Конкурсное задание

ИТ Сетевое и системное администрирование

Модуль B – Сетевое окружение

Представлено :
Christian Schöndorfer AT
Almut Leykauff-Bothe DE
Gustavo Adolfo Rodríguez Salinas CO
Jaeha Lee KR
Svetlana Lapenko KZ
Te Chao Liang TW

Содержание

Введение в конкурсное задание

Ниже приводится список разделов или информации, которые должны быть включены во все предложения по тестовым проектам, представляемые в WorldSkills.

- Содержание, включая список всех документов, рисунков и фотографий, составляющих Конкурсное задание.
- Введение/обзор
- Краткое описание проекта и задач
- Инструкция для участника
- Оборудование, машины, установки и материалы, необходимые для выполнения Конкурсного задания.
- Схема выставления оценок (включая критерии оценки)
- Другое

Введение

Знание сетевых технологий в настоящее время становится необходимым для людей, которые хотят построить успешную карьеру в любой области ИТ-инженерии. Этот тестовый проект содержит множество задач из реального жизненного опыта, в первую очередь ИТ-интеграцию и ИТ-аутсорсинг. Если вы сможете завершить этот проект с высоким баллом, вы определенно готовы обслуживать сетевую инфраструктуру любого многоотраслевого предприятия.

Описание проекта и задач

Этот тестовый проект разработан с использованием различных сетевых технологий, которые должны быть знакомы из сертификационных курсов Cisco. Задачи разбиты на следующие разделы конфигурации:

- Базовая конфигурация
- Коммутация
- Маршрутизация
- Службы

- Безопасность
- WAN и VPN

Все разделы независимы, но все вместе они создают очень сложную сетевую инфраструктуру. Некоторые задачи довольно просты и понятны; другие могут быть сложными. Вы можете заметить, что некоторые технологии должны работать поверх других технологий. Например, ожидается, что маршрутизация IPv6 будет работать поверх настроенных VPN, которые, в свою очередь, должны работать поверх маршрутизации IPv4, которая, в свою очередь, должна работать поверх PPPoE, и так далее. Важно понимать, что если вы не можете найти решение посреди такого стека технологий, это не значит, что остальная ваша работа вообще не будет оцениваться. Например, вы можете не настраивать маршрутизацию IPv4, которая требуется для VPN, из-за доступности IP, но вы можете использовать статические маршруты, а затем продолжить работу с конфигурацией VPN и всем, что работает поверх нее. В этом случае вы не получите баллы за маршрутизацию IPv4, но вы получите баллы за все, что вы сделали работоспособным, если функциональное тестирование прошло успешно.

Инструкция для участника

1. Прочтите все задачи в каждом разделе, прежде чем приступать к какой-либо настройке. Для завершения любого элемента может потребоваться завершение любого предыдущего или последующего элемента.
2. Баллы начисляются только за рабочие конфигурации. Перед отправкой тестового проекта проверьте функциональность всех требований. Будьте осторожны, потому что при настройке одной части вы можете нарушить предыдущее требование или конфигурацию.
3. Частичные баллы не могут быть предоставлены ни для одного аспекта; необходимо выполнить все требования, чтобы получить очки за аспект. Некоторые требования зависят от требований других аспектов, до или после текущего аспекта.
4. Чаще сохраняйте свои конфигурации; аварии бывают и будут.
5. Все виртуальные машины предустановлены. Используйте локальные учетные данные **admin\Skill39** для доступа к виртуальным машинам Windows и **root\Skill39** для доступа к виртуальным машинам Linux. Не меняйте эти пароли.

Необходимое оборудование, машины, установки и материалы

Ожидается, что все Конкурсные задания могут быть выполнены Конкурсантами на основе оборудования и материалов, указанных в Списке инфраструктуры.

Схема маркировки

Согласно Спецификациям стандартов WorldSkills в рамках настоящего Технического описания, все оценки по данному модулю тестового проекта относятся к разделу 7 «Настройка сетевых устройств», максимальная оценка которого составляет 25.

Базовая конфигурация

1. Настройте имена хостов для всех сетевых устройств, как показано в топологии.
2. Настройте доменное имя **wsc2022.net** для всех сетевых устройств в топологии.
3. Настройте **Skill39** в качестве пароля привилегированного режима для всех устройств.
   a. В конфигурации должен храниться только PBKDF2-хэш пароля.
4. Настройте адрес IPv4/IPv6 для всех сетевых устройств, как показано в топологии.
5. Настройте KST +9 в качестве часового пояса для всех сетевых устройств.

Коммутация

1. Настройте VTP на всех коммутаторах для синхронизации VLAN. Должна быть возможность изменять базу данных VLAN только с DSW1, а базы данных VLAN всех остальных коммутаторов должны синхронизироваться с DSW1. База данных VLAN на всех коммутаторах должна содержать следующие VLAN.
   a. VLAN 10 с именем SRV
   b. VLAN 20 с именем CLI
2. Настройте все соединения между коммутаторами как транковый порт.
   a. Не используйте протокол динамического согласования.
   b. Настройте отсечение вручную, чтобы разрешалась пересылка только для созданных VLAN.
3. Настройте EtherChannel между коммутаторами.
   a. Используйте следующие номера портов-каналов:
      1 – между коммутаторами DSW1 и DSW2

2 – между коммутаторами DSW1 и ASW1
3 – между коммутаторами DSW2 и ASW2

b. DSW1 и DSW2 не использует протокол динамического согласования.
c. Агрегированный канал между DSW1 и ASW1 использует проприетарный протокол Cisco для динамического согласования.
d. Агрегированный канал между DSW2 и ASW2 использует стандартный протокол для динамического согласования.
e. DSW1 и DSW2 должны инициировать согласование, а другие устройства должны отвечать, но не инициировать.
f. Настройте балансировку нагрузки и метод переадресации с MAC-адресами источника и назначения.

4. Настройте STP.
   a. DSW1 должен быть корневым мостом STP VLAN10. Если DSW1 выходит из строя, DSW2 должен стать корневым мостом STP.
   b. DSW2 должен быть корневым мостом STP для VLAN20. Если DSW2 выходит из строя, DSW1 должен стать корневым мостом STP.
   c. Трафик от HQ-CLI должен проходить через DSW1.
   d. Настройте порт, который подключен к конечному устройству, чтобы он сразу же переходил в состояние пересылки при подключении.

Маршрутизация

1. Настроить EIGRP.
   a. Убедитесь, что все виртуальные машины во внутренней сети могут взаимодействовать с другими.
   b. HQ1 и HQ2 должны анонсировать только суммарный маршрут 192.168.0.0/16 к BR1 и BR2.
2. Настройте BGP.
   a. Используйте интерфейс Loopback 0 для установления соседства eBGP между AS 65001 и 65002.
   b. Объявите все сети общедоступной сети Интернет (включая интерфейс Loopback) в BGP.
   c. Добавьте нулевой маршрут для сетей, необходимых для выполнения других задач. Распределите их по BGP на HQ1 и HQ2.
3. Настройте OSPFv3 на стороне HQ.

a. Убедитесь, что на канале между маршрутизаторами и коммутаторами нет выбора DR или BDR.
b. Включите аутентификацию в области 2022. Используйте 512-битный алгоритм SHA и ключ аутентификации **Skill39**.
c. HQ-SRV должен иметь возможность подключаться к DC-SRV по протоколу IPv6.

4. Настройте балансировку нагрузки для трафика. (Только IPv4)
   a. Настройте балансировку трафика между сайтом HQ и Интернетом, чтобы канал через HQ1 был предпочтительным.
   b. Настройте балансировку трафика между сайтами HQ и BR так, чтобы канал через HQ2 был предпочтительным. Если HQ2 выходит из строя, используется канал через HQ1.

Службы

1. Настроить NAT.
   a. Когда HQ-CLI связывается с Интернетом, этот IP-адрес должен быть преобразован в 98.76.12.1-98.76.12.10.
   b. Когда BR-CLI1 и BR-CLI2 обмениваются данными с Интернетом, эти IP-адреса должны быть преобразованы в IPv4-адрес интерфейса, который подключен к интернет-провайдеру на каждом маршрутизаторе.
   c. Интернет-клиенты могут получить доступ к DNS и HTTP на DC-SRV через IPv4-адрес внешнего интерфейса на FW1.
2. Настроить DHCP.
   a. HQ-CLI, BR-CLI1 и BR-CLI2 могут автоматически получать IP-адрес.
   b. Все DHCP-клиенты должны использовать **DC-SRV** в качестве DNS-сервера.
3. Настройте FHRP на DSW1 и DSW2.
   a. Используйте Hot Standby Router Protocol v2 для VLAN 10.
      i. DSW1 следует использовать в качестве шлюза по умолчанию.
      ii. Используйте 1 04 в качестве номера группы IPv4 и 1 06 в качестве номера группы IPv6.
      iii. Используйте **192.168.10.254** в качестве виртуального IPv4-адреса и **2002:624C:3201:10::254** в качестве виртуального IPv6-адреса.
      iv. HQ-SRV должен использовать этот VIP в качестве шлюза по умолчанию.
   b. Используйте Hot Standby Router Protocol v2 для VLAN 2 0.
      i. DSW2 следует использовать в качестве шлюза по умолчанию.
      i. Используйте 204 в качестве номера группы IPv4 и 206 в качестве номера группы IPv6.
      ii. Используйте **192.168.20.254** в качестве виртуального адреса IPv4. и **2002:624C:3201:20:254** в качестве виртуального IPv6-адреса.
      iii. HQ-CLI должен использовать этот VIP в качестве шлюза по умолчанию.
4. Настройте удаленный мониторинг с помощью SNMP на HQ1, HQ2 и FW1.
   a. Настройка местоположения устройства **Ilsan, Korea**
   b. Настройте системный контакт **admin@wsc2022.net**

c. Сервер мониторинга Cacti предварительно настроен на HQ-SRV. Вы можете использовать его, чтобы проверить, работает ли SNMP правильно или нет, через http://192.168.10.1/cacti (имя пользователя: admin, пароль: Skill39)

5. Настройте провайдера как NTP-сервер. Все сетевые устройства должны синхронизировать время с провайдером.

Безопасность

1. Настройте аутентификацию консоли на всех сетевых устройствах.
   a. Используйте локальную учетную запись. Создайте пользователя **admin** с паролем **Skill39** .
   b. После успешной аутентификации пользователи должны автоматически переходить в привилегированный режим (кроме FW1) .
2. HQ1 и HQ2.
   a. Используйте сервер RADIUS для аутентификации.
      i. Используйте HQ-SRV в качестве сервера RADIUS.
      ii. Используйте **Skill39** в качестве общего ключа.
      iii. Протестируйте аутентификацию RADIUS, используя следующих пользователей с паролем **Skill39**:
         имя пользователя **user1** с максимальным уровнем привилегий
         имя пользователя **user2** с уровнем привилегий 5
   b. Пользователь **user2** должен иметь возможность настраивать любые параметры IP интерфейса и административно включать или отключать любой из этих интерфейсов.
   c. Если сервер RADIUS выйдет из строя, используйте локальную учетную запись в качестве резервного метода аутентификации.
   d. Убедитесь, что только HQ-CLI разрешен доступ через SSH.
3. Настройте безопасность порта на порту, который подключен к HQ-CLI, используя следующие параметры:
   a. Максимальный MAC-адрес – 2
   b. В случае нарушения политики на консоли должно отображаться сообщение безопасности, порт должен быть отключен.
   c. Восстановите отключенный порт через 3 минуты.
4. Настройте отслеживание DHCP для VLAN 20 на ASW2.

WAN и VPN

1. Настройте ISP как сервер PPPoE и BR1 как клиент PPPoE.
   a. Используйте CHAP для аутентификации с учетными данными **chapuser**/**Skill39**.
2. Настройте туннели между HQ1, HQ2, BR1 и BR2.
   a. Используйте интерфейс Loopback в качестве исходного интерфейса туннеля на каждом маршрутизаторе.

b. Сайты HQ и BRANCH должны иметь возможность общаться друг с другом через этот туннель.

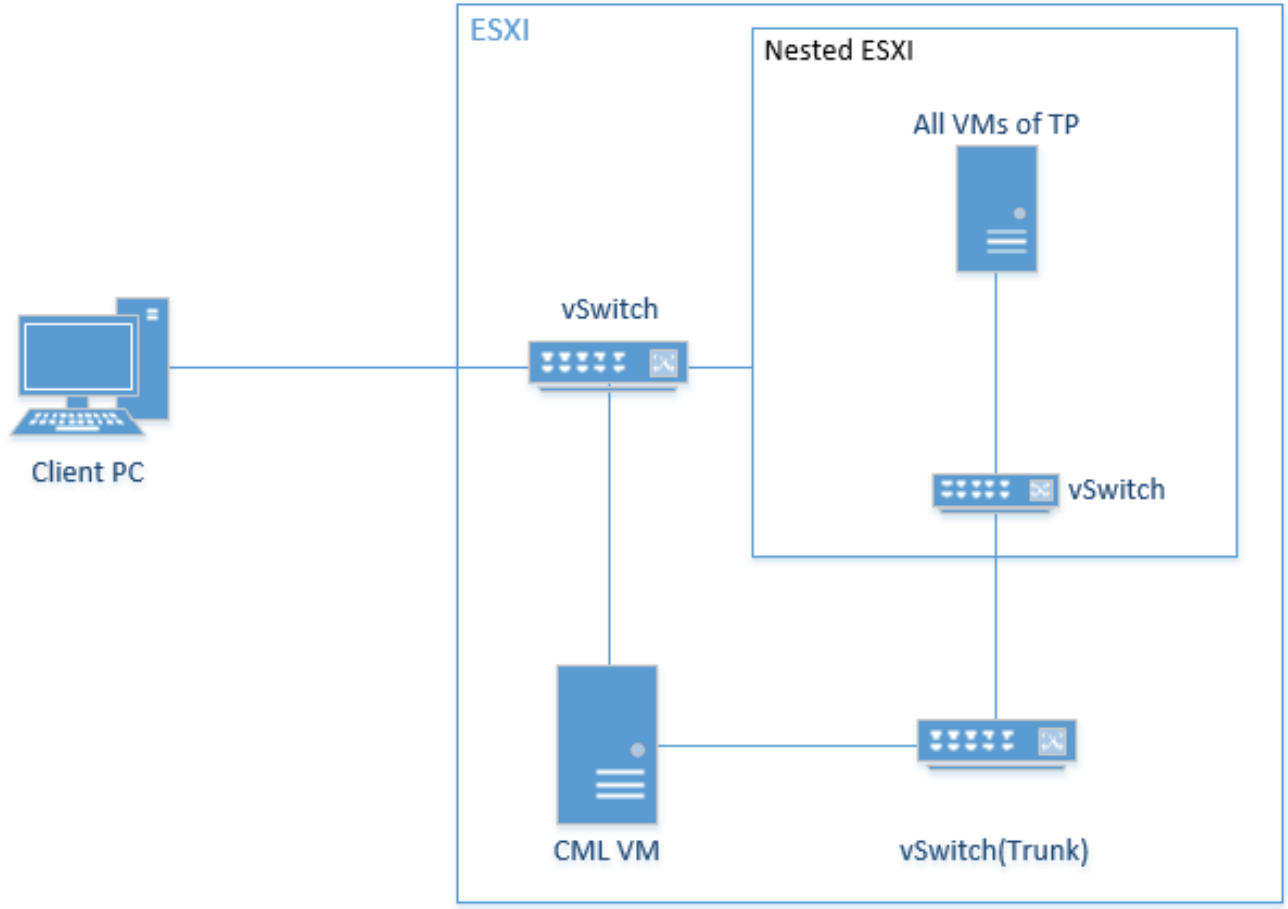
3. Настройте туннель между HQ1 и FW1.
   a. Убедитесь, что HQ-CLI, BR-CLI1 и BR-CLI2 могут взаимодействовать с DC-SRV.
4. Настройте AnyConnect VPN на FW1.
   a. Создайте локального пользователя **vpnuser** с паролем **Skill39** на FW1.
   b. Убедитесь, что VPN-клиент может обмениваться данными с DC-SRV и HQ-SRV.
   c. После подключения клиента vpn клиент должен использовать внутренний адрес **DC-SRV** в качестве DNS-сервера.

Таблица конфигурации

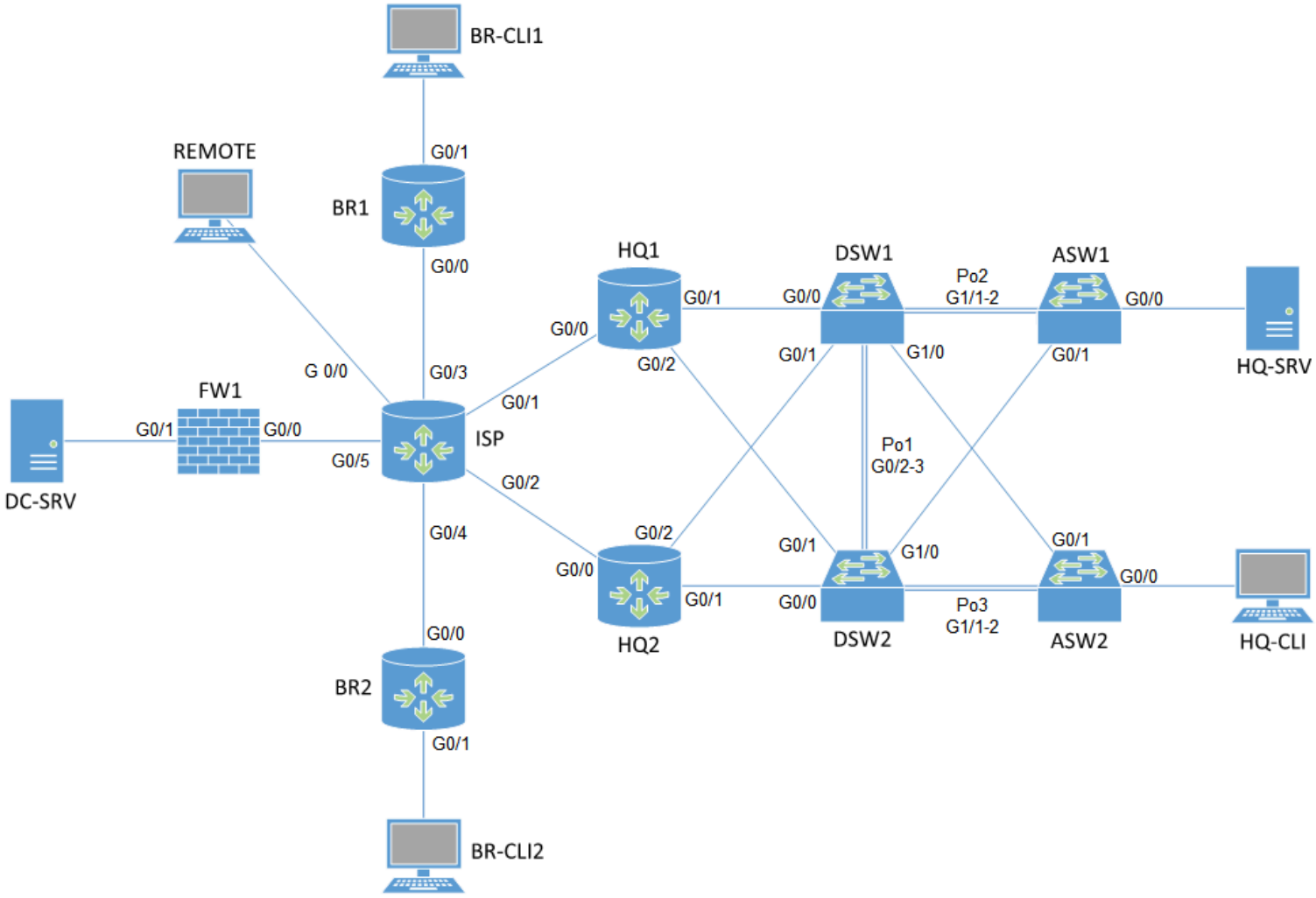
Сайт _	Устройство	Интерфейс	Адрес
Internet	ISP	Loopback0	8.8.8.8/32
		GigabitEthernet0/0	98.76.54.254/24
		GigabitEthernet0/1	98.76.1.254/24
		GigabitEthernet0/2	98.76.2.254/24
		GigabitEthernet0/3	98.76.3.254/24
		GigabitEthernet0/4	98.76.4.254/24
		GigabitEthernet0/5	98.76.5.254/24
	REMOTE	Ethernet 0	98.76.54.1/24
Headquarter	HQ1	Loopback0	1.1.1.1/32
		GigabitEthernet0/0	98.76.1.1/24
		GigabitEthernet0/1	192.168.1.2/30
		GigabitEthernet0/2	192.168.1.6/30
	HQ2	Loopback0	2.2.2.2/32
		GigabitEthernet0/0	98.76.2.1/24
		GigabitEthernet0/1	192.168.2.2/30
		GigabitEthernet0/2	192.168.2.6/30
	DSW1	GigabitEthernet0/0	192.168.1.1/30
		GigabitEthernet0/1	192.168.2.5/30
		Vlan 10	192.168.10.253/24 2001:624C:3201:10::253/64
		Vlan 20	192.168.20.253/24 2001:624C:3201:20::253/64
	DSW2	GigabitEthernet0/0	192.168.2.1/30
		GigabitEthernet0/1	192.168.1.5/30
		Vlan 10	192.168.10.252/24 2001:624C:3201:10::252/64
		Vlan 20	192.168.20.252/24 2001:624C:3201:20::252/64
	ASW1	Vlan 10	192.168.10.201/24 2001:624C:3201:10::201/64

	ASW2	Vlan 10	192.168.10.202/24 2001:624C:3201:10::202/64
	HQ-SRV	ens192	192.168.10.1/24 2001:624C:3201:10::1/64
	HQ-CLI	Ethernet 0	192.168.20.x/24 (DHCP) 2001:624C:3201:20::x/64
Branch office1	BR1	Loopback0	3.3.3.3/32
		GigabitEthernet0/0	98.76.3.1/24
		GigabitEthernet0/1	172.20.10.254/24
	BR-CLI1	Ethernet 0	172.20.10.x/24 (DHCP)
Brach office 2	BR2	Loopback0	4.4.4.4/32
		GigabitEthernet0/0	98.76.4.1/24
		GigabitEthernet0/1	172.20.20.254/24
	BR-CLI2	Ethernet 0	172.20.20.x/24 (DHCP)
Datacenter	FW1	GigabitEthernet0/0 (outside)	98.76.5.1/24
		GigabitEthernet0/1 (inside)	192.168.100.254/24 2001:624C:3201:100::254/64
	DC-SRV	ens192	192.168.100.1/24 2001:624C:3201:100::1/64

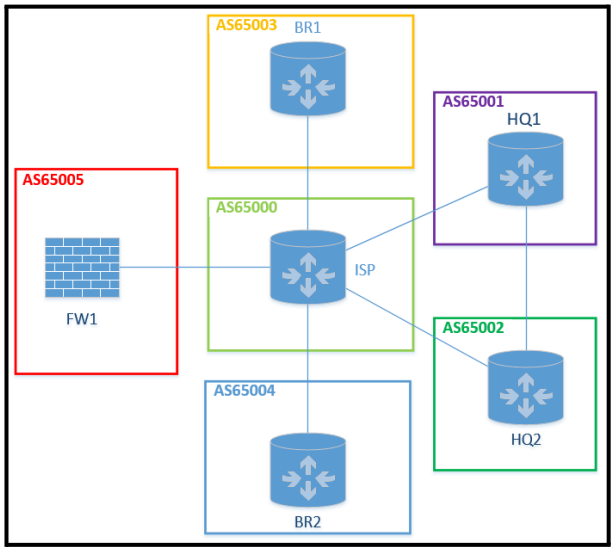
Физическая схема

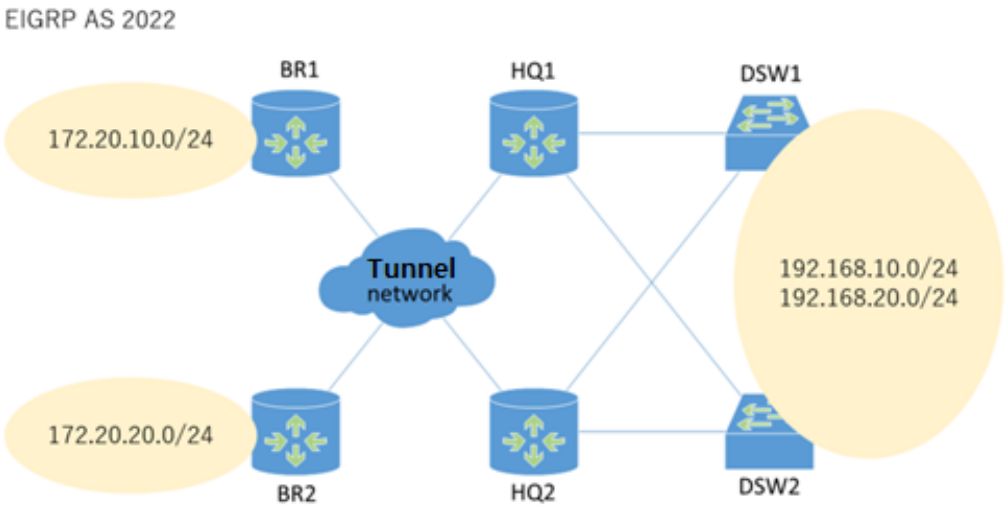


Топология сети



Топология маршрутизации IPv4





Топология маршрутизации IPv6