**КОМПЕТЕНЦИЯ**

**«СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»**

**КОНКУРСНОЕ ЗАДАНИЕ**

**МОДУЛЬ C:**

**ПУСКО-НАЛАДКА ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ**

**Разработано экспертами WSR:**

**Сертифицированным экспертом WSR:**

**Добрыниным С.И.**

**Дата: 29.06.18**

**Версия: 8.3**

## **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, CCNA Security, CCNP 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
* Конфигурация подсистемы телефонной связи

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 L2TP 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 перенастроенную сетевую инфраструктуру предприятия, состоящую из головного офиса HQ и двух удаленных офисов BR1 и BR2. Офисы имеют связь через двух 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, HQSW1, HQSW2, HQ1, ASA, BR1 и BR2. **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, 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, которую вы должны использовать в качестве PC1, PC2, PC3 и PC4, подключая ее к соответствующим устройствам согласно топологии L1.

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 первоначального подключения используйте протокол Telnet. Для подключения к ASA 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**

Для подключения к устройствам в главном офисе HQ, подключите рабочую станцию к порту f0/10 коммутатора SW2 и настройте адрес в соответствии с диаграммой L3, устройства доступны по следующим адресам:

SW1 – 172.16.10.10

SW2 – 172.16.10.20

HQSW1 – 172.16.10.1

HQSW2 – 172.16.10.2

HQ1 – 172.16.10.100

ASA – 172.16.10.200

Для подключения к устройствам в удаленном офисе BR1, подключите рабочую станцию в порт GigabitEthernet0 маршрутизатора BR1. BR1 доступен по адресу 192.168.1.1.

Для подключения к устройствам в удаленном офисе BR2, подключите рабочую станцию в порт GigabitEthernet0 маршрутизатора BR2. BR2 доступен по адресу 192.168.2.1.

## **ОЦЕНКА**

Для оценки выполненного задания используется автоматизированный метод. Проверочный модуль будет включен в порт F0/11 коммутатора SW2, поэтому следует убедиться, что он настроен корректно.

**Важно!** Убедитесь в возможности удаленного подключения с порта F0/11 ко ВСЕМ сетевым устройствам компании, в том числе к BR1 и BR2, если к каким-либо из устройств будет отсутствовать доступ, эти устройства оцениваться не будут.

**Базовая настройка**

1. Задайте имя всех устройств в соответствии с топологией
2. Назначьте для всех устройств доменное имя wsr2018.ru
3. Создайте на всех устройствах пользователя wsr2018 с паролем cisco.
   1. Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
   2. Пользователь должен обладать максимальным уровнем привилегий.
4. Для всех устройств реализуйте модель AAA.
   1. Аутентификация на удаленной консоли должна производиться с использованием локальной базы данных
   2. После успешной аутентификации при входе с удаленной консоли пользователь сразу должен попадать в режим с максимальным уровнем привилегий (кроме межсетевого экрана ASA).
   3. Настройте необходимость аутентификации на локальной консоли.
   4. При успешной аутентификации на локальной консоли пользователь должен попадать в режим с максимальным уровнем привилегий.
   5. На BR2 при успешной аутентификации на локальной консоли пользователь должен попадать в режим с минимальным уровнем привилегий
5. На маршрутизаторе HQ1 на всех виртуальных терминальных линиях настройте аутентификацию с использованием RADIUS-сервера.
6. Порядок аутентификации:
   * 1. По протоколу RADIUS
     2. Локальная
7. Используйте общий ключ “cisco”.
8. Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно
9. Адрес RADIUS-сервера 172.16.0.10
10. Настройте авторизацию при успешной аутентификации
11. Проверьте удаленное подключение к маршрутизатору HQ1 по протоколу RADIUS, используя учетную запись radius\cisco
12. На всех устройствах установите пароль wsr на вход в привилегированный режим.
    1. Пароль должен храниться в конфигурации НЕ в виде результата хэш-функции.
    2. На межсетевом экране ASA настройте вход в привилегированный режим по паролю пользователя (без запроса имени пользователя).
    3. Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.
13. Все устройства должны быть доступны для управления по протоколу SSH версии 2.

**Настройка коммутации**

1. Добавьте порт f0/0/21 коммутатора HQSW1 во VLAN 300.
2. Переведите порты f0/10 и f0/11 коммутатора SW2 из VLAN100 во VLAN300.
3. Для централизованного конфигурирования VLAN в коммутируемой сети предприятия используйте протокол VTP версии 3.
   1. В качестве сервера VTP настройте HQSW1.
   2. В качестве домена используйте wsr2018.ru
   3. Все остальные коммутаторы должны быть настроены в режим клиента.
   4. Таблица VLAN должна соответствовать:
4. VLAN100 с именем MGT.
5. VLAN200 с именем DATA.
6. VLAN300 с именем OFFICE.
7. VLAN400 с именем VOIP.
8. Между всеми коммутаторами настройте режим работы магистральных соединений по протоколу IEEE 802.1q.
9. Магистральные соединения между коммутатором HQSW1 и HQSW2, а также между SW1 и SW2 должно быть настроено без согласования. Явно отключите динамическое согласование магистральных соединений.
10. Магистральные соединения между коммутаторами HQSW1 и SW1, SW2, а также между HQSW2 и SW1, SW2 должны использовать протокол динамического согласования параметров, коммутаторы HQSW1 и HQSW2 должны инициировать создание магистрального канала, а коммутаторы SW1 и SW2 должны ожидать начала согласования параметров от соседа, но сами не инициируют согласование.
11. Настройте агрегирование каналов связи между коммутаторами.
12. Номера портовых групп:

1 – между коммутаторами HQSW1 (f0/0/6-7) и SW1 (f0/6-7);

2 – между коммутаторами HQSW2 (f0/0/6-7) и SW2 (f0/6-7);

3 – между коммутаторами HQSW1 (f0/0/1-2) и HQSW2 (f0/0/1-2);

1. Агрегированный канал между HQSW1 и SW1 должен быть организован с использованием протокола согласования LACP. HQSW1 должен быть настроен в активном режиме, SW1 в пассивном.
2. Агрегированный канал между HQSW2 и SW2 должен быть организован с использованием протокола согласования PAgP. HQSW2 должен быть настроен в предпочтительном, SW2 в автоматическом.
3. Агрегированный канал между HQSW1 и HQSW2 должен быть без использования протоколов согласования.
4. Конфигурация протокола остовного дерева:
5. Коммутатор HQSW1 должен являться корнем связующего дерева во всех VLAN, в случае отказа HQSW1, корнем должен стать коммутатор HQSW2.
6. Настройте используемые порты коммутаторов HQSW1 и HQSW2 так, чтобы во всех VLAN корнем связующего дерева могли стать только HQSW1 или HQSW2, а при получении BPDU пакета с лучшим приоритетом корня, порт должен перейти в состояние root-inconsistent.
7. Необходимо обеспечить не более двух экземпляров деревьев во всей сети с минимальными затратами системных ресурсов.
8. Настройте порт f0/0/21 коммутатора HQSW1, таким образом, что при включении он сразу переходил в состояние forwarding не дожидаясь пересчета остовного дерева. При получении BPDU пакета данный порт должен переходить в состояние error-disabled.
9. Настройте протокол IEEE 802.1AB таким образом, чтобы приём служебных сообщений был возможен на всех портах устройств HQSW1 и HQSW2, а передача только на портах между данными устройствами.

**Настройка подключений к глобальным сетям**

1. Настройте подключение PPPoE между ISP1 и маршрутизатором HQ1.
   * 1. Настройте PPPoE клиент на HQ1.
     2. Используйте имя пользователя cisco и пароль cisco.
     3. Устройства походят одностороннюю аутентификацию по протоколу CHAP по паролю PPPoE, только ISP1 проверяет имя пользователя и пароль.
     4. HQ1 должен автоматически получать адрес от ISP1.
2. Провайдер ISP1 использует протокол L2TP для подключения офиса BR1.
3. Настройте BR1 в качестве L2TP клиента.
   * 1. Используйте адрес 10.1.1.1 в качестве сервера L2TP.
     2. Настройте VirtualPPP с номером 100.
     3. BR1 должен автоматически получать адрес от ISP1.
     4. MTU 1450
4. Настройте подключение HQ1 к ISP2 с помощью Frame Relay.
   * 1. Frame Relay с фирменным инкапсулирующим заголовком Cisco.
     2. Используйте DLCI 102.
5. Настройте подключение BR2 к провайдеру ISP2 с помощью протокола PPP.
   * 1. Настройте протокол Multilink PPP.
     2. Для аутентификации используйте протокол, в котором пароль не передается в открытом виде. Имя пользователя PPPASA и паролю PPP
     3. BR2 должен автоматически получать адрес от ISP2.
6. Для подключения BR2 к провайдеру ISP1 настройте GRE туннель. Используйте туннельный интерфейс с номером 10. В качестве транспорта используйте адреса в соответствии с диаграммой L3.
7. ASA подключена к провайдеру ISP1 и ISP2 с помощью IPoE и имеет статический адрес.

**Настройка маршрутизации**

1. В офисе HQ, на устройствах HQSW1, HQSW2, HQ1 и ASA настройте протокол динамической маршрутизации OSPF.
   1. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   2. Используйте зону с номером 0
   3. HQSW1 и HQSW2 должны входить в состояние смежности между собой, только в сети 172.16.0.0/30.
   4. В сети DMVPN маршрутизатор HQ1 должен исполнять роль DR .
   5. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
2. Настройте протокол динамической маршрутизации OSPF в офисах BR1 и BR2 с главным офисом HQ.
   1. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   2. Соседства между офисами (HQ, BR1 и BR2) должны устанавливаться через защищенную DMVPN сеть.
   3. В офисе BR1 используйте зону с номером 1.
   4. В офисе BR2 используйте зону с номером 2.
   5. На HQ1 настройте передачу маршрутов в офисы BR1 и BR2, только к подсетям 172.16.0.8/30 и 192.168.3.0/24.
   6. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
3. ISP1 предоставляет подсеть PA (Provider Aggregatable) адресов (11.11.11.11/32) для офиса BR1. На маршрутизаторе BR1 настройте протокол динамической маршрутизации EIGRP с номером автономной системы 2018.
   1. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   2. Используйте алгоритм аутентификации key-chain с ключом WSR.
   3. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
   4. Провайдер ISP1 выполняет редистрибуцию маршрута 11.11.11.11/32 в сеть BGP, убедитесь в том, что вы корректно анонсируете данный маршрут провайдеру.
4. Офисы HQ и BR2 имеют подсети PI (Provider Independent) адресов и автономную систему 65000 и 65020 соответственно. На маршрутизаторах настройте протокол динамической маршрутизации BGP в соответствии с таблицей

|  |  |
| --- | --- |
| Устройство | AS |
| HQ1 | 65000 |
| ASA | 65000 |
| ISP1 | 65001 |
| ISP2 | 65002 |
| BR2 | 65020 |

* 1. Настройте автономные системы в соответствии с Routing-диаграммой.
  2. Маршрутизатор HQ1 и ASA должны быть связаны с помощью iBGP.
  3. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
  4. На HQ1 и ASA настройте редистрибуцию маршрутов к сетям 10.10.10.10/32, 20.20.20.20/32 и 30.30.30.0/27 из OSPF в BGP, а также редистрибуцию маршрута по умолчанию из BGP в OSPF.
  5. BR2 не должен получать все BGP маршруты, а только маршрут по умолчанию от ISP1 и ISP2.
  6. Настройте распределение исходящего трафика BR2, таким образом, чтоб приоритетом использовался канал через ISP1.
  7. Настройте распределение входящего трафика на BR2, таким образом, чтоб приоритетом использовался канал через ISP1.

1. Настройте прокол динамической маршрутизации OSPFv3 поверх сети DMVPN. На маршрутизаторах HQ1, BR2, BR3 и на коммутаторах HQSW1, HQSW2 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.
   1. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   2. Маршрутизатор HQ1 должен исполнять роль DR в сети DMVPN.
   3. Используйте зону с номером 0.

**Настройка служб**

1. В сетевой инфраструктуре сервером синхронизации времени является SRV1. Настройте в качестве клиента HQ1. Все остальные сетевые устройства должны использовать в качестве сервера времени HQ1.
   1. Настройте временную зону с названием YEKT, укажите разницу с UTC +5 часа.
   2. Настройте сервер синхронизации времени. Используйте стратум 2.
   3. Используйте аутентификацию MD5 с ключом WSR
2. На маршрутизаторах HQ1 настройте динамическую трансляцию портов (PAT) для сети OFFICE в адрес петлевого интерфейса 1.1.1.1.
3. На коммутаторе HQSW1 и HQSW2 настройте службу отказоустойчивости внутреннего шлюза
4. Настройте VRRP группу для подсети OFFICE
5. Номер группы — 20
6. В качестве виртуального ip-адреса используйте адрес 192.168.3.254
7. Настройте приоритет 100 для маршрутизатора HQSW1, для HQSW2 — 110.
8. Настройте аутентификацию по паролю vrrp
9. Настройте протокол динамической конфигурации хостов со следующими характеристиками
10. На маршрутизаторе HQ1 для подсети OFFICE:
11. адрес сети – 192.168.3.0/24
12. адрес шлюза по умолчанию — виртуальный ip-адрес настроенной VRRP группы
13. адрес TFTP-сервера 172.16.0.10
14. На коммутаторах HQSW1 и HQSW2 настройте DHCP-relay.
15. На маршрутизаторе HQ1 настройте удостоверяющий центр
16. Задайте включение FQDN маршрутизатора HQ1 в выдаваемые сертификаты
17. Используйте автоматическую выдачу сертификатов
18. На маршрутизаторах BR1 и BR2 и межсетевом экране ASA сделайте запрос цифрового сертификата у маршрутизатора HQ1. Не используйте проверку сертификатов на отзыв

**Настройка механизмов безопасности**

1. На маршрутизаторе BR2 настройте пользователей с ограниченными правами.
   1. Создайте пользователей user1 и user2 с паролем cisco.
   2. Пользователь user1 должен иметь возможность выполнять все команды пользовательского режима, а также выполнять перезагрузку и удалять начальную конфигурацию.
   3. Создайте и назначьте view-контекст “sh\_view” на пользователя
2. Команду show version
3. Все команды show ip \*
4. Команду who
   1. Создайте view-контекст “ping\_view”. Включите в него
5. Команду ping
6. Команду traceroute
   1. Создайте superview-контекст, объединяющий эти 2 контекста. При входе на маршрутизатор пользователь user2 должен попадать в данный контекст
   2. Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.
7. На порту f0/10 коммутатора SW1, включите и настройте Port Security со следующими параметрами:
8. не более 2 адресов на интерфейсе
9. адреса должны быть динамически сохранены в текущей конфигурации
10. при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.
11. На коммутаторе SW1 включите DHCP-snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных
12. На коммутаторе SW1 включите динамическую проверку ARP-запросов в сети OFFICE. Создайте лист контроля доступа, разрешающий статический IP-адрес 192.168.3.10.
13. На маршрутизаторе BR2 настройте брандмауэр зональной политики (ZBF).
    1. Настройте зоны:
       1. Зона с именем ISP1 для интерфейса G0'0/0.
       2. Зона с именем ISP2 для интерфейса Multilink 1.
       3. Зона с именем LOCAL для интерфейса G0.
       4. Зона с именем DMVPN для интерфейса Tunnel1.
    2. Используйте подсеть 192.168.2.0/24 для зоны LOCAL.
    3. Между зонами ISP1 и ISP2 запретите пересылку трафика.
    4. Из зоны LOCAL в зоны ISP1 и ISP2 разрешите работу следующих сервисов: HTTPS, SSH, DNS. В обратную сторону разрешите SSH.
    5. Из зоны LOCAL в зону DMVPN разрешите работу следующих сервисов: HTTPS, FTP, TELNET, SSH, DNS, ICMP. В обратную сторону разрешите SSH и ICMP.
    6. Средствами ZBF на маршрутизаторе BR2 обеспечьте работу следующих сервисов: NTP, SNMP, BGP, DMVPN, OSPF, OSPFv3. Весь остальной трафик должен блокироваться.

**Настройка параметров мониторинга и резервного копирования**

1. На маршрутизаторе HQ1 и межсетевом экране ASA настройте журналирование системных сообщений на сервер SRV1, включая информационные сообщения.
2. На маршрутизаторе HQ1 и межсетевом экране ASA настройте возможность удаленного мониторинга по протоколу SNMP v3.
   1. Задайте местоположение устройств YEKT, Russia
   2. Задайте контакт [admin@wsr.ru](mailto:admin@hitech.ru)
   3. Используйте имя группы WSR.
   4. Создайте профиль только для чтения с именем RO.
   5. Используйте режим, который обеспечивает максимальный уровень безопасности.
   6. Используйте имя пользователя: snmpuser и пароль: snmppass
3. На маршрутизаторе HQ1 настройте резервное копирование конфигурации
   1. Резервная копия конфигурации должна сохраняться на сервер SRV1 по протоколу TFTP при каждом сохранении конфигурации в памяти устройства
   2. Для названия файла резервной копии используйте шаблон <hostname>-<time>.cfg

**Конфигурация виртуальных частных сетей**

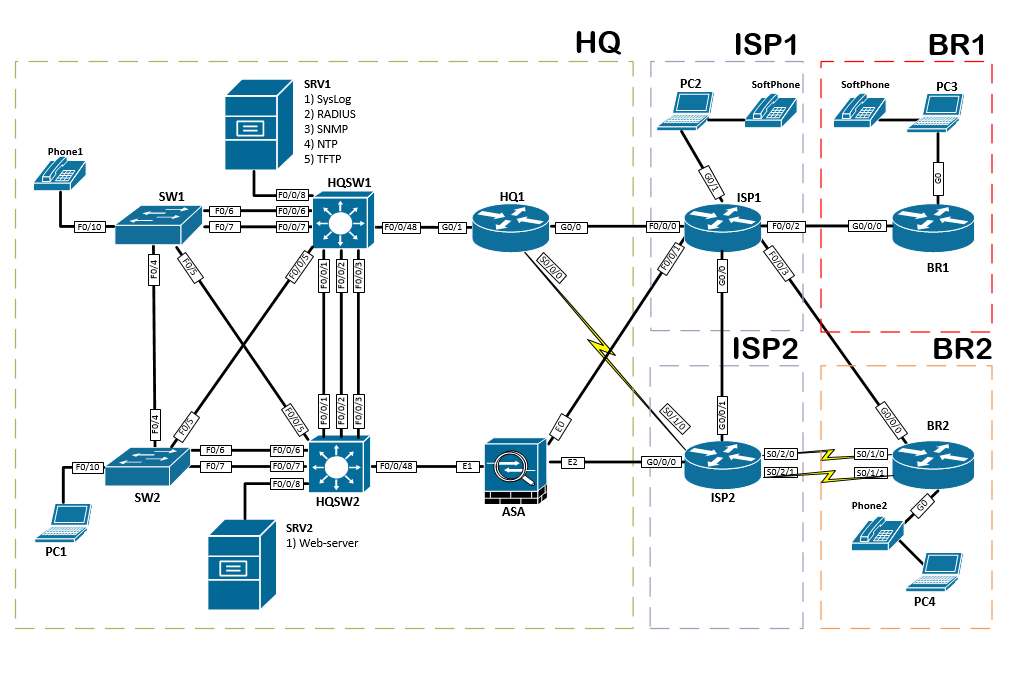
1. На маршрутизаторах HQ1, BR1 и BR2 настройте DMVPN:
2. Используйте в качестве VTI интерфейс Tunnel1
3. На каждом интерфейсе установите значение MTU равное 1400
4. Используйте адресацию в соответствии с VPN-диаграммой
5. Режим — GRE Multipoint
6. Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.
7. Настройки NHRP:
8. Идентификатор сети — 100
9. Пароль для аутентификации NHRP – WSR2018
10. В качестве DMVPN-хаба и NHS-сервера используйте маршрутизатор HQ1.
11. Защита туннелей DMVPN должна обеспечиваться с помощью IPsec.
12. Параметры политики первой фазы:
13. Проверка целостности – SHA-384
14. Шифрование – AES-192
15. Группа Диффи-Хэлмана – 5
16. Используйте аутентификацию по цифровому сертификату.
17. Используйте сертификаты, полученные от удостоверяющего центра HQ1.
18. Обеспечьте работу IKEv2
19. Параметры преобразования трафика для второй фазы:
20. Протокол – ESP
21. Шифрование – AES
22. Проверка целостности – MD5
23. На межсетевом экране ASA настройте возможность подключения удаленных клиентов с помощью SSL-VPN
24. Создайте на ASA локального пользователя vpnuser с паролем cisco
25. Клиенты должны подключаться с помощью клиента AnyConnect, образ которого находится во флеш-памяти межсетевого экрана ASA.
26. Подключение должно происходить по адресу 40.15.5.2.
27. Подключение проверять с PC2.

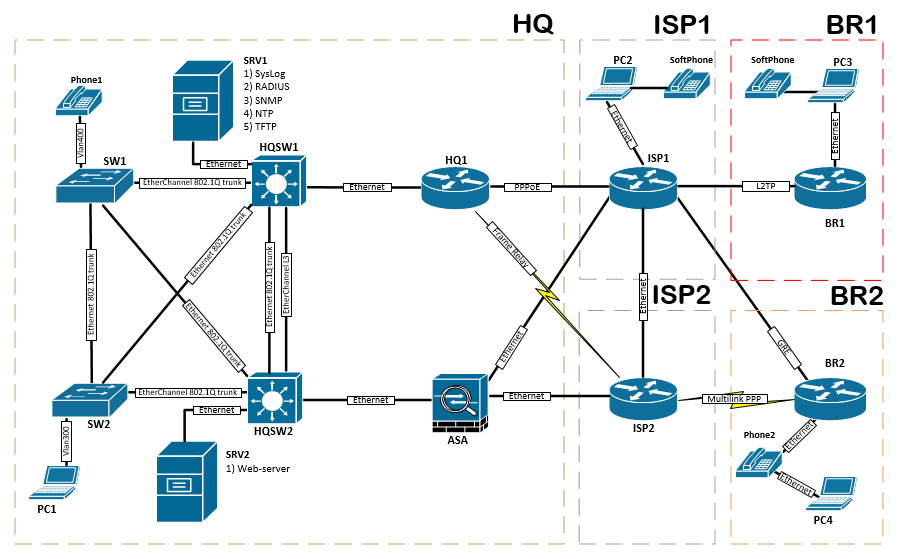
**Конфигурация подсистемы телефонной связи**

На маршрутизаторах HQ1 и BR2 настройте Call Manager Express по протоколу SIP со следующими параметрами:

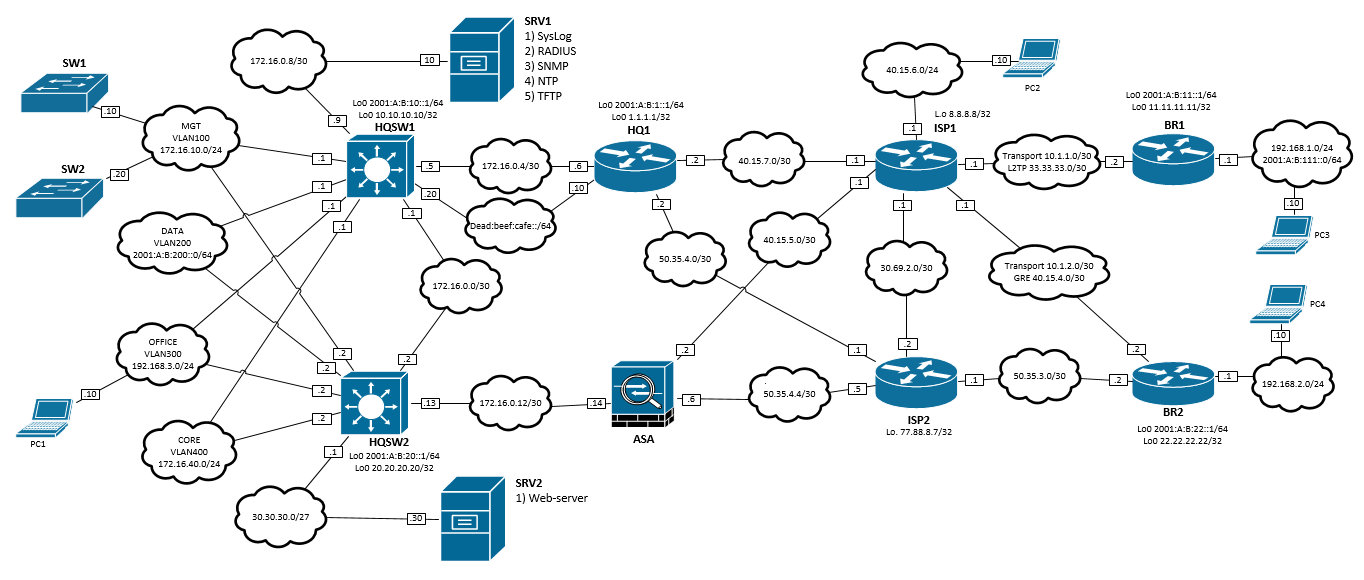
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| User | Line | Extension | Device | СМЕ |
| DugurovD | 1 | 101 | Softphone1 | CME HQ |
| DobryninS | 1 | 102 | Phone1 | CME HQ |
| SilaevN | 1 | 103 | Phone2 | CME HQ |
| ShmakovL | 1 | 104 | Softphone2 | CME BR2 |

1. Настройте IP-телефоны таким образом, чтобы на экране отображалось имя вместо номера. Убедитесь в том, что при звонке также отображается имя, а не номер телефона.
2. Настройте Music-on-Hold на сайте HQ. Используйте файл MOH.wav, расположенный на роутере HQ1.
3. Настройте конференц-связь поддерживающую как минимум трех участников для группового звонка.
4. На телефоне Dobrynin необходимо настроить вторую кнопку (вторая линия) таким образом, чтобы после её нажатия срабатывал intercom на номер SilayevN При звонке на этот номер телефон должны автоматически отвечать с выключенным режимом громкой связи, микрофон должен быть отключен
5. Настройте парковку звонков по нажатию кнопки Park. При звонке на номер 100 любой пользователь должен иметь возможность принять припаркованный звонок
6. Настройте правило трансляции так, чтобы при звонке на номер 88005555555 звонил телефон с номером 104.
7. Настройте кнопку 2 быстрого набора телефона DobryninS, на телефоне ShmakovL

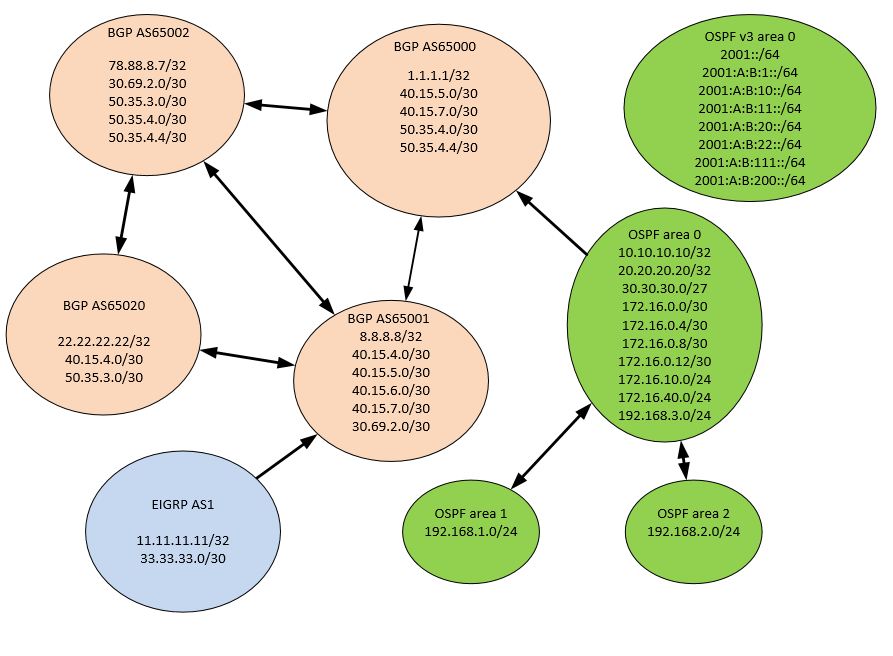
Топология L1

Топология L2

Топология L3



Routing-диаграмма



VPN диаграмма



Диаграмма IP-Телефонии

