

Модуль С: «Пусконаладка телекоммуникационного оборудования» **Версия 1 от 16.02.2021**

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 удастся 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_Logs
- 2) RADIUS - FreeRadius
- 3) SNMP – для проверки используется пакет Net-SNMP используйте команду snmp_test. Например, если вы хотите протестировать подключение к HQ1 нужно ввести команду ./snmp_test.sh HQ1
- 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

Первоначальное подключение осуществляется по протоколу Telnet по следующим адресам. С PC1 Доступны

SW1 – 192.168.0.10

SW2 – 192.168.0.20

SW3 – 192.168.0.30

SW4 – 192.168.0.40

HQ1 – 192.168.0.1

HQ2 – 192.168.0.2

С PC2 Доступны

BR1 – 192.168.2.1

Для подключения используйте следующие учетные данные

Username – cisco

Password – cisco

Enable – cisco

Базовая настройка

- 1) Задайте имя всех устройств в соответствии с топологией.
- 2) Назначьте для всех устройств доменное имя **rea2021.net**
- 3) Создайте на всех устройствах пользователей **reauser** с паролем **skills**
 - a) Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции `script`.
 - b) Пользователь должен обладать максимальным уровнем привилегий.
- 4) На всех устройствах установите пароль **rea21** 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.
- 6) Для всех устройств реализуйте модель AAA
 - a) Аутентификация на линиях виртуальных терминалов с 0 по 15, а также на локальной консоли должна производиться с использованием локальной базы данных
 - b) После аутентификации пользователь должен получать соответствующий уровень привилегий
- 7) Для устройств HQ1 и HQ2 реализуйте аутентификацию с использованием RADIUS сервера
 - a) RADIUS сервером является SRV1
 - b) Используйте общий ключ `gea`
 - c) В качестве портов для аутентификации и учета используйте 1812 и 1813 соответственно
 - d) Проверьте возможность аутентификации, используя учетную запись **radius** с паролем **cisco**
- 8) На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля, назначьте IP-адреса.
- 9) Все устройства должны быть доступны для управления по протоколу SSH версии 2.

```
radius server ACCESS_SERVER_1  
address ipv4 192.168.1.1 auth-port 1111 acct-port 2222  
key KEY-RADIUS
```

```
aaa group server radius ACCESS  
server name ACCESS_SERVER_1
```

```
aaa authentication login default group ACCESS local  
aaa authorization exec default group ACCESS local
```

Настройка коммутации

- 1) Создайте таблицу VLAN:
 - a) VLAN1000 с именем **MGT**.
 - b) VLAN1200 с именем **DATA**.
 - c) VLAN1300 с именем **OFFICE**.
 - d) VLAN1500 с именем **NATIVE**.
 - e) VLAN1600 с именем **SHUTDOWN**.
 - f) VLAN1700 с именем **iBGP**
 - g) VLAN1800 с именем **HQ1**
 - h) VLAN1900 с именем **HQ2**
- 2) Отключите протокол VTP явным образом
- 3) Между всеми коммутаторами настройте транки с использованием протокола IEEE 802.1q.
 - a) Транки между SW1, SW3 и SW4 должны быть согласованы по DTP. SW1 должен инициировать согласование, а SW3 и SW4 должны ожидать согласования от соседа
 - b) Транки между SW2, SW3, SW4 должны быть согласованы по DTP. SW2 должен инициировать согласование, SW3 и SW4 должны ожидать согласования от соседа.
 - c) На остальных портах между коммутаторами транки должны быть согласованы статически. Отключите протокол DTP явным образом
- 4) Настройте агрегирование каналов связи между коммутаторами.
 - a) Номера портовых групп
 - i) 1 Между коммутаторами SW1 и SW3
 - ii) 2 Между коммутаторами SW2 и SW4
 - iii) 3 Между коммутаторами SW1 и SW2
 - b) Между коммутаторами SW1 и SW3 согласование портовых групп должно происходить с использованием протокола LACP. SW1 должен инициировать согласование, а SW3 ожидать согласования от соседа.

- c) Между коммутаторами SW2 и SW4 согласование должно происходить с использованием протокола RaGP. SW2 должен инициировать согласование, а SW4 должен ожидать согласования от соседа.
 - d) Между коммутаторами SW1 и SW2 согласование портовых групп должно происходить без использования протоколов динамического согласования. Портовая группа должна функционировать в режиме L3. Сконфигурируйте адреса в соответствии с L3 диаграммой
 - e) На всех коммутаторах настройте балансировку нагрузки по mac адресу источника.
- 5) Конфигурация протокола остоного дерева:
- a) Используйте протокол, совместимый со стандартом 802.1w.
 - b) Корнем для всех VLAN должен быть SW1, при отказе SW1 корнем должен стать SW2
 - c) На портах в сторону PC1 и SRV1 сконфигурируйте защиту от перехвата роли корневого моста.
 - d) Сконфигурируйте порты в сторону HQ1, HQ2, SRV1, PC1 для работы без ожидания протокола Spanning-tree
 - e) Сконфигурируйте порты в сторону SRV1 и PC1 таким образом, чтобы при получении BPDU они переходили в состояние err-disabled. Сконфигурируйте автоматическое восстановление из этого состояния в течении двух минут.

#Установка BPDUGUARD

Залетаешь на каждый интерфейс:

```
errdisable recovery cause bpduguard
errdisable recovery interval 120
```

- 6) Настройте порты e0/3 коммутаторов SW3 и SW4 в соответствии с L2 диаграммой.
- 7) На всех устройствах, отключите неиспользуемые порты.
- 8) На всех коммутаторах, неиспользуемые порты переведите во VLAN 1600.

Настройка подключений к глобальным сетям

- 1) Провайдер предоставляет IPoE и статический IP адрес. На роутерах HQ1 и HQ2 настройте адреса в соответствии с L3 диаграммой.
- 2) Подключите BR1 ко второму провайдеру при помощи протокола PPPoE
 - a) Сконфигурируйте mtu 1492
 - b) Для аутентификации используйте следующие учетные данные
 - i) Логин – reapproe
 - ii) Пароль -- reaPPPOEPass
 - iii) Протокол – CHAP
 - c) Используйте интерфейс Dialer1
 - d) Адрес должен быть получен автоматически.

PPPoE Router like Client

```
(config)# vpdn enable
(config)# vpdn-group 1
(config)# accept-dialin
(config)# protocol any
(config)# int Dialer 1
    ip address negotiated
    ip mtu 1492
    encapsulation ppp
    dialer pool 1
    dialer-group 1
    ppp authentication chap pap callin
    ppp chap hostname reappoe
    ppp chap password 0 reappoePass
```

на интерфейсе в сторону ИСПА:

```
pppoe global
pppoe-client dial-pool-number 1
```

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.

Также, стоит учесть, что провайдеры фильтруют маршруты полученные по BGP, если они не соответствуют диаграмме маршрутизации.

- 1) На маршрутизаторах HQ1 и HQ2 сконфигурируйте BGP
 - а) В качестве локальной автономной системы на обоих маршрутизаторах используйте 65010. Автономная система провайдера 65000
 - б) Анонсируйте сети в соответствии с Routing диаграммой
- 2) На маршрутизаторе BR1 для связи с провайдером сконфигурируйте BGP
 - а) В качестве локальной автономной системы используйте 65020. Автономная система провайдера – 65000
 - б) Исключите из таблицы маршрутизации сеть 14.88.22.8

```
ip access-list standard FILTER
deny 14.88.22.8
permit any
route-map FILTER permit 10
match ip address FILTER
neighbor IP NEIGHBOUR route-map FILTER in
```

- в) Анонсируйте сети в соответствии с Routing диаграммой
- 3) Для обмена маршрутной информацией в офисе HQ сконфигурируйте протокол EIGRP

- a) В процессе маршрутизации участвуют HQ1, HQ2, SW1, SW2
- b) Используйте номер автономной системы 1
- c) Обеспечьте аутентификацию по паролю EIGRPass
- 4) (config)#key chain TEST - сделали цепочку ключей**
- 2) (config-keychain)#key 1 - номер ключа 1**
- 5) (config-keychain-key)#key-string EIGRPass- сам ключ**
- 6) interface serial 0/0.1 - пошли на интерфейс, где будет сосед**
- 7) (config-subif)#ip authentication mode eigrp 6000 md5 - задали тип аутентификации**
- 8) (config-subif)#ip authentication key-chain eigrp (AS_NUMBER) TEST - привязали к нему конкретный ключ**
- 9) Для связи офисов HQ и BR сконфигурируйте протокол OSPF поверх защищенной сети DMVPN
 - a) Анонсируйте сети в соответствии с роутинг диаграммой
 - b) В процессе маршрутизации участвуют HQ1, HQ2 и BR1
 - c) Маршрутизатор HQ1 должен быть DR, при отказе HQ1 DR должен стать HQ2
 - d) На роутерах HQ1 и HQ2 произведите редистрибьюцию всех маршрутов из EIGRP в OSPF
 - e) Маршрутизатор BR1 должен отдавать суммарный маршрут до сетей Lo10 и Lo20

#OSPF в DMVPN

- 1) Одна особенность, что надо на интерфейс повесить явно ip ospf network broadcast**
- 2) redistribute eigrp 1 metric 100 subnets**

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. Для обеспечения отказоустойчивости настройте HSRP между HQ1 и HQ2 для внешней подсети
 - a) Используйте номер группы 254
 - b) Сконфигурируйте виртуальный IP адрес. В качестве IP адреса используйте последний из данной подсети.
 - c) Сконфигурируйте аутентификацию по паролю HSRPass
 - d) Разрешите перехват роли активного шлюза маршрутизатору с большим приоритетом

3. Настройте трансляцию сетевых адресов из подсетей VLAN1200 и VLAN1300 в виртуальный адрес HSRP группы.

- a) Трансляция должна производиться на основе source port.

#HSRP+NAT

Сначала просто настройка HSRP:

- 1) Идем на интерфейс, который хотим добавить в процесс HSRP

- a) standby 254 ip 100.45.5.6
 - b) standby 254 preempt
 - c) standby 254 auth HSRPass

Процедура повторяется, на другом роутере - для проверки do sh standby

```
HQ1(config)#do sh standby
GigabitEthernet0/1 - Group 254
  State is Standby
    3 state changes, last state change 01:20:24
  Virtual IP address is 100.45.5.6
  Active virtual MAC address is 0000.0c07.acfe
  Local virtual MAC address is 0000.0c07.acfe (vl default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.896 secs
  Authentication text, string "HSRPass"
  Preemption enabled
  Active router is 100.45.5.3, priority 100 (expires in 10.720 sec)
  Standby router is local
  Priority 100 (default 100)
```

На коммутаторах SW1 и SW2 сконфигурируйте отказоустойчивость для подсетей VLAN1200 и VLAN1300 с использованием протокола VRRP.

- b) Используйте номера групп 120 и 130 для VLAN1200 и VLAN1300 соответственно
 - c) Сконфигурируйте аутентификацию по паролю VRRPass
 - d) Разрешите перехват роли активного шлюза коммутатору с большим приоритетом
 - e) В качестве виртуального адреса используйте первый адрес в соответствующей подсети

#VRRP

Заходим на нужный нам интерфейс влан:

- 1) vrrp 130 ip 192.168.100.1
- 2) vrrp 120 ip 172.16.20.1
- 3) vrrp 130 auth text VRRPass
- 4) vrrp 120 auth text VRRPass

Для проверки - do sh vrrp br

```
SW2(config-if)#do sh vrrp br
SW2(config-if)#do sh vrrp br
Interface      Grp Pri Time  Own Pre State  Master addr  Group addr
Vl1200         120 100 3609      Y Master  172.16.20.3   172.16.20.1
Vl1300         130 100 3609      Y Backup   192.168.100.1 192.168.100.1
```

- 5)

- 1) В офисе BR1 используется аутентификация клиентов с помощью протокола L2TP. Для этого настройте сервер L2TP на BR1.
 - f) Аутентификация PC2 на сервере L2TP должна осуществляться по логину pc2user и паролю pc2pass.
 - g) PC2 должен получать ip адрес от L2TP сервера автоматически.
 - h) В качестве подсети используйте 172.16.254.0/24
 - i) Транспортный адрес сконфигурируйте на свое усмотрение
 - j) Проверьте соединение с PC2

#L2TP

- 1) Создание L2TP соединения
 - a) (conf)#vpdn enable
 - b) (conf)#vpdn-group L2TP
 - c) (conf-vpdn)# accept-dialin
 - d) (conf-vpdn-accept)# protocol l2tp
 - e) (conf-vpdn-accept)#virtual-template 1
 - f) (conf-vpdn)# no l2tp tunnel auth
- 2) Создали пул адресов для клиентов
 - a) (conf)# ip local pool L2TP 172.16.250.100
- 3) Создаем виртуальный интерфейс для подключения
 - a) (conf)#int virtual-templ 1
 - b) (conf-if)#ip unnumbered g0/1
 - c) (conf-if)#peer default ip address pool L2TP
 - d) (conf-if)#ppp auth chap ms-chap ms-chap-v2
- 4) Далее колотим шифрование
 - a) crypto isakmp policy 10
 - b) encr 3des
 - c) authentication pre-share
 - d) group 2
 - e) lifetime 3600
- 5) crypto ipsec transform-set L2TP esp-3des esp-sha-hmac
 - a) mode transport
- 6) crypto isakmp key cisco address 0.0.0.0
- 7) crypto dynamic-map L2TP 10
 - a) set transform-set L2TP
- 8) crypto map L2TP 10 ipsec-isakmp dynamic L2TP
- 9) int g0/1
 - a) crypto map L2TP

Далее настройка AAA

- 10) aaa authentication ppp default local
- 11) aaa authorization network default local
- 12) username pc2user password pc2pass

На Windows создай L2TP подключение, тут вроде умеешь вруби там все возможные и невозможные протоколы аутентификации

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 G0/3 коммутаторов SW3 и SW4 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 G0/3 коммутаторов SW3 и SW4 реализуйте защиту от перехвата трафика между двумя узлами в одном широковещательном домене
- 4) На коммутаторе SW3 включите DHCP Snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных.
- 5) На коммутаторе SW3 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.

Настройка параметров мониторинга и резервного копирования

- 1) На маршрутизаторах HQ1 и HQ2 настройте журналирование системных сообщений на сервер SRV1, включая информационные сообщения.

- 2) На маршрутизаторах HQ1 и HQ2 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.

snmp-server location MSK, Russia

snmp-server contact admin@wsr.ru

snmp-server group WSR v3 priv

snmp-server community RO ro

snmp-server user snmpuser WSR v3 auth sha snmppass priv aes 128 snmppass

- 3) На маршрутизаторах HQ1 и HQ2 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**

Конфигурация виртуальных частных сетей

- 1) Для защищенного соединения между офисами настройте DualHub SingleCloud Phase 3 DMVPN со следующими параметрами
- a) В качестве Hub выступают HQ1 и HQ2, в качестве Spoke – BR1
 - b) Используйте аутентификацию NHRP по паролю **cisco**
 - c) Установите значение **mtu 1400**
 - d) В качестве интерфейса-источника используйте соответствующий Loopback интерфейс на маршрутизаторе
 - e) Остальные параметры сконфигурируйте на свое усмотрение

#Создание DMVPN DualHub по сертификатам

шаг 1: Выпустить сертификаты для всех роутеров, которые будем использовать в подключении

- 1) Создать трастпоинт
- a) **HQ1# conf t**
 - b) **HQ1(config)# crypto pki trustpoint CA**
 - c) **HQ1(ca-trustpoint)#exit**
 - d) **HQ1(config)# crypto key generate rsa label HQ1.rea2021.net modulus 2048 exportable**

- e) HQ1(config)# crypto pki trustpoint CA
- f) HQ1(ca-trustpoint)#rsakeypair HQ1.rea2021.net
- g) HQ1(ca-trustpoint)# revocation-check none
- h) HQ1(ca-trustpoint)# enrollment terminal
- i) HQ1(ca-trustpoint)# exit
- j) HQ1(ca-trustpoint)# subject-name CN=HQ1.rea2021.net
- k) HQ1(config)# crypto pki authenticate CA - на этом этапе роутеру нужно скормит сертификат с ЦА. Тут просто cat /etc/ca/cacert.pem и что увидишь туда копируй

2) Теперь заказываем серт от ЦА

- a) HQ1(config)# crypto pki enroll CA

```

RTR(config)#crypto pki enroll DomSubCA
% Start certificate enrollment ..

% The subject name in the certificate will include: RTR.final.wsr
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: FTX165283NB
% Include an IP address in the subject name? [no]: 31.33.7.2
% Please answer 'yes' or 'no'.
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[:]: 1.1.1.1
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIIBqTCCARICAQAuSDFGMBIGA1UEBRMLR1RYMTY1MjgzTkIwFAYJKoZIhvcNAQkI
EwcxLjEuMS4xMBoGCSqGSIb3DQEJAhYNULRSLmZpbmFsLndzcjCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwYkCgYEAAt2NKdGXjjlyUkrNz5orhrzUBgKnwd5M8Vhgu7wB2
47jmEgaBBwUiH1k1Z48bHCj7zA44GPa4kKGRgm8yBdeJdiwkrz+tz38i5UdQuzNv
ZH3/kdT9We02kK9jqul+2AFeIngdf4fKcXxASznLHHxgUTI27TtsaneupjQ8rmkk
jUECAwEAAaAhMB8GCSqGSIb3DQEJDjESMBAwDgYDVROPAQH/BAQDAgWgMA0GCSqG
SIb3DQEBBQUAA4GBAAG5lmp+86WKxqE/O/wrs2f3IalHiW3/RDyEVYUeUZcqOV0t
t490+WcHP012+fCKVwXVFDpVvZEQ3kFXUhnG56nI3We2x7nnoB4UjFCVJk8BC+Qm
vdsYHvHpzSbWXTtRr0/wvp6pP1z11wvrIGiORwls+a/pKfLUn71slGIRzEaC

---End - This line not part of the certificate request---
```

Копируй

- 3)
- 4) То что скопировал вставляй в newreq.pem, крайне важно соблюдать формат документа -----BEGIN-----END---


```

root@SRV1:/usr/lib/ssl/misc# cat newreq.pem
-----BEGIN CERTIFICATE REQUEST-----
MIIC1DCCABwCAQAwbjEYMBYGA1UEAxMPSFExLnJlYTIwMjEubmV0MVIwFAYJKoZI
hvcNAQkIEwcZLjMuMy4zMBwGA1UEBRMVOUpYMUUVIUUdTU1lTWlVJN0hPVkhSMBwG
CSqGSIb3DQEJAhYPSFExLnJlYTIwMjEubmV0MIIIBIjANBgkqhkiG9w0BAQEFAAOc
AQ8AMIIBCgKCAQEAz9GEtWukivag/QP09QZmCghTSDMFdgMImeToB2NHR8wWbyNI
Ij/tDGS2Rg3asH8bUy9aj4lhX5H8CdhivV3iR+lkK0vv1Cx5/8JuPaSoyBJSfEiv
bUV95t199W/+6KcLj4NfaJ0F5PDhtI096DaaotTf3o2WlchJyo2lihwEU2hxUJ7F
DMQfVZTKvSlzMKiYz5UumJB0baqPBgSdzJTa5dsxfv+ajScoYxQ2NfzFv2ZcjISb
9DZq4hnaM81b15aaBdINEfufnDlRCbqu8eVfjFfqq90IkDfkiDNRgyYrvFsVY/b9
ClQmp5a0p+hAukbdwukJ30Ci4MMxyfXzfB1HpQIDAQABoCEwHwYJKoZIhvcNAQkO
MRIwEDAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQADggEBACJ02F6UnE2h
20PxS/RWoFubB5iNc+ivsyEW9fJNWNysyAoiINzgbqXHjBeFe1tcXlKyf7JWYvfs
s+e1BTyFYe6FxdWh3F/qb6SeI774YLccbwzyc6DDB05Z2u2qw6ZdfDqzPvcorkH
ThVsbidBJzzIMesjcz1Kn0mqxPuzIqL4gZWgur3dK3PNdQbaNcCV560+DH4qsMJ
4J+0R1EsGKUK4Fwjdfp/hNgDLNHKcYP0zi7K/KCYh215wWcBeOvWVT9E0tGCLrUw
wXxRMERQ2scDThZJHuDSou3w6c+3Vm7d/dJoAuGxjjCOoanv6W9dhLBPrbyWZ6L8
NvleXrIwx5w=
-----END CERTIFICATE REQUEST-----

```


- 5) Выписывай сертификат через ./CA.pl -sign. Полученный серт в base64 надо импортировать в Cisco
- 6) HQ1(config)# crypto pki import CA certificate

Запомни как выглядит успех:

```

LLEaMM1Cy1eWl1HmNBQBP0RQNVSIz+aTQk6w7ctqv+6+yZ6Dq3tpDQyqLa
RYCwph80LLHhIOZLxzPf09xo030eLeaH5tKyCGdDcK5H6FrIj5ZXrqGaqq
PgSgHkLn0iOZam+p/H2mp6CSs+2cDPdZYzR0t4TRQE1hDPDdgagGMSZkcny
WotmHBw5TUanCj1IjzdUbR+U=
cl-----END CERTIFICATE-----
tquit
R% Router Certificate successfully imported
G
A BRANCH(config)#
K BRANCH(config)#
  BRANCH(config)#

```



#IPSEC IKEv2 DMVPN по сертам, летс гоу

- 1) Создали предложение, где указали настройки шифрования

HQ1#conf t

HQ1(config)#crypto ikev2 proposal DMVPN

HQ1(config-ikev2-proposal)# encryption 3des

HQ1(config-ikev2-proposal)# group 5

HQ1(config-ikev2-proposal)# integrity sha1

HQ1(config-ikev2-proposal)# prf sha1

Приделали это предложение к политике

HQ1(config)# crypto ikev2 policy DMVPN

HQ1(config-ikev2-policy)# proposal DMVPN

Профиль IKEv2 (только FQDN на каждом меняй для опознания других

HQ1(config)# crypto ikev2 profile IPSEC

HQ1(config-ikev2-profile)# match identity remote fqdn HQ2.rea2021.net

HQ1(config-ikev2-profile)# match identity remote fqdn BR1.rea2021.net

HQ1(config-ikev2-profile)# identity local fqdn HQ1.rea2021.net

HQ1(config-ikev2-profile)# authentication local rsa-sig

HQ1(config-ikev2-profile)# authentication remote rsa-sig

HQ1(config-ikev2-profile)# pki trustpoint CA

HQ1(config)# no crypto ikev2 http-url cert

Создаем IPSEC

```
HQ1(config)# crypto ipsec transform-set DMVPN esp-aes esp-md5-hmac
```

```
HQ1(cfg-crypto-trans)# mode tunnel
```

биндим к IPSEC профилю наши настройки

```
HQ1(config)# crypto ipsec profile DMVPN
```

```
HQ1(ipsec-profile)# set transform-set DMVPN
```

```
HQ1(ipsec-profile)# set ikev2-profile DMVPN
```

Данные команды актуальны для всех устройств в DMVPN.

Для HQ1

```
int tun1
```

```
ip address 172.16.3.1 255.255.255.0
```

```
no ip redirects
```

```
ip nhrp network-id 1
```

```
ip nhrp auth cisco
```

```
tunnel source lo0
```

```
tunnel mode gre multipoint
```

```
tunnel protection ipsec profile DMVPN
```

Для HQ2

```
int tun2
```

```
ip address 172.16.3.2 255.255.255.0
```

```
no ip redirects
```

```
ip nhrp network-id 1
```

```
ip nhrp auth cisco
```

```
tunnel source lo0
```

```
tunnel mode gre multipoint
```

```
tunnel protection ipsec profile DMVPN
```

Для BR1

```
int tun1
```

```
ip address 172.16.3.3 255.255.255.0
```

```
no ip redirects
```

```
ip nhrp map 172.16.3.1 1.1.1.1
```

```
ip nhrp auth cisco
```

```
ip nhrp map multicast 1.1.1.1
```

```
ip nhrp map 172.16.3.2 2.2.2.2
```

```
ip nhrp map multicast 2.2.2.2
```

```
ip nhrp network-id 1
```

```
ip nhrp nhs 172.16.3.1
```

```
ip nhrp nhs 172.16.3.2
```

```
tunnel source lo0
```

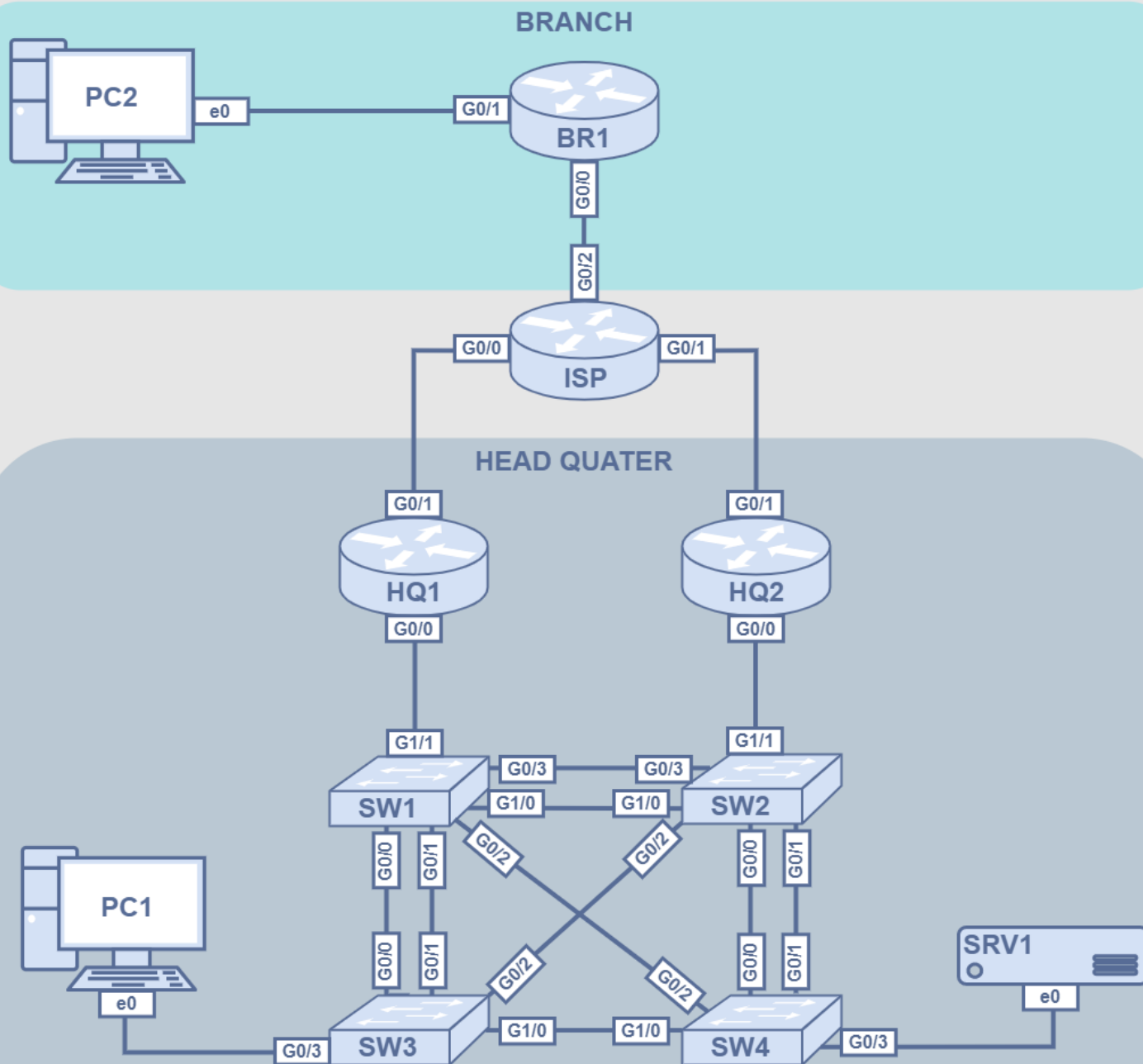
```
tunnel mode gre multipoint
```

```
tunnel protection ipsec profiles DMVPN shared
```

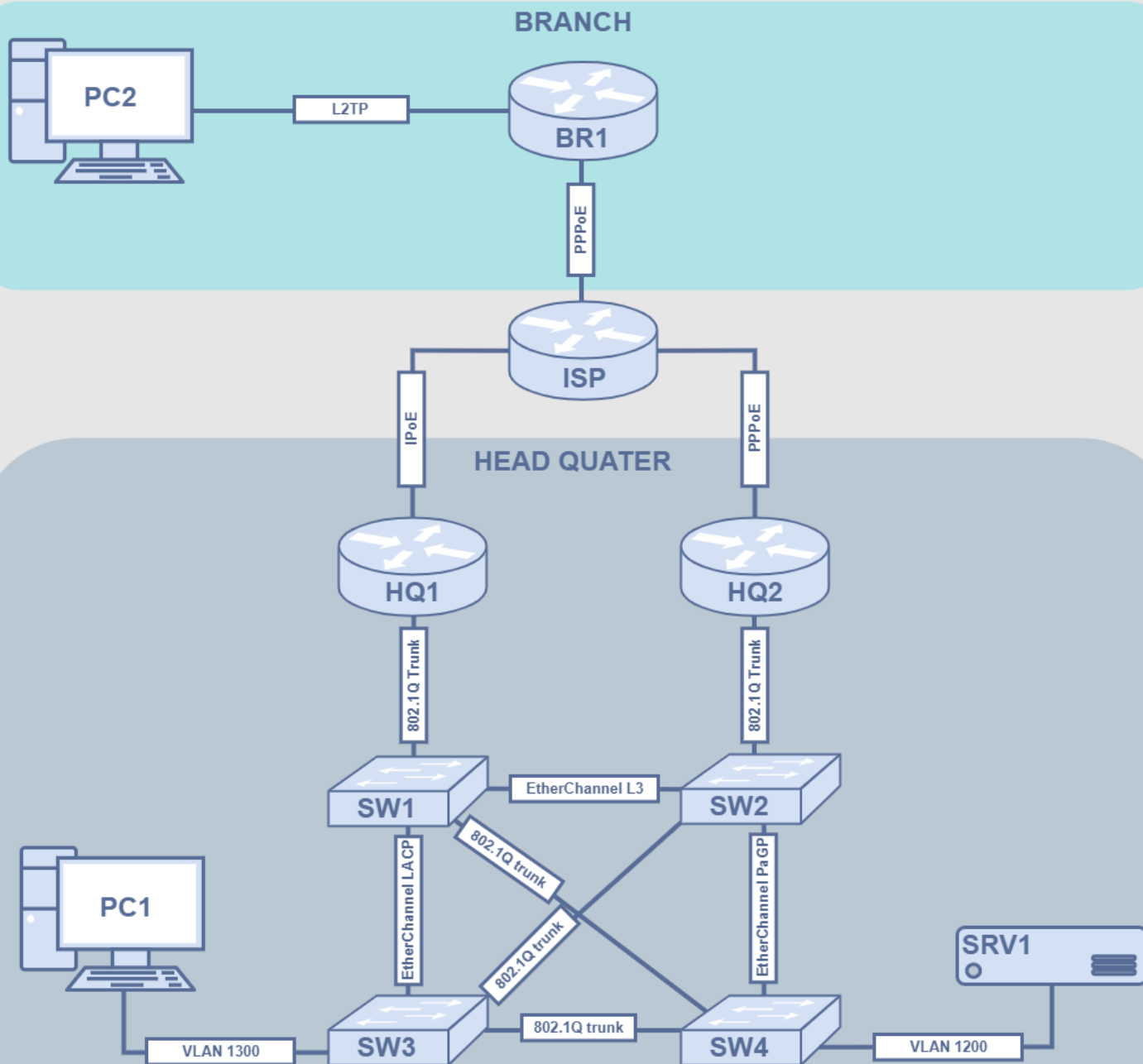
- 2) Защита туннеля должна обеспечиваться с помощью IKEv2 IPSEC.
- a) Обеспечьте шифрование только GRE трафика.
 - b) Используйте аутентификацию по цифровым сертификатам.
 - c) Остальные параметры произвольные

Для получения цифровых сертификатов, на сервере SRV1 развернут центр сертификации. Для того, чтобы получить сертификат, необходимо сформировать файл newreq.pem. Файл должен содержать запрос сертификата с роутера. После формирования файла необходимо выполнить команду CA.pl -sign. При запросе пароля укажите P@ssw0rd. После подписи запроса в текущей директории появится файл newcert.pem, который необходимо импортировать на роутер. Корневой сертификат можно найти по следующему пути: /etc/ca/cacert.pem.

Топология L1

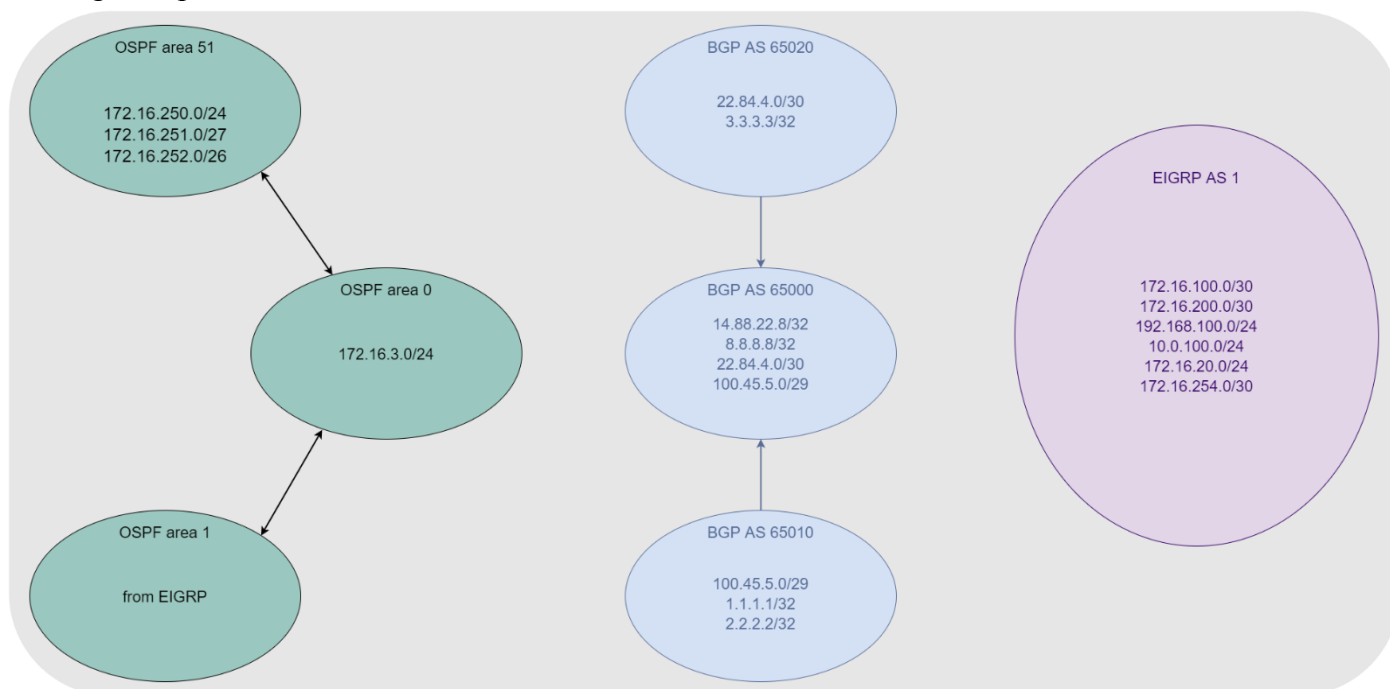


Топология L2



Топология L3

Routing-диаграмма



VPN диаграмма

