Test Project

IT Network Systems Administration

Module B – Networking Environment

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

Contents

Introduction to Test Project

The following is a list of sections or information that must be included in all Test Project proposals that are submitted to WorldSkills.

- Contents including list of all documents, drawings and photographs that make up the Test Project
- Introduction/overview
- Short description of project and tasks
- Instructions to the Competitor
- Equipment, machinery, installations and materials required to complete the Test Project
- Marking scheme (incl. assessment criteria)
- Other

Introduction

Network technology knowledge is becoming essential nowadays for people who want to build a successful career in any IT engineering field. This test project contains a lot of challenges from real life experience, primarily IT integration and IT outsourcing. If you are able to complete this project with the high score, you are definitely ready to service the network infrastructure for any multi-branch enterprise.

Description of project and tasks

This test project is designed using a variety of network technologies that should be familiar from the Cisco certification tracks. Tasks are broken down into following configuration sections:

- Basic configuration
- Switching
- Routing
- Services
- Security
- WAN and VPN

All sections are independent but all together they build very complex network infrastructure. Some tasks are pretty simple and straightforward; others may be tricky. You may see that some technologies are expected to work on top of other technologies. For example, IPv6 routing is expected to run on top of configured VPNs, which are, in turn, expected to run on top of IPv4 routing, which is, in turn, expected to run on top of PPPoE, and so on. It is important to understand that if you are unable to come up with a solution in the middle of such technology stack it doesn’t mean that the rest of your work will not be graded at all. For example, you may not configure IPv4 routing that is required for VPN because of IP reachability but you can use static routes and then continue to work with VPN configuration and everything that runs on top. You won’t receive points for IPv4 routing in this case but you will receive points for everything that you made operational on top as long as functional testing is successful.

Important notice to the Competitor

Your configuration will be marked with scripts, so therefore we need two important basic configurations:

1. no ip domain-lookup
2. exec-timeout 0 0 on console

Both configurations are already preconfigured on all switches and routers, so do not change these configurations.

Instructions to the Competitor

1. Read all tasks in each section before proceeding with any configuration. The completion of any item may require the completion of any previous or later item.
2. Points are awarded for working configurations only. Test the functionality of all the requirements before you submit the test project. Be careful, because as you configure one part, you may break a previous requirement or configuration.
3. No partial points can be granted for any aspect; all requirements need to be fulfilled to receive the points for the aspect. Some requirements depend on other aspect's requirements, either before or after the current aspect.
4. Save your configurations frequently; accidents do and will happen.
5. All virtual machines are pre-installed. Use **admin\Skill39** local credentials to access windows virtual machines and **root\Skill39** to access linux virtual machines. Do not change these passwords.
6. Hosts are preconfigured but check the configuration and change it when necessary.
7. Please use industrial best practice where possible!

Equipment, machinery, installations, and materials required

It is expected that all Test Projects can be completed by Competitors based on the equipment and materials specified in the Infrastructure List.

Marking Scheme

According to the WorldSkills Standards Specifications within current Technical Description all marks for this test project module fall into section 7 «Configuring network devices» which has a maximum mark of 25.

Basic configuration

1. Configure hostnames for all network devices as you see on the topology.
2. Configure domain name **wsc2022.net** for all network devices on the topology.
3. Configure **Skill39** as a privileged mode password for all devices.
4. Only PBKDF2 hash of the password should be stored in configuration.
5. Configure IPv4/IPv6 address for all network devices as you see on the topology.
6. Configure KST +9 as timezone for all network devices.
7. On HQ1 and BR2 configure automatic config backup. Config should be written to "/srv/tftp/cisco/" on local device, with the name of the hostname + time and the ".save" extension.

Switching

1. Configure VTP on all switches to synchronize VLANs. It should be possible to modify VLAN database only from DSW1, and VLAN databases of all the other switchies should be synchronized from DSW1. VLAN database on all switches should contain following VLANs.

   (a) VLAN 10 with name SRV
   (b) VLAN 20 with name CLI

2. Configure all links between switches as trunk port.

   (a) Do not use dynamic negotiation protocol.
   (b) Configure manual pruning so that only created VLANs are allowed forwarding.

3. Configure EtherChannel between switches.

   (a) Use following port-channel numbers:

      (i) – between switches DSW1 and DSW2
      (ii) – between switches DSW1 and ASW1

   (b) 3 – between switches DSW2 and ASW2
   (c) The aggregated channel between DSW1 and DSW2 do not use dynamic negotiation protocol.
   (d) The aggregated channel between DSW1 and ASW1 use a Cisco proprietary protocol for dynamic negotiation.
   (e) The aggregated channel between DSW2 and ASW2 use a standard protocol for dynamic negotiation.
   (f) DSW1 and DSW2 should initiate negotiation and the other devices should respond but don’t initiate.
   (g) Configure the load balancing and forwarding method with source and destination MAC address.

4. Spanning tree configuration.

   (a) DSW1 should be root bridge of VLAN10. If DSW1 goes down DSW2 should take over as the root bridge.
   (b) DSW2 should be root bridge of VLAN20. If DSW2 goes down DSW1 should take over as the root bridge.
   (c) The traffic from HQ-CLI should pass through DSW1.
   (d) Configure port which is connected to end device so that it immediately begins forwarding when connected.

Routing

1. Configure EIGRP.

   (a) Make sure all virtual machines in the inside network can communicate with the others.
   (b) HQ1 and HQ2 should advertise only summarized route 192.168.0.0/16 to BR1 and BR2.

2. Configure BGP.

   (a) Use Loopback 0 interface for eBGP neighbor between AS 65001 and 65002.
   (b) Advertise all networks of internet public network (include Loopback interface) into BGP.
   (c) Add null route for networks needed to accomplish other tasks. Distribute them to BGP on HQ1 and HQ2.

3. Configure OSPFv3 on HQ site.

   (a) Ensure there is no DR or BDR election on the link between routers and switches.
   (b) Enable authentication in area 2022. Use the 512-bit SHA algorithm and the authentication key **Skill39**.
   (c) HQ-SRV should be able to connect to DC-SRV using IPv6.

4. Configure load balancing for traffic. (Only IPv4)

   (a) Configure traffic balancing between HQ site and internet so that the channel through HQ1 is preferred.
   (b) Configure traffic balancing between HQ site and BR sites so that the channel through HQ2 is preferred. If HQ2 goes down, the channel through HQ1 is used.

Services

1. Configure NAT.

   (a) When HQ-CLI communicate with internet, these IP address should be translated to 98.76.12.1-98.76.12.10
   (b) When BR-CLI1 and BR-CLI2 communicate with internet, these IP address should be translated to IPv4 address of the interface which is connected to ISP on each router.
   (c) The internet clients can access to DNS and HTTP on DC-SRV via IPv4 address of outside interface on FW1.

2. Configure DHCP.

   (a) HQ-CLI, BR-CLI1 and BR-CLI2 can obtain IP address automatically.
   (b) All DHCP clients should use **DC-SRV** as DNS server.

3. Configure FHRP on DSW1 and DSW2.

   (a) Use Hot Standby Router Protocol v2 for VLAN 10.

      (i) DSW1 should be used as default gateway.
      (ii) Use 104 as group number of IPv4, and 106 as group number of IPv6.
      (iii) Use **192.168.10.254** as virtual IPv4 address and **2001:624C:3201:10::254** as virtual IPv6 address.
      (iv) HQ-SRV should use this VIP as default gateway.

   (b) Use a Hot Standby Router Protocol v2 for VLAN 20.

      (i) DSW2 should be used as default gateway.
      (ii) Use 204 as group number of IPv4, and 206 as group number of IPv6.
      (iii) Use **192.168.20.254** as virtual IPv4 address and **2001:624C:3201:20::254** as Virtual IPv6 address.
      (iv) HQ-CLI should use this VIP as default gateway.

4. Configure remote monitoring using SNMP on HQ1, HQ2 and FW1.

(a) Configure device location **Ilsan, Korea**
(b) Configure system contact **admin@wsc2022.net**
(c) Cacti monitoring server is pre-configured on HQ-SRV. You can use it to check weather SNMP is working correctly or not via http://192.168.10.1/cacti (username: admin, password: Skill39)
(d) In Cacti, there is a template only for FW1 configured, so you have to configure templates for HQ1 and HQ2 too.

5. Configure ISP as NTP server. All network devices should synchronize time from ISP.

Security

1. Configure console authentication on all network devices.

   (a) Use local account. Create user **admin** with password **Skill39**.
   (b) After successful authentication, users should automatically land in priviledged mode (except FW1)

2. Configure SSH version 2 for remote access on HQ1 and HQ2.

   (a) Use RADIUS server for authentication.

   (i) Use HQ-SRV as RADIUS server.
   (ii) Use **Skill39** as the shared key.
   (iii) Test RADIUS authentication using following users with password **Skill39**:

   username **user1** with maximum priviledge level
   username **user2** with priviledge level 5

   (b) User **user2** should be able to configure any interface IP settings and administratively enable or disable any of these interfaces.
   (c) If RADIUS server goes down, use local account as backup authentication method.
   (d) Ensure only HQ-CLI is allowed to access via SSH.

3. Configure port-security on the port which is connected to HQ-CLI using following parameters:

   (a) Maximum MAC address – 2
   (b) In case of policy violation, security message should be displayed on the console, port should be disabled.
   (c) Recover disabled port after 3 minutes.

4. Configure DHCP snooping for VLAN 20 on ASW2.

WAN and VPN

1. Configure ISP as PPPoE server and BR1 as PPPoE client.

   (a) Use CHAP for authentication with **chapuser/Skill39** credential.
   (b) Use suitable authentication.

2. Configure tunnels between HQ1, HQ2, BR1 and BR2.

   (a) Use Loopback interface as tunnel source interface on each router.
   (b) HQ and BRANCH sites should be able to communicate each other through this tunnel.

3. Configure fast and secure tunnel between HQ1 and FW1.

   (a) Make sure HQ-CLI, BR-CLI1 and BR-CLI2 can communicate with DC-SRV.

4. Configure a remote access connection between VPN on FW1.

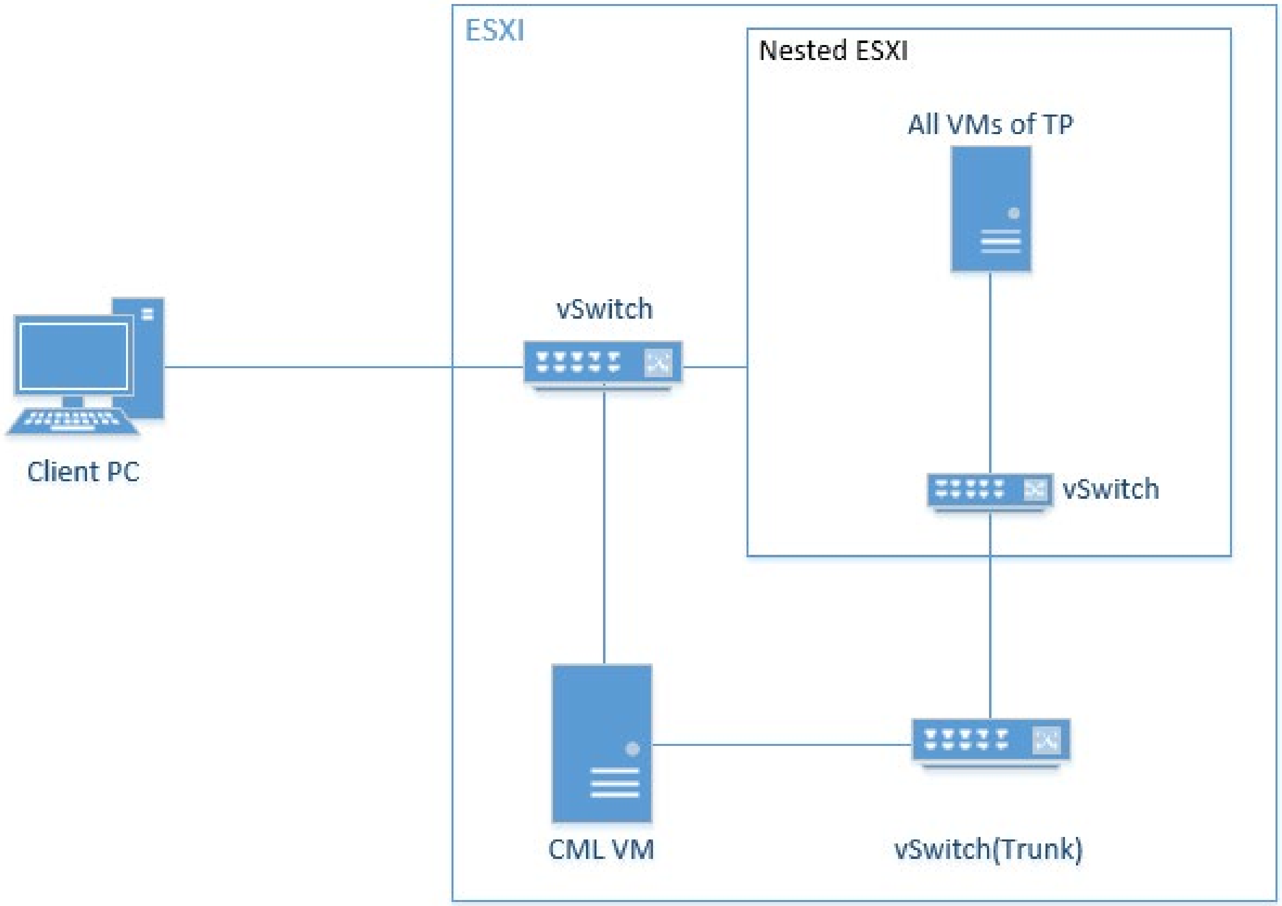
   (a) Create local user **vpnuser** with password **Skill39** on FW1.
   (b) Make sure VPN client can communicate with DC-SRV and HQ-SRV.
   (c) After vpn client is connected, client should use internal address of **DC-SRV** as DNS server
   (d) Necessary images can be found on your Workstation on desktop.
   (e) Please check, if the preconfigured IPv6 interface-IP on DC-SRV is set correct to 2001:624C:3201:100::1/64

Configuration Table

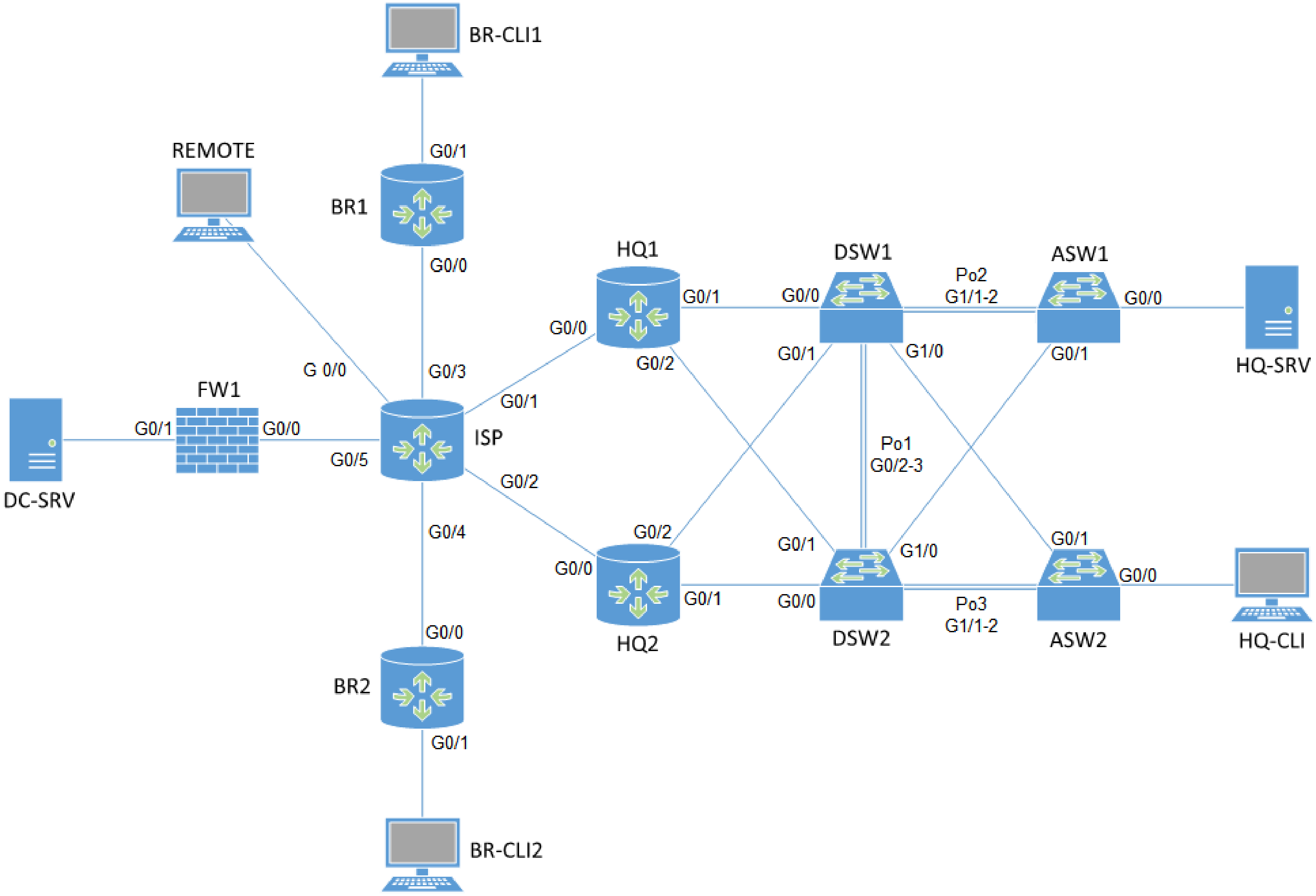
Site	Device	Interface	Address
Internet	ISP	Loopback0	8.8.8.8/32
		GigabitEthernet0/0	98.76.54.254/24
		GigabitEthernet0/1	98.76.1.254/24
		GigabitEthernet0/2	98.76.2.254/24
		GigabitEthernet0/3	98.76.3.254/24
		GigabitEthernet0/4	98.76.4.254/24
		GigabitEthernet0/5	98.76.5.254/24
	REMOTE	Ethernet 0	98.76.54.1/24
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

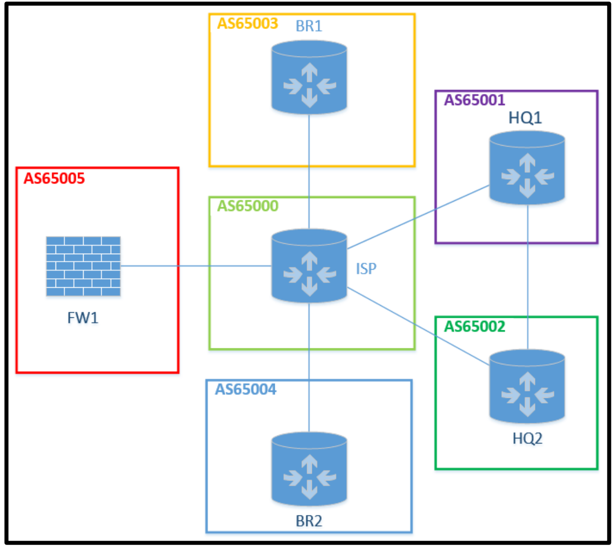
Physical Diagram

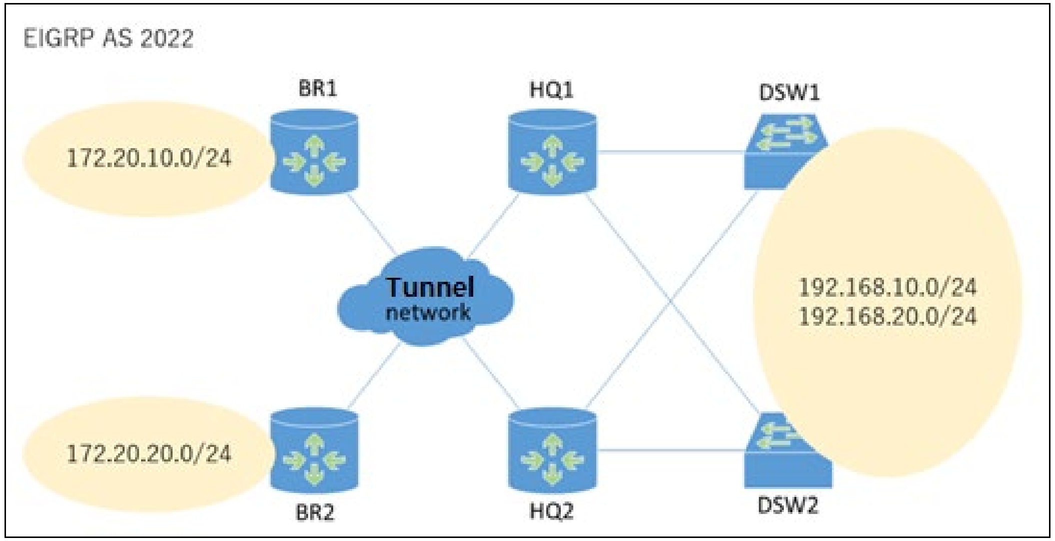


Network Topology

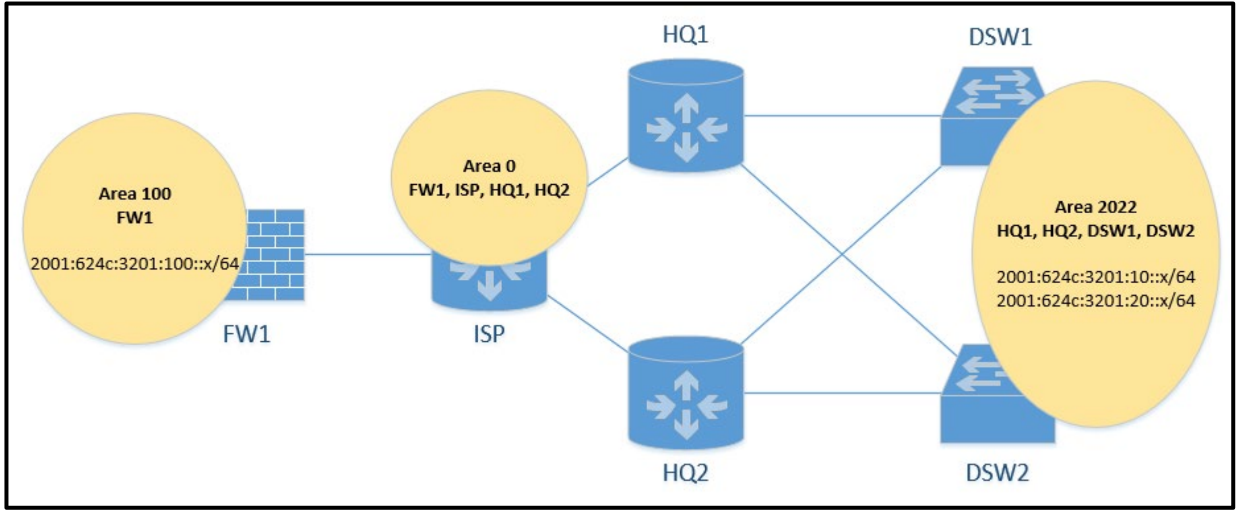


IPv4 Routing Topology





IPv6 Routing Topology


HQ1
DSW1
Area 100
FW1
2001:624c:3201:100::x/64
Area 0
FW1, ISP, HQ1, HQ2
Area 2022
HQ1, HQ2, DSW1, DSW2
2001:624c:3201:10::x/64
2001:624c:3201:20::x/64
FW1
ISP
HQ2
DSW2