического стека, это не значит, что решенные задачи не будут оценены. Например, если вы не можете настроить динамическую маршрутизацию IPv4, которая необходима для работы виртуальной частной сети, вы можете использовать статическую маршрутизацию и продолжать работу над настройкой виртуальной частной сети и всем что должно работать поверх нее. В этом случае вы не получите баллы за динамическую маршрутизацию, но вы получите баллы за всё что должно работать поверх нее (в случае если функциональные тесты пройдены успешно).

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью и составить алгоритм выполнения работы. Вам предстоит вносить изменения в действующую, преднастроенную сетевую инфраструктуру предприятия, состоящую из головного офиса HQ и удаленного офиса BR1. Офисы имеют связь через провайдеров ISP1 и ISP2. Вы не имеете доступа к оборудованию провайдеров, оно полностью настроено и не требует дополнительного конфигурирования. Вам необходимо настраивать оборудование предприятия, а именно: SW1, SW2, SW3, HQ1, FW1 и BR1.

У вас отсутствует консольный доступ к устройствам, будьте очень внимательны при выполнении задания! В случае потери связи с оборудованием, вы будете виноваты сами. **Разрешается перезагрузка оборудования** – только техническими экспертами. Например, применили неправильный ACL, который закрыл доступ по telnet, но вы не успели сохранить конфигурацию.

Руководствуйтесь пословицей: **Семь раз отмерь, один раз отрежь**. Для выполнения задания у вас есть одна физическая машина (PC1 с доступом по Telnet и установленным ASDM), которую вы должны использовать в качестве:

PC2 Виртуальный ПК, Windows 10, Putty. Пользователь User пароль P@ssw0rd

SRV1 Виртуальный ПК, Debian пользователь root пароль toor, с предустановленными сервисами

1) SysLog папка для проверки /Cisco_Log
2) RADIUS - FreeRadius
3) SNMP – для проверки используется пакет Net-SNMP используйте команду snmp_test
4) NTP
5) TFTP папка для проверки /Cisco_TFTP

Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. Например, задание 3 в секции «Настройка служб» предписывает вам настроить службу протокола автоматической конфигурации хостов, которая, разумеется, не будет работать пока не будут выполнены необходимые настройки в секции «Конфигурация коммутации». На вас возлагается ответственность за распределение своего рабочего времени.

Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется **тщательно проверять** результаты своей работы.

Убедитесь в том, что ваши настройки на всех устройствах функционируют после перезагрузки всего оборудования.

ПОДКЛЮЧЕНИЕ К УСТРОЙСТВАМ

Для подключения к FW1 используете учетную запись с логином: **cisco** и паролем: **cisco**, для входа в привилегированный режим используйте пароль **cisco**. Для подключения к остальным сетевым устройствам используйте пароль: **cisco** и пароль для привилегированного режима: **cisco**

A. **Базовая настройка**

1) Задайте имя всех устройств в соответствии с топологией.
2) Назначьте для всех устройств доменное имя **worldskills.ru**
3) Создайте на всех устройствах пользователей **wsruser** с паролем **network**
    a) Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
    b) Пользователь должен обладать максимальным уровнем привилегий.
4) На всех устройствах установите пароль **wsr** на вход в привилегированный режим.
    a) Пароль должен храниться в конфигурации в виде результата хэш-функции.
5) Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде. На FW1 используйте шифрование AES.
6) Для всех устройств реализуйте модель AAA.
    a) Аутентификация на линиях виртуальных терминалов с 0 по 15 должна производиться с использованием локальной базы учётных записей. (кроме маршрутизатора HQ1)
    b) После успешной аутентификации при удаленном подключении пользователи сразу должен получать права, соответствующие их уровню привилегий или роли (кроме межсетевого экрана FW1).
    c) Настройте необходимость аутентификации на локальной консоли.
    d) При успешной аутентификации на локальной консоли пользователи должны сразу должен получать права, соответствующие их уровню привилегий или роли.
7) На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля, назначьте IP-адреса.
8) На маршрутизаторе HQ1 на виртуальных терминальных линиях с 0 по 15 настройте аутентификацию с использованием RADIUS-сервера.
    a) Используйте на линиях vty с 0 по 15 отдельный список методов с названием method_man
    b) Порядок аутентификации:
    c) Локальная
    d) RADIUS
    e) Используйте общий ключ cisco
    f) Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно
    g) Адрес RADIUS-сервера 172.16.20.20
    h) Настройте авторизацию при успешной аутентификации
    i) Проверьте аутентификацию по протоколу RADIUS при удаленном подключении к маршрутизатору HQ1, используя учетную запись **radius** с паролем **cisco**

9) Все устройства должны быть доступны для управления по протоколу SSH версии 2.

B. Настройка коммутации

1) Создайте таблицу VLAN:
   i) VLAN1000 с именем **MGT**.
   ii) VLAN1200 с именем **DATA**.
   iii) VLAN1300 с именем **OFFICE**.
   iv) VLAN1500 с именем **NATIVE**.
   v) VLAN1600 с именем **SHUTDOWN**.

2) Отключите протокол VTP явным образом
3) Между всеми коммутаторами настройте транки с использованием протокола IEEE 802.1q.
   a) Порты F0/10 коммутаторов SW2 и SW3, а также порт F0/1 коммутатора SW1 должны работать без использования согласования. Отключите протокол DTP явным образом.
   b) Транк между коммутаторами SW2 и SW3 должен быть настроен без использования согласования. Отключите протокол DTP явным образом.
   c) Транки между коммутаторами SW1 и SW2, а также между SW1 и SW3, должны быть согласованы по DTP, коммутатор SW1 должен инициировать создание транка, а коммутаторы SW2 и SW3 должны ожидать начала согласования параметров от соседа, но сами не инициировать согласование.
   d) Для всех магистральных каналов назначьте native vlan 500.
   e) Запретите пересылку по магистральным каналам все неиспользуемые VLAN, в том числе VLAN1
4) Настройте агрегирование каналов связи между коммутаторами.
   a) Номера портовых групп:

1 – между коммутаторами SW1 (F0/5-6) и SW2 (F0/5-6);
2 – между коммутаторами SW1 (F0/3-4) и SW3 (F0/3-4);

   b) Агрегированный канал между SW1 и SW2 должен быть организован с использованием протокола согласования LACP. SW1 должен быть настроен в активном режиме, SW2 в пассивном.
   c) Агрегированный канал между SW1 и SW3 должен быть организован с использованием протокола согласования PAgP. SW1 должен быть настроен в предпочтительном, SW3 в автоматическом.
5) Конфигурация протокола остовного дерева:
   a) Используйте протокол MST.
   b) Сконфигурируйте имя региона WSR39
   c) Сконфигурируйте 2 инстанса
      a. 1 - VLAN100, VLAN1200,VLAN1300
      b. 2 - VLAN 1500, VLAN 1600

d) В качестве корневого коммутатора для 1 инстанса сконфигурируйте SW1
e) В качестве корневого коммутатора для 2 инстанса сконфигурируйте SW2
f) Обеспечьте быстрое согласование магистральных каналов (Без ожидания MSTP)

6) Настройте порты F0/10 коммутаторов SW2 и SW3 в соответствии с L2 диаграммой.
7) Между HQ1 и FW1 настройте взаимодействие по протоколу IEEE 802.1Q.
8) На всех устройствах, отключите неиспользуемые порты.
9) На всех коммутаторах, неиспользуемые порты переведите во VLAN 1600.

C. Настройка подключений к глобальным сетям

1) Подключение FW1 к ISP1 и ISP2 осуществляется с помощью IPoE, настройте интерфейсы в соответствии с диаграммами L2 и L3.
   a) Передача данных между FW1 и ISP1 осуществляется не тегированным трафиком.
   b) Передача данных между FW1 и ISP2 осуществляется тегированным трафиком с использованием VLAN 901.
2) ISP3 предоставляет L2 VPN между офисами HQ и BR1.
   a) Настройте передачу между HQ1, FW1 и BR1 тегированного трафика.

   В зависимости от используемой модели межсетевого экрана, выберите один из двух следующих пунктов задания:

   Для ASA5505:

   b) Взаимодействие должно осуществляться по VLAN 10.

   Для ASA5506:

   b) Для обеспечения L2 связности между маршрутизатором BR1 и маршрутизатором HQ1, на межсетевом экране FW1 используйте Bridge group Virtual Interface (BVI) под номером 2. Для этого на межсетевом экране добавьте в BVI2, два подинтерфейса: с тегом 10 в сторону провайдера ISP3, с тегом 11 в сторону маршрутизатора HQ1. На маршрутизаторе HQ1 в сторону межсетевого экрана FW1, создайте соответствующий подинтерфейс.
3) Настройте подключение BR1 к провайдеру ISP1 с помощью протокола PPP.
   a) Настройте Multilink PPP с использованием двух Serial-интерфейсов.
   b) Используйте 1 номер интерфейса.
   c) Не используйте аутентификацию.
   d) BR1 должен автоматически получать адрес от ISP1.
4) Настройте подключение BR1 к провайдеру ISP2 с помощью протокола HDLC.

D. Настройка маршрутизации

ВАЖНО! При настройке протоколов динамической маршрутизации, будьте предельно внимательны и анонсируйте подсети в соответствии с диаграммой

маршрутизации, иначе не получите баллы за протокол, в котором отсутствует необходимая подсеть, и за тот протокол, в котором эта подсеть оказалась лишней.
Также, стоит учесть, что провайдеры фильтруют маршруты полученные по BGP, если они не соответствуют диаграмме маршрутизации.

1) В офисе HQ, на устройствах HQ1 и FW1 настройте протокол динамической маршрутизации OSPF.
   a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   b) HQ1 и FW1 между собой должны устанавливать соседство, только в сети 172.16.3.0/24.
   c) Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
2) Настройте протокол динамической маршрутизации OSPF в офисе BR1 с главным офисом HQ.
   a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   b) Используйте магистральную область для GRE туннелей.
   c) Соседства между офисами HQ и BR1 должны устанавливаться, как через канал L2 VPN, так и через защищенный туннель.
   d) Убедитесь в том, что при отказе выделенного L2 VPN, трафик между офисами будет передаваться через защищённый GRE туннель.
   e) Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
3) Настройте протокол BGP в офисах HQ и BR1 для взаимодействия с провайдерами ISP1 и ISP2.
   a) На устройствах настройте протокол динамической маршрутизации BGP в соответствии с таблицей 1

Таблица 1 – BGP AS

Устройство	AS
HQ1	65000
FW1	65000
ISP1	65001
ISP2	65002
BR1	65010

   b) Настройте автономные системы в соответствии с Routing-диаграммой.

c) Маршрутизаторы HQ1 и FW1 должны быть связаны с помощью iBGP. Используйте для этого соседства, интерфейсы, которые находятся в подсети 30.78.87.0/29.
d) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
e) Для офиса BR исключите из таблицы маршрутизации сеть 14.88.22.8

4) Настройте протокол динамической маршрутизации EIGRP поверх защищенного туннеля и выделенного канала L2 VPN между маршрутизаторами HQ1 и BR1.
a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
b) Используйте номер автономной системы 6000.

E. Настройка служб

1) В сетевой инфраструктуре сервером синхронизации времени является SRV1. Все остальные сетевые устройства должны использовать его в качестве сервера времени.
a) Передача данных между осуществляется без аутентификации.
b) Настройте временную зону с названием MSK, укажите разницу с UTC +3 часов.
2) Настройте динамическую трансляцию портов (PAT):
a) На маршрутизаторе HQ1 и BR1 настройте динамическую трансляцию портов (PAT) для сети 192.168.2.0/24 в соответствующие адреса петлевых интерфейсов.
b) Убедитесь в том, что для PC2 для выхода в интернет использует один из каналов до ISP1 или ISP2 от BR1, при недоступности обоих каналов, PC2 должен осуществлять выход в сеть интернет через каналы офиса HQ.
c) Убедитесь, в том, что есть все необходимые маршруты, иначе проверить корректность настроенной трансляции портов, будет невозможно.

3) Настройте протокол динамической конфигурации хостов со следующими характеристиками
a. На маршрутизаторе HQ1 для подсети OFFICE:
i) Адрес сети – 30.78.21.0/24.
ii) Адрес шлюза по умолчанию интерфейс роутера HQ1.
iii) Адрес NTP-сервера 172.16.20.20.
iv) Компьютер PC1 должен получать адрес 30.78.21.10.

4) В офисе BR1 используется аутентификация клиентов с помощью протокола L2TP. Для этого настройте сервер L2TP на BR1.
c) Аутентификация PC2 на сервере L2TP должна осуществляться по логину pc2user и паролю pc2pass.
d) PC2 должен получать ip адрес от L2TP сервера автоматически.

e) В качестве транспортного адреса используте адреса из подсети 192.168.2.0/24
f) В качестве туннельных адресов используйте подсеть 10.8.8.0/24

F. Настройка механизмов безопасности

1) На маршрутизаторе BR1 настройте пользователей с ограниченными правами.
   a) Создайте пользователей **user1** и **user2** с паролем **cisco**
   b) Назначьте пользователю **user1** уровень привилегий 5. Пользователь должен иметь возможность выполнять все команды пользовательского режима, а также выполнять перезагрузку, а также включать и отключать отладку с помощью команд **debug**.
   c) Создайте и назначьте view-контекст **sh_view** на пользователя **user2**
      i) Команду show cdp neighbor
      ii) Все команды show ip *
      i) Команду ping
      ii) Команду traceroute
   d) Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.
2) На порту F0/10 коммутатора SW2, включите и настройте Port Security со следующими параметрами:
   a) не более 2 адресов на интерфейсе
   b) адреса должны динамически определяться, и сохраняться в конфигурации.
   c) при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.

3) На порту f0/10 коммутатора SW2 реализуйте защиту от перехвата трафика между двумя узлами в одном широковещательном домене
4) На коммутаторе SW2 включите DHCP Snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных.
5) На коммутаторе SW2 включите динамическую проверку ARP-запросов в сети OFFICE.
6) На маршрутизаторе BR1 настройте расширенный список контроля доступа для подсети 192.168.2.0/24. Заблокируйте весь исходящий и входящий трафик от подсети 192.168.2.0/24 в интернет за исключением:
   a) Разрешите работу с DNS сервером 8.8.8.8.
   b) Разрешите исходящий TCP трафик по портам 80 и 443.
   c) Разрешите входящий трафик по TCP, только для тех соединений, если узел из подсети 192.168.2.0/24 инициирует это соединение.

G. Настройка параметров мониторинга и резервного копирования

1) На маршрутизаторе HQ1 и межсетевом экране FW1 настройте журналирование системных сообщений на сервер SRV1, включая информационные сообщения.
2) На маршрутизаторе HQ1 и межсетевом экране FW1 настройте возможность удаленного мониторинга по протоколу SNMP v3.
    a) Задайте местоположение устройств MSK, Russia
    b) Задайте контакт admin@wsr.ru
    c) Используйте имя группы WSR.
    d) Создайте профиль только для чтения с именем RO.
    e) Используйте для защиты SNMP шифрование AES128 и аутентификацию SHA1.
    f) Используйте имя пользователя: **snmpuser** и пароль: **snmppass**
    g) Для проверки вы можете использовать команду snmp_test на SRV1.
3) На маршрутизаторе HQ1 настройте резервное копирование конфигурации
    a) Резервная копия конфигурации должна сохраняться на сервер SRV1 по протоколу TFTP при каждом сохранении конфигурации в памяти устройства
    b) Для названия файла резервной копии используйте шаблон <hostname>-<time>.cfg

H. Конфигурация виртуальных частных сетей

1) Между HQ1 и BR1 настройте GRE туннель со следующими параметрами:
    a) Используйте в качестве VTI интерфейс Tunnel1
    b) Используйте адресацию в соответствии с L3-диаграммой
    c) Режим — GRE multipoint
    d) HQ1 является хабом
    e) Параметры NHRP сконфигурируйте по своему усмотрению
    f) Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.
    g) Обеспечьте работу туннеля с обеих сторон через провайдера ISP1

2) Защита туннеля должна обеспечиваться с помощью IPsec между BR1 и FW1.
    a) Обеспечьте шифрование только GRE трафика.
    b) Используйте аутентификацию по общему ключу.
    c) Параметры IPsec произвольные.

Конфигурация подсистемы телефонной связи

1) На маршрутизаторе HQ1 сконфигурируйте CME со следующими параметрами
    a) Зарегистрируйте программный телефон на PC1 с номером 104
    b) Зарегистрируйте программный телефон на PC2 с номером 107
    c) Обеспечьте возможность звонков с одного телефона на другой
    d) Произведите необходимые настройки BR1 для регистрации телефона на PC2 в HQ CME

Конфигурация служб удаленного доступа
В данном модуле настройка не предусмотрена

Конфигурация веб- и почтовых служб
В данном модуле настройка не предусмотрена

Конфигурация служб хранения данных
В данном модуле настройка не предусмотрена
Виртуализация
В данном модуле настройка не предусмотрена

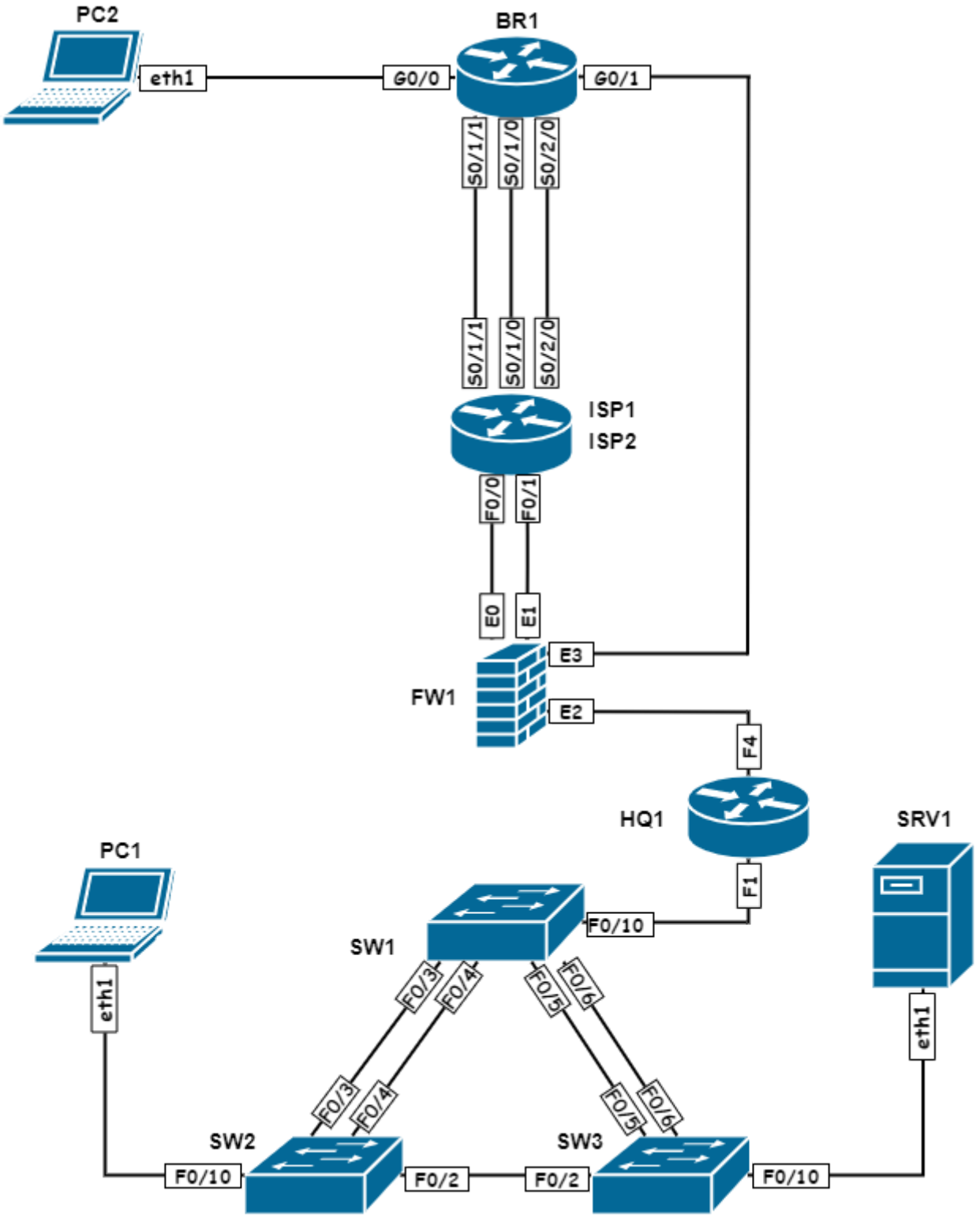
СУБД
В данном модуле настройка не предусмотрена

Конфигурация систем централизованного управления пользователями и компьютерами
В данном модуле настройка не предусмотрена

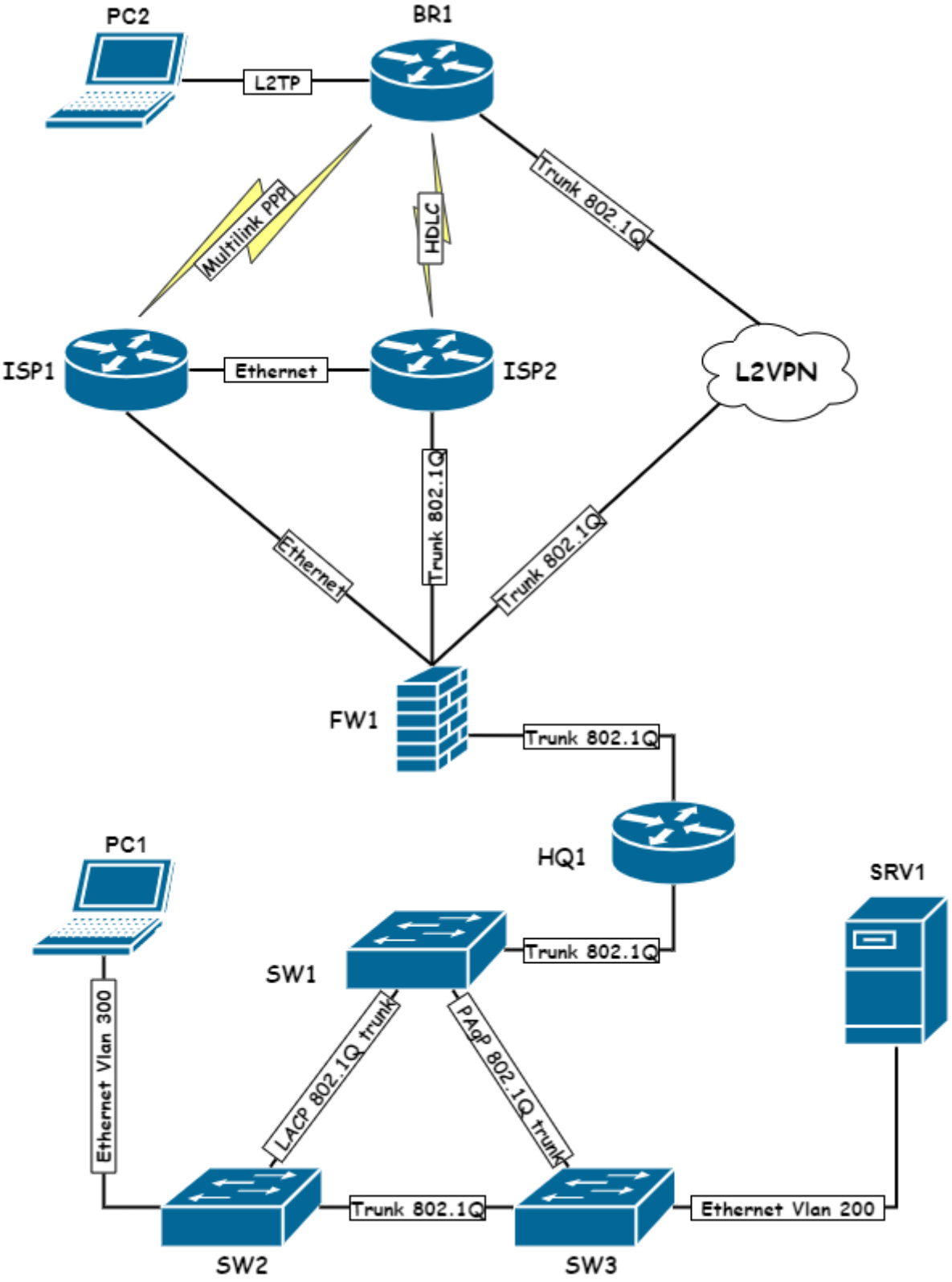
Автоматизация администрирования
В данном модуле настройка не предусмотрена

Конфигурация и установка системы
В данном модуле настройка не предусмотрена

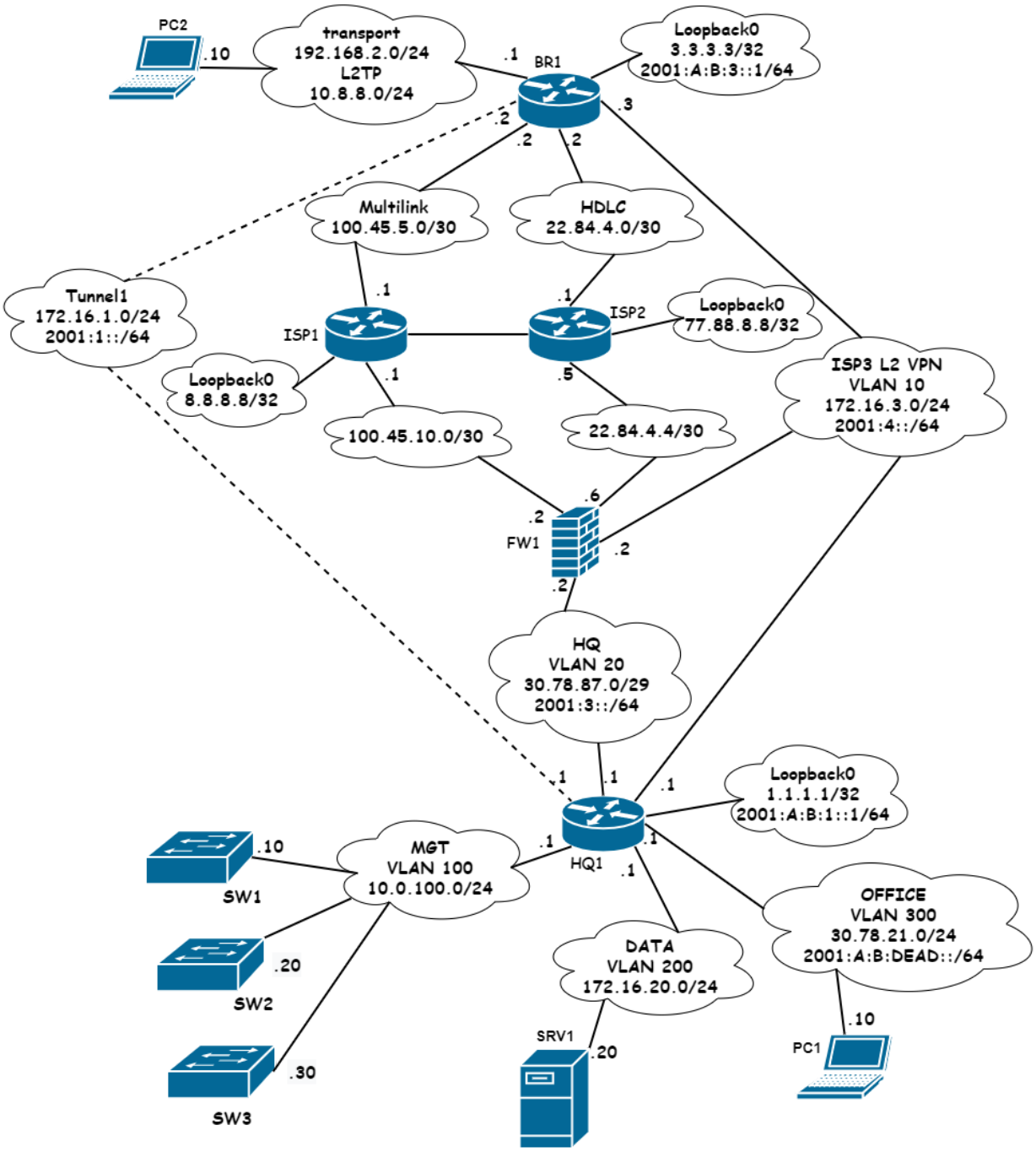
Топология L1



Топология L2



Топология L3



Routing-диаграмма