

Test Project

Module C Networking Environment

IT Network Systems Administration

Independent Test Project Designer: Rasika Nayanajith Manannalage, Bai Qing

Independent Test Project Validator: Kravitz Hwang SCM

Contents

Introduction to Test Project.....	3
Introduction	3
Description of project and tasks	3
Physical Topology	4
Logical Topology	7
Routing Topology.....	8
Instructions to the Competitor	9
Configuration Tasks	9
Basic Configurations	9
L2 Services	15
EIGRP	16
OSPF	16
BGP	17
IP Services	19
Security and VPN	19

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
- Other

Introduction

In today's IT landscape, proficiency in network technology is increasingly vital for individuals aspiring to excel in any IT engineering discipline. This test project presents numerous challenges drawn from real-world scenarios, focusing predominantly on IT Networking and Integration. Successfully completing this project with a high score demonstrates your readiness to manage network infrastructures for multi-branch enterprises.

Description of project and tasks

This test project is designed using a variety of network technologies that should be familiar to those who have studied for Cisco **ENARSI** (Implementing Cisco Enterprise Advanced Routing and Services) certification track. In addition to the knowledge gained from this certification track, you are expected to have **CCNA** - Implementing and Administering Cisco Solutions certification knowledge to complete this Test Project.

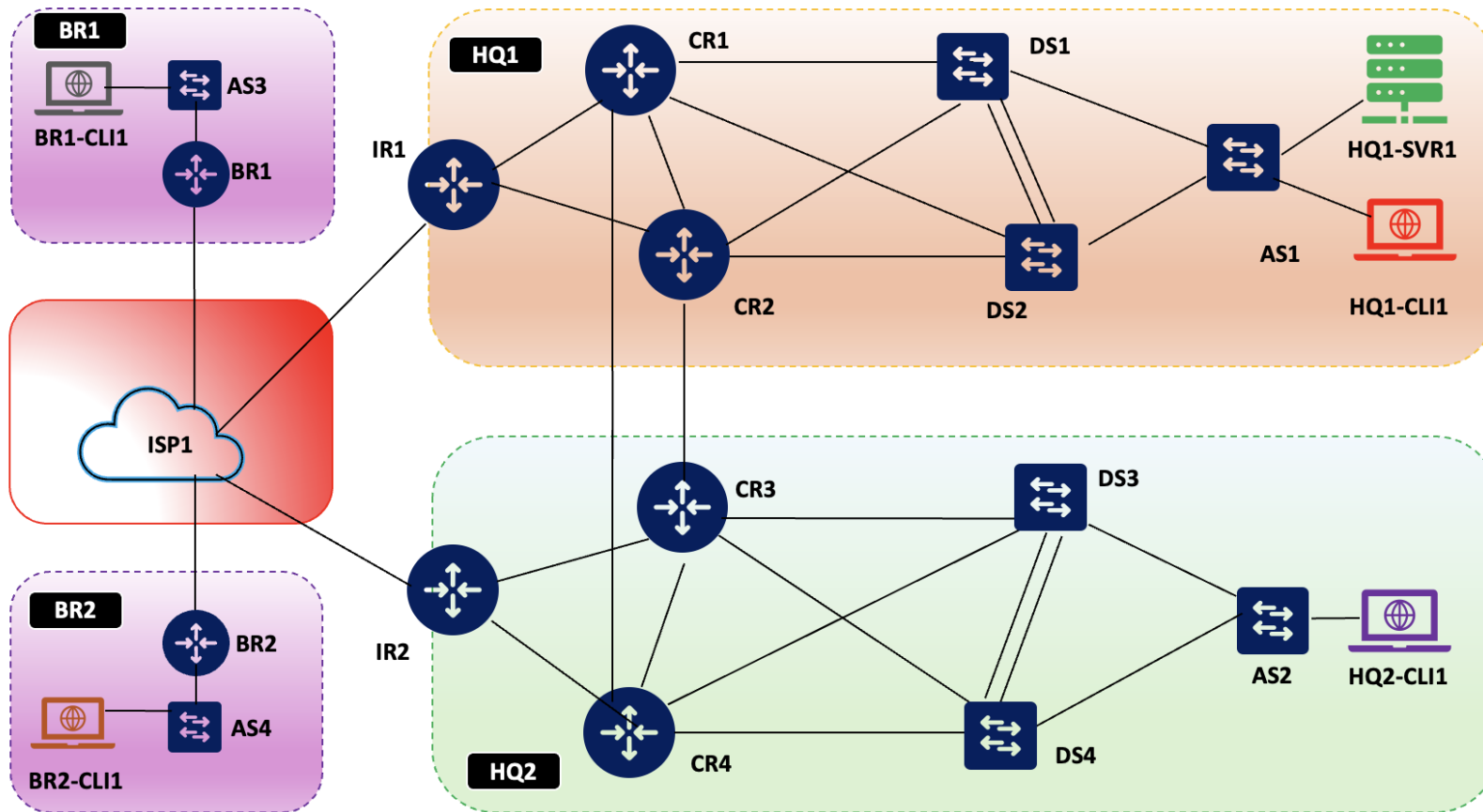
Configuration tasks are broken down into seven areas given below expanded in section Instructions to the Competitors. Percentage shows the distribution of marks to each area.

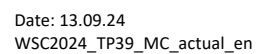
- Basic configuration [10%]
- L2 services [15%]
- OSPF [15%]
- EIGRP [15%]
- BGP [15%]
- IP Services [15%]
- VPN and Security [15%]

Physical Topology

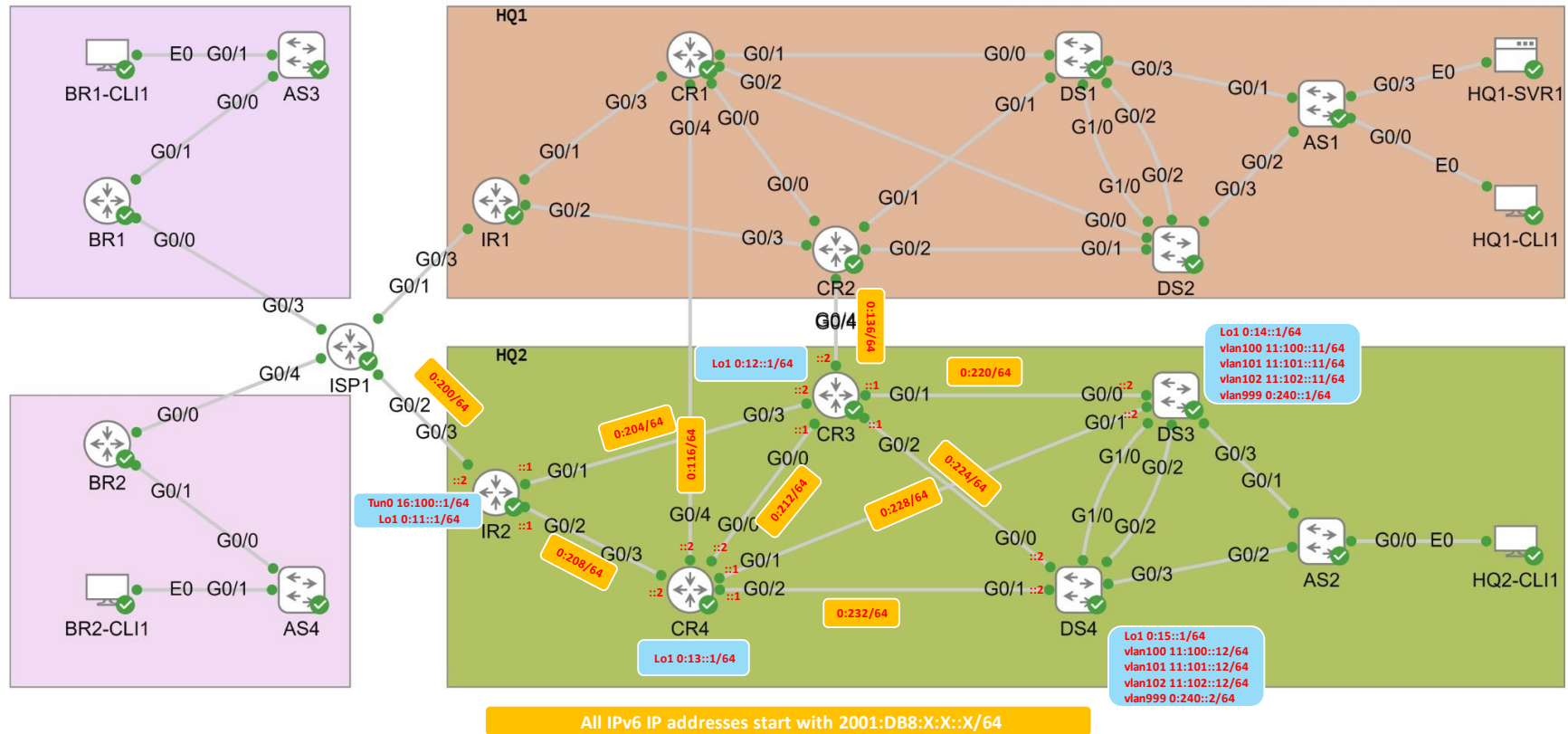
Below is the physical topology of the Test Project.

WSC2024_TD39_Physical_Topology





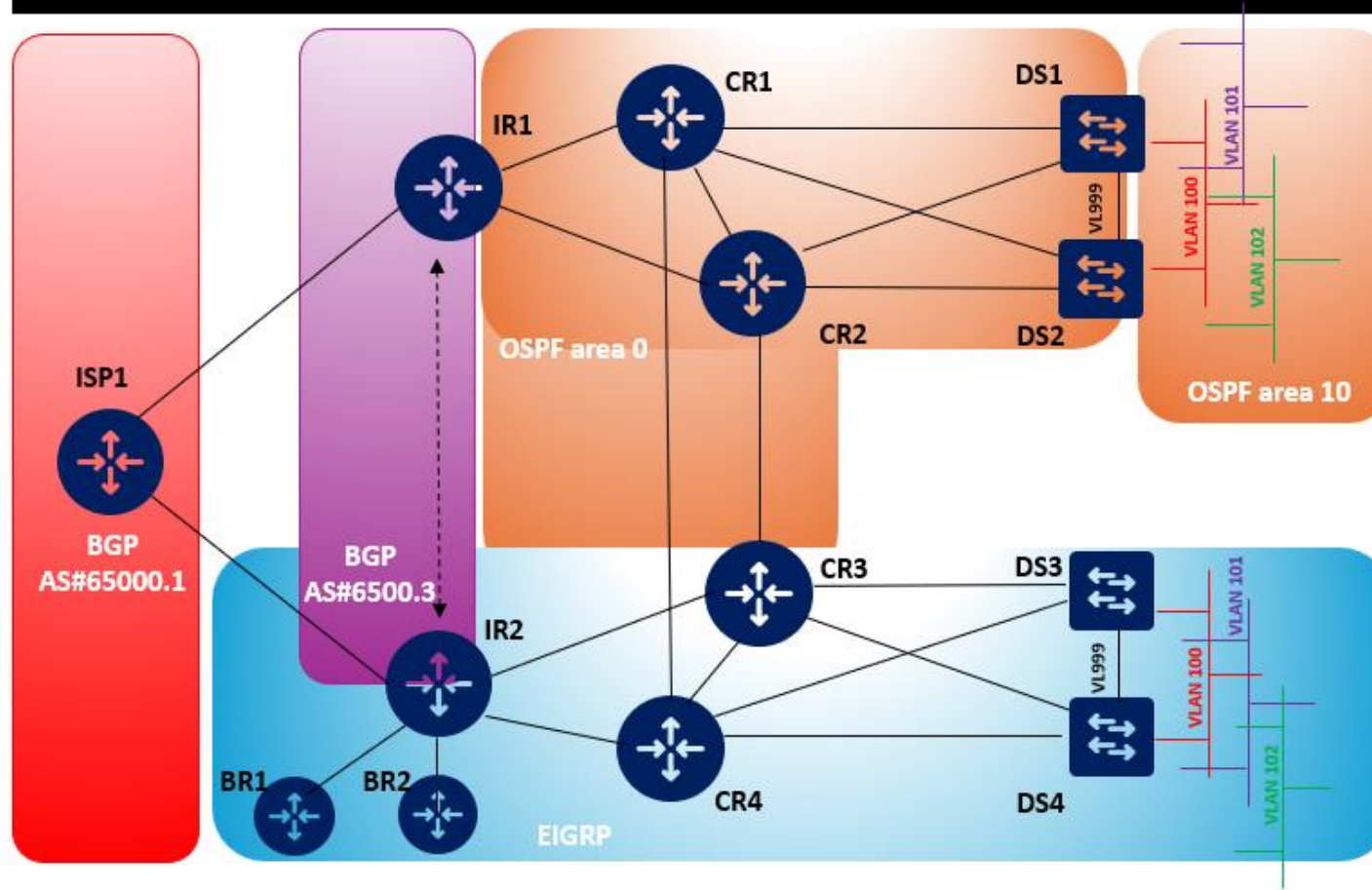
WSC2024_TD39_Physical_Topology



Logical Topology

Logical Network Topology is as shown below.

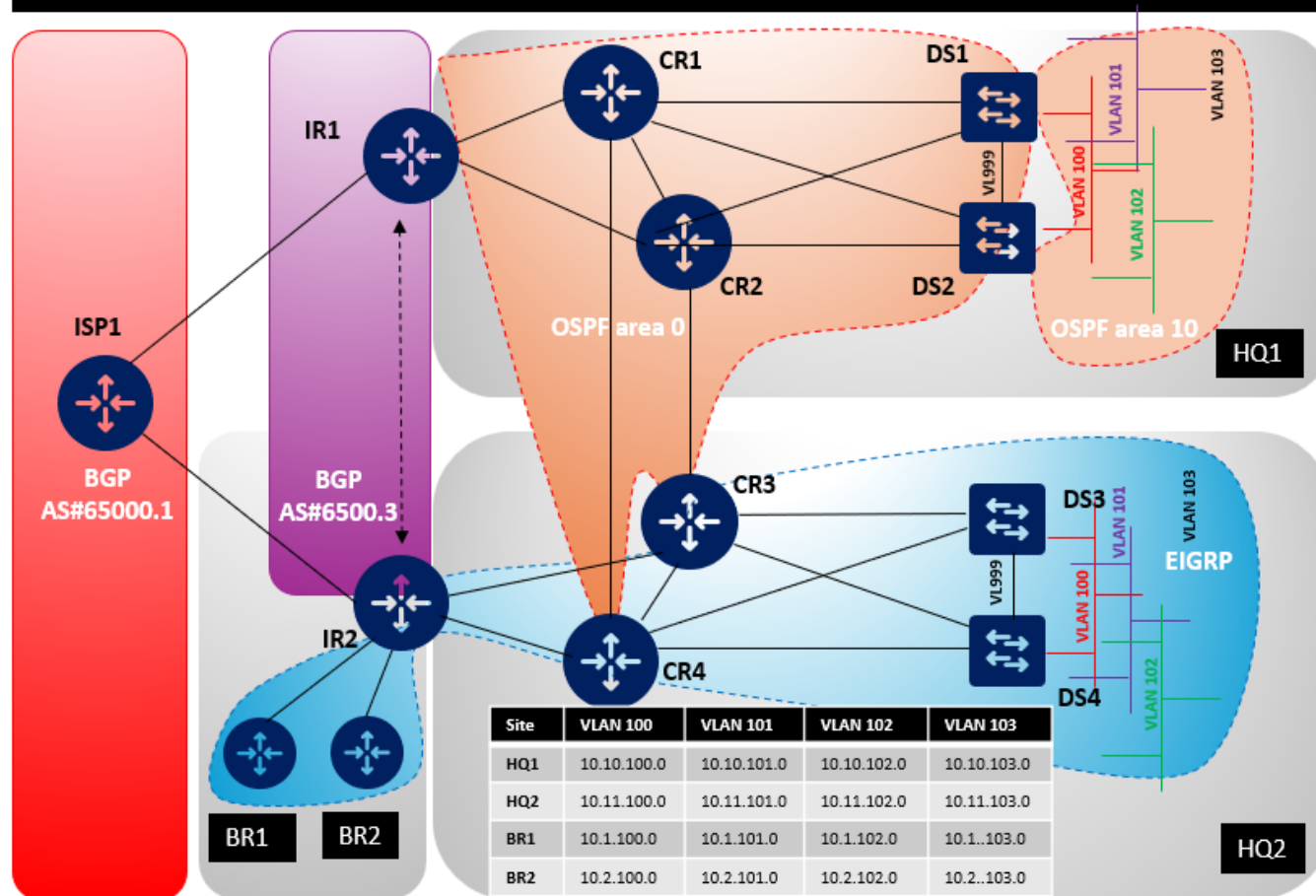
WSC2024_TD39_Logical_Topology



Routing Topology

BGP, EIGRP, and OSPF Routing topology is shown below.

WSC2024_TD39_Routing Topology



Instructions to the Competitor

Please carefully read below instruction.

1. Please do not modify ISP1's configuration. All ISP1 configurations are completed, and you are not supposed to touch that device.
2. Your configuration will be marked with scripts, so therefore we need two important basic configurations:
 - (a) no ip domain lookup
 - (b) exec-timeout 0 0 on console
 Both configurations are already preconfigured on all routers and switches. So please do not change these configurations.
3. 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.
4. 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.
5. 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.
6. Save your configurations frequently; accidents do and will happen.
7. All Clients (HQ1-CLI1, HQ2-CLI, BR1-CLI1, BR2-CLI1) and Server (HQ1-SVR1) can be accessible with **admin\Skill39@Lyon** credentials. Do not change these passwords.
8. Hosts are preconfigured but check the configuration and change it when necessary.
9. If you disabled any interfaces for testing, ensure that all of them are enabled before submitting your Test Project.
10. No static route configurations are allowed unless it is automatically generated as part of your OSPF/EIGRP configurations.
 - (a) There is one exception when you are configuring BR1 and BR2 in Task 2 of "Security and VPN" section.

Configuration Tasks

Basic Configurations

1. Please configure IPv4 address for DS1-4, AS1-4 and BR1-2 devices in the topology.
 - (a) IR1-2 and CR1-4 interfaces configuration already done for you.

DEVICE	INTERFACE	IPv4 ADDRESS	NEIGHBOR
ISP1	GigabitEthernet0/1	192.0.2.101/28	IR1
ISP1	GigabitEthernet0/2	192.0.2.201/28	IR2
ISP1	GigabitEthernet0/3	192.0.2.1/30	BR1
ISP1	GigabitEthernet0/4	192.0.2.5/30	BR2
ISP1	Loopback100	198.51.100.1/24	N/A

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
ISP1	Loopback200	203.0.113.1/24	N/A
IR1	GigabitEthernet0/1	10.10.0.105/30	CR1
IR1	GigabitEthernet0/2	10.10.0.109/30	CR2
IR1	GigabitEthernet0/3	192.0.2.102/28	ISP1
IR1	Loopback1	10.10.0.1/32	N/A
IR2	GigabitEthernet0/1	10.10.0.205/30	CR3
IR2	GigabitEthernet0/2	10.10.0.209/30	CR4
IR2	GigabitEthernet0/3	192.0.2.202/28	ISP1
IR2	Tunnel0	172.16.100.1/24	BR1/BR2
IR2	Loopback1	10.10.0.11/32	N/A
CR1	GigabitEthernet0/0	10.10.0.113/30	CR2
CR1	GigabitEthernet0/1	10.10.0.121/30	DS1
CR1	GigabitEthernet0/2	10.10.0.125/30	DS2
CR1	GigabitEthernet0/3	10.10.0.106/30	IR1
CR1	GigabitEthernet0/4	10.10.0.117/30	CR4
CR1	Loopback1	10.10.0.2/32	N/A
CR2	GigabitEthernet0/0	10.10.0.114/30	CR1
CR2	GigabitEthernet0/1	10.10.0.129/30	DS1
CR2	GigabitEthernet0/2	10.10.0.133/30	DS2
CR2	GigabitEthernet0/3	10.10.0.110/30	IR1
CR2	GigabitEthernet0/4	10.10.0.137/30	CR3
CR2	Loopback1	10.10.0.3/32	N/A
CR3	GigabitEthernet0/0	10.10.0.213/30	CR4
CR3	GigabitEthernet0/1	10.10.0.221/30	DS3
CR3	GigabitEthernet0/2	10.10.0.225/30	DS4

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
CR3	GigabitEthernet0/3	10.10.0.206/30	IR2
CR3	GigabitEthernet0/4	10.10.0.138/30	CR2
CR3	Loopback1	10.10.0.12/32	N/A
CR4	GigabitEthernet0/0	10.10.0.214/30	CR3
CR4	GigabitEthernet0/1	10.10.0.229/30	DS3
CR4	GigabitEthernet0/2	10.10.0.233/30	DS4
CR4	GigabitEthernet0/3	10.10.0.210/30	IR2
CR4	GigabitEthernet0/4	10.10.0.118/30	CR1
CR4	Loopback1	10.10.0.13/32	N/A
DS1	GigabitEthernet0/0	10.10.0.122/30	CR1
DS1	GigabitEthernet0/1	10.10.0.130/30	CR2
DS1	Loopback1	10.10.0.4/32	N/A
DS1	Vlan100	10.10.100.11/24	N/A
DS1	Vlan101	10.10.101.11/24	N/A
DS1	Vlan102	10.10.102.11/24	N/A
DS1	Vlan103	10.10.103.11/24	N/A
DS1	Vlan999	10.10.0.141/30	DS2
DS2	GigabitEthernet0/0	10.10.0.126/30	CR1
DS2	GigabitEthernet0/1	10.10.0.134/30	CR2
DS2	Loopback1	10.10.0.5/32	N/A
DS2	Vlan100	10.10.100.12/24	N/A
DS2	Vlan101	10.10.101.12/24	N/A
DS2	Vlan102	10.10.102.12/24	N/A
DS2	Vlan103	10.10.103.12/24	N/A
DS2	Vlan999	10.10.0.142/30	DS2

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
DS3	GigabitEthernet0/0	10.10.0.222/30	CR3
DS3	GigabitEthernet0/1	10.10.0.230/30	CR4
DS3	Loopback1	10.10.0.14/32	N/A
DS3	Vlan100	10.11.100.11/24	N/A
DS3	Vlan101	10.11.101.11/24	N/A
DS3	Vlan102	10.11.102.11/24	N/A
DS3	Vlan103	10.11.103.11/24	N/A
DS3	Vlan999	10.10.0.241/30	DS4
DS4	GigabitEthernet0/0	10.10.0.226/30	CR3
DS4	GigabitEthernet0/1	10.10.0.234/30	CR4
DS4	Loopback1	10.10.0.15/32	N/A
DS4	Vlan100	10.11.100.12/24	N/A
DS4	Vlan101	10.11.101.12/24	N/A
DS4	Vlan102	10.11.102.12/24	N/A
DS4	Vlan103	10.11.103.12/24	N/A
DS4	Vlan999	10.10.0.242/30	DS3
AS1	Vlan103	10.10.103.1/24	N/A
AS2	Vlan103	10.11.103.1/24	N/A
BR1	GigabitEthernet0/0	192.0.2.2/30	ISP1
BR1	GigabitEthernet0/1.100	10.1.100.10/24	N/A
BR1	GigabitEthernet0/1.101	10.1.101.10/24	N/A
BR1	GigabitEthernet0/1.102	10.1.102.10/24	N/A
BR1	GigabitEthernet0/1.103	10.1.103.10/24	N/A
BR1	Loopback1	10.10.0.21/32	N/A
BR1	Tunnel0	172.16.100.11/24	IR2

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
AS3	Vlan103	10.1.103.1/24	N/A
BR2	GigabitEthernet0/0	192.0.2.6/30	ISP1
BR2	GigabitEthernet0/1.100	10.2.100.10/24	N/A
BR2	GigabitEthernet0/1.101	10.2.101.10/24	N/A
BR2	GigabitEthernet0/1.102	10.2.102.10/24	N/A
BR2	GigabitEthernet0/1.103	10.2.103.10/24	N/A
BR2	Loopback1	10.10.0.22/32	N/A
BR2	Tunnel0	172.16.100.12/24	IR2
AS4	Vlan103	10.2.103.1/24	N/A

2. Configure IPv6 addresses in HQ2 devices as per below table.

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
IR2	GigabitEthernet0/1	2001:DB8:0:204::1/64	CR3
IR2	GigabitEthernet0/2	2001:DB8:0:208::1/64	CR4
IR2	GigabitEthernet0/3	2001:DB8:0:200::2/64	ISP1
IR2	Tunnel0	2001:DB8:16:100::1/64	BR1
IR2	Loopback1	2001:DB8:0:11::1/64	N/A
CR3	GigabitEthernet0/0	2001:DB8:0:212::1/64	CR4
CR3	GigabitEthernet0/1	2001:DB8:0:220::1/64	DS3
CR3	GigabitEthernet0/2	2001:DB8:0:224::1/64	DS4
CR3	GigabitEthernet0/3	2001:DB8:0:204::2/64	IR2
CR3	Loopback1	2001:DB8:0:12::1/64	N/A
CR4	GigabitEthernet0/0	2001:DB8:0:212::2/64	CR3
CR4	GigabitEthernet0/1	2001:DB8:0:228::1/64	DS3
CR4	GigabitEthernet0/2	2001:DB8:0:232::1/64	DS4

DEVICE	INTERFACE	IPv4 ADDRESS	NEIGHBOR
CR4	GigabitEthernet0/3	2001:DB8:0:208::2/64	IR2
CR4	Loopback1	2001:DB8:0:13::1/64	N/A
DS3	GigabitEthernet0/0	2001:DB8:0:220::2/64	CR3
DS3	GigabitEthernet0/1	2001:DB8:0:228::2/64	CR4
DS3	Loopback1	2001:DB8:0:14::1/64	N/A
DS3	Vlan100	2001:DB8:11:100::11/64	N/A
DS3	Vlan101	2001:DB8:11:101::11/64	N/A
DS3	Vlan102	2001:DB8:11:102::11/64	N/A
DS3	Vlan999	2001:DB8:0:240::1/64	DS4
DS4	GigabitEthernet0/0	2001:DB8:0:224::2/64	CR3
DS4	GigabitEthernet0/1	2001:DB8:0:232::2/64	CR4
DS4	Loopback1	2001:DB8:0:15::1/64	N/A
DS4	Vlan100	2001:DB8:11:100::12/64	N/A
DS4	Vlan101	2001:DB8:11:101::12/64	N/A
DS4	Vlan102	2001:DB8:11:102::12/64	N/A
DS4	Vlan999	2001:DB8:0:240::2/64	DS3

3. Configure all routers and switches in HQ1, HQ2, BR1 and BR2 to use CET (UTC+1) timezone.

- (a) Make sure it considers summer time (start at 2:00 a.m. last Sunday of March and end at 3:00 a.m. last Sunday of October)

4. Configure domain name **wsc2024.net** for all devices in the topology.

5. Configure enable password **Skill39@Lyon** in all routers and switches. Also define local username admin with password Skill39@Lyon in all routers and switches. That user should have the highest privilege you can give.

- (a) Ensure all passwords use type 9 encryption (as shown below).

```
AS3(config)#do sh run | i admin | enable
username admin privilege 15 secret 9
$9$NOUZJkpL/2WNiv$PL9bus2.Tf90j8ZBwV1AwBfv/jPJFmmzmWtH0WUF2/Q
enable secret 9 $9$eXQkNfnt7wXC5f$wmtQW14ysBLUDV87oOrKy90eX8FXdYKP77JaEMr7ddo
```

L2 Services

1. Configure VTP domain “**WSC2024**” on DS1, DS2, DS3, DS4, AS1, AS2, AS3 and AS4. No VTP message propagation allowed in any of these switches.
2. Configure following VLANs across all distribution (DSx) and access switches (ASx) in this topology.

VLAN ID	VLAN NAME	DEVICES
100	SERVER	DS1, DS2, DS3, DS4, AS1, AS2, AS3, AS4
101	CLIENT_1	DS1, DS2, DS3, DS4, AS1, AS2, AS3, AS4
102	CLIENT_2	DS1, DS2, DS3, DS4, AS1, AS2, AS3, AS4
103	MGMT	DS1, DS2, DS3, DS4, AS1, AS2, AS3, AS4
999	L3_P2P	DS1, DS2, DS3, DS4

3. Configure STP to meet the requirements below
 - (a) In HQ1, DS1 should be the STP root bridge for all vlans (including future vlans) and DS2 should become the root bridge if DS1 is down.
 - (b) In HQ2, DS3 should be the STP root bridge for all vlans (including future vlans) and DS4 should become the root bridge if DS3 is down.
 - (c) These STP convergences require to happen as quickly as possible. Choose the right STP mode to achieve that outcome.
4. Configure all distribution switches (DS1-4) ports connect to AS1 and AS2 as trunk ports. Configure vlan 888 as native vlan across these trunk ports.
 - (a) Also configure AS3 and AS4 G0/0 interface as trunk ports. You can leave vlan 1 as native vlan for these trunk ports.
5. Configure a logical interface (use 12 for interface number) between DS1 and DS2 to pass all vlan across it. Assign physical interface G0/2 and G1/0 to it. You require to use LACP as protocol and both switches should be able to initiate the negotiation. Traffic should be loadbalance across both links based on source and detination IP addresses.
6. Configure a logical interface (use 34 for interface number) between DS3 and DS4 without using any dynamic negotiation. Assign G0/2 and G1/0 physical interface into logical interface.
7. Configure HSRP for the 4 vlans (100-103) to meet following conditions.
 - (a) In each subnet, default gateway IP address needs to be .10 in each /24 subnet. Use vlan number as HSRP group number when configuring.
 - (b) DS1 should be the HSRP active for HQ1 and DS3 should be the HSRP active for HQ2.
 - (c) In case of active device (DS1 or DS3) goes down DS2 or DS4 should act as active device in each site. When DS1 or DS3 comes back after failure, it should take over HSRP active role once it is operational.
8. In HQ2, configure IPv6 HSRP for vlan 101 and 102 on DS3 and DS4.
 - (a) Use group number 1101 for vlan 101 and group number 1102 for vlan 102.
 - (b) HSRP virtual IPv6 address should be FE80::10 for both vlans.
 - (c) DS3 should be the HSRP active device and DS4 should be the standby Device

EIGRP

Configure EIGRP protocol in HQ2 (IR2, CR3, CR4, DS3 and DS4 devices) to achieve the following requirements. You will be asked to configure EIGRP on BR1 and BR2 as part of section “Security and VPN”

1. Configure an EIGRP process in each of those devices where you can enable both IPv4 and IPv6 under same EIGRP instance. You need to use the name “**WSC2024**” for this EIGRP configuration. Do not enable EIGRP on interfaces connecting to CR1 and CR2 in HQ1.
2. For IPv4, use autonomous system number 100. Make sure loopback 1 IP address become EIGRP router-id.
3. Advertise all loopback and /30 P2P (point-to-point/) networks into EIGRP on IR2, CR3, CR4, DS3 and DS4. Advertise vlan 100-103 networks into EIGRP in DS3 and DS4.
4. By default, all EIGRP hello messages should be suppressed in all interfaces. Only enable it on interfaces where EIGRP adjacencies required.
5. IR2 to advertise default route into EIGRP if it receives a default route from ISP1 via BGP.
6. Modify administrative distance of external EIGRP learned route to 100 on CR3 and CR4.
7. On Router CR3 and CR4, summarize HQ2 vlan 100-103 subnets and advertise it via EIGRP to IR2.
8. Configure EIGRP on IPv6 on HQ2
 - (a) Use same EIGRP instance WSC2024 configured in the above
 - (b) Use autonomous system number 100 for IPv6 as well.
 - (c) On DS3 and DS4, IPv6 EIGRP adjacencies should not be established across vlan 100,101,102 or vlan 103.
 - (d) Verify you can ping IR2 loopback 1 address (2001:DB8:0:11::1/64) from HQ2-CLI1.

OSPF

Configure OSPF protocol in HQ1 (IR1, CR1, CR2, DS1 and DS2 devices) to achieve the following requirements.

1. Configure OSPF process 100 in each of those devices. Use Loopback 1 interface as router-id in each of those devices.
2. Advertise all /30. P2P links and Loopback 1 interfaces to OSPF area 0.
3. DS1 and DS2, configure vlan 100-103 network in OSPF area 10.
4. OSPF hello messages should be only sent via /30 networks where devices are interconnected.
5. When establish OSPF adjacencies, devices should not elect DR/BDR
6. Ensure IR1 is advertise default route to other OSPF routers if it receives a default route from ISP1. This should appear as Type 2 route with metric value of 5000.
 - (a) Advertise a default route into OSPF on CR4 with metric value 4000.
 - (b) CR4 should inject the default route into OSPF only if 10.10.0.208/30 network (ie G 0/3 interface is up) on their routing table
7. Configure mutual route redistribution between EIGRP and OSPF on CR3 and CR4 so that HQ1 can access HQ2 subnets (vice-versa)
 - (a) Define IP prefix lists “**HQ1-SUBNETS**” and “**HQ2-SUBNETS**” to include loopback IPs, P2P and vlan100-103 IPs in HQ1 and HQ2.
 - (b) When HQ2 routes go into OSPF they should come with tag value 34.
 - (c) When HQ1 routes go into EIGRP they should come with tag value 12.
 - (d) Prevent any routing loops while performing mutual route-redistribution.
8. Configure OSPF summary routes on ABR and ASBR routers only 10.10.100.0/22 route being advertised.

9. After configuring the routing for BR1 and BR2 (sec 3.7.1-3.7.3), ensure that summary routes (10.1.100.0/22 and 10.2.100.0/22) and loopback addresses (10.10.0.21 and 10.10.0.22) are available on HQ1 devices OSPF routing table (like sample output shown below).

```
DS1#sh ip route | in 10.10.0.21/32
O E2   10.10.0.21/32 [110/20] via 10.10.0.121, 00:04:31, GigabitEthernet0/0
DS1#sh ip route | in 10.10.0.22/32
O E2   10.10.0.22/32 [110/20] via 10.10.0.121, 00:04:37, GigabitEthernet0/0
DS1#sh ip route | in 10.1.100
O E2   10.1.100.0/22 [110/20] via 10.10.0.121, 00:04:41, GigabitEthernet0/0
DS1#sh ip route | in 10.2.100
O E2   10.2.100.0/22 [110/20] via 10.10.0.121, 00:03:39, GigabitEthernet0/0
```

BGP

Configure the BGP protocol on IR1 and IR2 routers to meet the given requirements. The IP addresses of service provider (ISP1) WAN links (in the 192.0.2.x/24 range) should not be advertised to any routers other than those locally connected (IR1, IR2, BR1 and BR2)

1. Configure eBGP sessions on IR1 and IR2 (both in AS#65000.3) with ISP router G0/1 and G0/2 IPs (192.0.2.101 and 192.0.2.201 IPs). Note that ISP router already configured with following settings.
 - (a) Keepalive interval 10s and Holddown time of 30s
 - (b) Authentication password **Skill39@Lyon**
2. Configure an iBGP peer group named “**WSC2024**” on on IR1 and IR2 to establish iBGP peering among themselves. It requires following settings.
 - (a) Keepalive interval 10s and Holddown time of 30s
 - (b) Authenticate each iBGP sessions with password **Skill39@Lyon**
 - (c) BGP peering to use loopback1 interface IP
3. Advertise 10.10.100.0/22 and 10.11.100.0/22 routes into BGP on IR1 and IR2.
 - (a) ISP should not receive any accidental routes from IR1 or IR2 other than above summary routes (use a route-map named **ISPV4_EXPORT** to control it)
4. Configure BGP on IR1 and IR2 such a way all internet traffic is going out via IR2 as primary path and only go via IR1 in case of a failure in the primary path.
 - (a) Use “local preference” BGP attribute to achieve this task.
5. Configure BGP on IR1 and IR2 such a way all incoming internet traffic come via IR2 as primary path and come via IR1 in case of a failure in the primary path.
 - (a) ISP1 will not accept any routes that got “AS-PATH” prepending. Therefore, use another BGP attribute to achieve this task.
6. On IR1 and IR2, you receive prefixes 198.51.100.0/24 and 203.0.113.0/24 from ISP1. You are required to configure IR1 as primary path (incoming and outgoing) for reaching to these prefixes from HQ1 and HQ2.
 - (a) You can use “198.51.100.1” and “203.0.113.1” IP addresses for reachability testing (ping and traceroute) from HQ-CLI1 and HQ2-CLI1.
7. Verify internet traffic is working in a scenario of failing primary internet router (IR2).
 - (a) Simulate a failure of IR2 by shutting down G 0/3 interfaces of CR3 and CR4.

```
CR3(config)#int g0/3
```

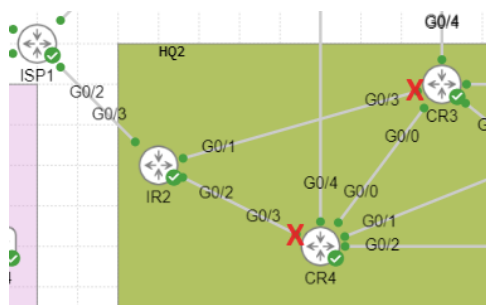
```
CR3(config-if)#shut
```

```
!
```

```
CR4(config)#int g0/3
```

```
CR4(config-if)#shut
```

```
!
```



- (b) Ping 8.8.8.8 from HQ1-CLI1 and ensure that it is successful. Traceroute output should confirm traffic go via IR1

```
HQ1-CLI1:~$ traceroute 8.8.8.8
```

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 46 byte packets
```

```
1 10.10.101.11 (10.10.101.11) 8.110 ms 6.477 ms 6.440 ms
2 10.10.0.142 (10.10.0.142) 9.587 ms 12.553 ms 8.434 ms
3 10.10.0.125 (10.10.0.125) 7.655 ms 14.774 ms 7.074 ms
4 10.10.0.105 (10.10.0.105) 11.138 ms 16.037 ms 9.988 ms
5 192.0.2.101 (192.0.2.101) 11.284 ms 25.961 ms *
```

- (c) Ping 8.8.8.8 from HQ2-CLI1 and ensure that it is successful. Traceroute output should confirm traffic go via IR1

```
HQ2-CLI1:~$ traceroute 8.8.8.8
```

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 46 byte packets
```

```
1 10.11.102.11 (10.11.102.11) 4.603 ms 6.894 ms 5.212 ms
2 10.10.0.221 (10.10.0.221) 9.680 ms 8.064 ms 9.047 ms
3 10.10.0.137 (10.10.0.137) 9.039 ms 10.686 ms 8.120 ms
4 10.10.0.109 (10.10.0.109) 8.147 ms 15.148 ms 8.367 ms
5 192.0.2.101 (192.0.2.101) 19.074 ms 19.037 ms *
```

If steps **b** and **c** above are not successful, fix that issue.

IP Services

You have been asked to configure following IP services.

1. When vlan 101-102 users (~400 in total users and require simultaneous internet access) in HQ1, HQ2, BR1 and BR2 communicate with internet (You can use 8.8.8.8 IP for testing) their addresses should be translated to following addresses depend on the internet router it goes through.
 - (a) Traffic goes via IR1 -> 192.0.2.104 -192.0.2.110
 - (b) Traffic goes via IR2 -> 192.0.2.193 -192.0.2.199
2. When HQ1-SVR1 with IP address 10.10.100.101 goes to internet it should appear as 192.0.2.99 or 192.9.2.205 depend on if traffic goes via IR1 or IR2 respectively. You can configure AS1 G0/3 to vlan 100 to test this configuration.
 - (a) HQ-SVR1 has already configured with 10.10.100.101 statically.
3. IR1 and IR2 should get its time from ISP1 peering address (192.0.2.101 and 192.0.2.201).
 - (a) All other devices in HQ1, HQ2, BR1 and BR2 should use IR1 (10.10.0.1) and IR2 (10.10.0.11) as their NTP servers.
 - (b) Use loopback address for NTP communication with IR1 and IR2. (Except AS1 to AS4 where you can use SVI 103 IP)
4. Configure DHCP services on DS1 and DS3 to meet requirements below.
on DS1
 - (a) VL101 DHCP address scope 10.10.101.101-10.10.101.254 with default router of 10.10.101.10
 - (b) VL102 DHCP address scope 10.10.102.101-10.10.102.254 with default router of 10.10.102.10
on DS3
 - (c) VL101 DHCP address scope 10.11.101.101-10.11.101.254 with default router of 10.11.101.10
 - (d) VL102 DHCP address scope 10.11.102.101-10.11.102.254 with default router of 10.11.102.10
5. Configure DHCP services BR1 and BR2 in a way clients BR1-CLI1 get IP address from vlan 101 and BR2-CLI1 get IP address from vlan 102.
 - (a) BR1- VL101 DHCP address scope 10.1.101.101-10.1.101.254 with default-gateway 10.1.101.10.
 - (b) BR2- VL102 DHCP address scope 10.2.102.101-10.2.102.254 with default-gateway 10.2.102.10.
6. Configure DS3 to give IPv6 addresses to clients on vlan 102 in HQ2.

Security and VPN

Multiple branch sites need to connect to the HQ2 network. To test the new connectivity, BR1 & BR2 have been required to configure as DMVPN spoke site with IR2 router in HQ2.

1. Configure IR2 as DMVPN Hub for branch sites connectivity. You require to consider below when configuring IR2.
 - (a) Use network-id **2024**.
 - (b) Tunnel interface 0 to use 172.16.100.1/24 IP address.
 - (c) Use string **WSC2024** to identify NHRP domain when establishing VPN connectivity.

2. Configure BR1 & BR2 as DMVP Spoke sites.

(a) You are allowed to add following static routes in BR1 and BR2

BR1

ip route 192.0.2.96 255.255.255.240 192.0.2.1

ip route 192.0.2.192 255.255.255.240 192.0.2.1

BR2

ip route 192.0.2.96 255.255.255.240 192.0.2.5

ip route 192.0.2.192 255.255.255.240 192.0.2.5

(b) BR1 tunnel interface 0 to use 172.16.100.11/24 IP address.

(c) BR2 tunnel interface 0 to use 172.16.100.12/24 IP address.

(d) BR1 and BR2 should establish dynamic tunnel between them when communicating each other.

3. Configure EIGRP between BR1, BR2 and IR2.

(a) BR1 and BR2 to advertise a summary route for networks corresponds to vlan 100-103 networks at that site.

4. Enable SSH on IR1 and IR2 routers to meet requirements given below.

(a) Use most secure SSH version.

(b) Use **admin/Skill39@Lyon** credential.

(c) Telnet should not be allowed when accessing network devices.

(d) On two internet routers (IR1 and IR2) increase SSH security by limiting SSH MAC algorithm to **hmac-sha2-512** and **hmac-sha2-256**

5. Limit only HQ1-SVR1(10.10.100.101/24) can SSH into IR1 and IR2.

6. Enable port security on HQ1-CLI and HQ2-CLI1 connected switchports. There is a plan to deploy VOIP handsets in HQ1 and HQ2 on vlan 150. You can define VLAN150 (named VOIP) on AS1 and AS2 for this task.

(a) Limit the mac addresses to minimum required if those PCs go behind VOIP phone.

(b) In case of port security violation, port should be disabled and syslog message to be generated.

(c) Port should be automatically recovered in 3 minutes.

7. Implement an ACL to block vlan 102 users in HQ1, HQ2, BR1 and BR2 to HQ1-SVR1 server. This should not break any previously configured access from HQ1-SVR1 to other devices.