worldskills

Test Project

Module C – Networking Environment

IT Network Systems Administration

Submitted by:

Rasika Nayanajith Manannalage - SE360 PTY LTD, Independent Test Project Designer
Wanderlyn Cetauro Raposo Junior - Read Write, Independent Test Project Validator

Contents

Introduction **3**
Description of project and tasks **3**
Topology **4**
Physical Topology 4
HQ IPv6 Topology 5
Logical Topology 6
Routing Topology 7
Instructions to the Competitor **8**
Part 1: Basic Configuration **9**
Part 2: L2 Services **14**
Part 3: EIGRP **16**
Part 4: OSPF **17**
Part 5: BGP **17**
Part 6: IP Services **18**
Part 7: Security and VPN **19**

© WorldSkills International

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** 300-410 (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.

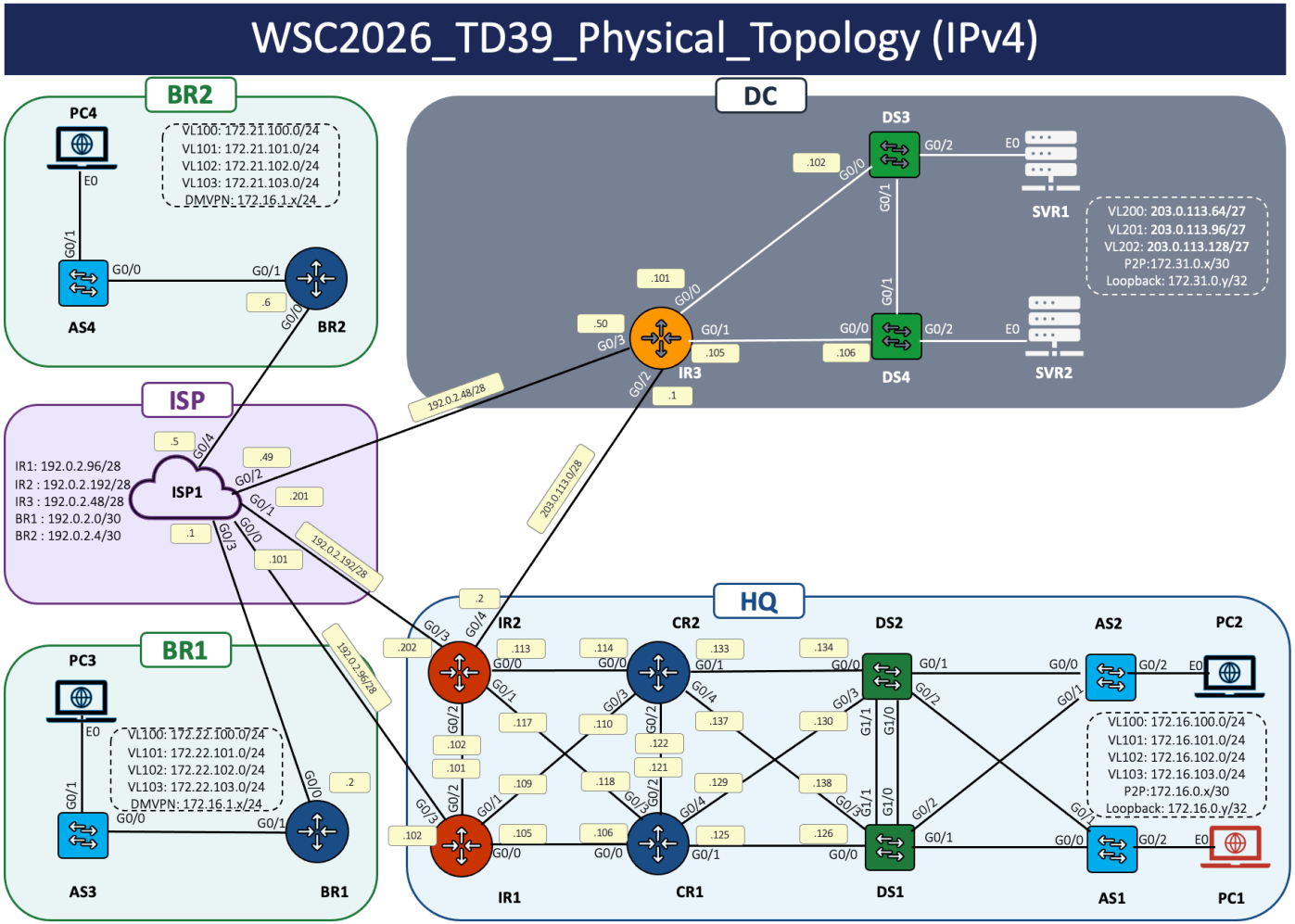
Configuration tasks are broken down into seven areas given below. Percentage shows the distribution of marks to each area.

- Basic configuration [10%]
- L2 services [15%]
- OSPF [10%]
- EIGRP [20%]
- BGP [15%]
- IP Services [15%]
- VPN and Security [15%]

© WorldSkills International

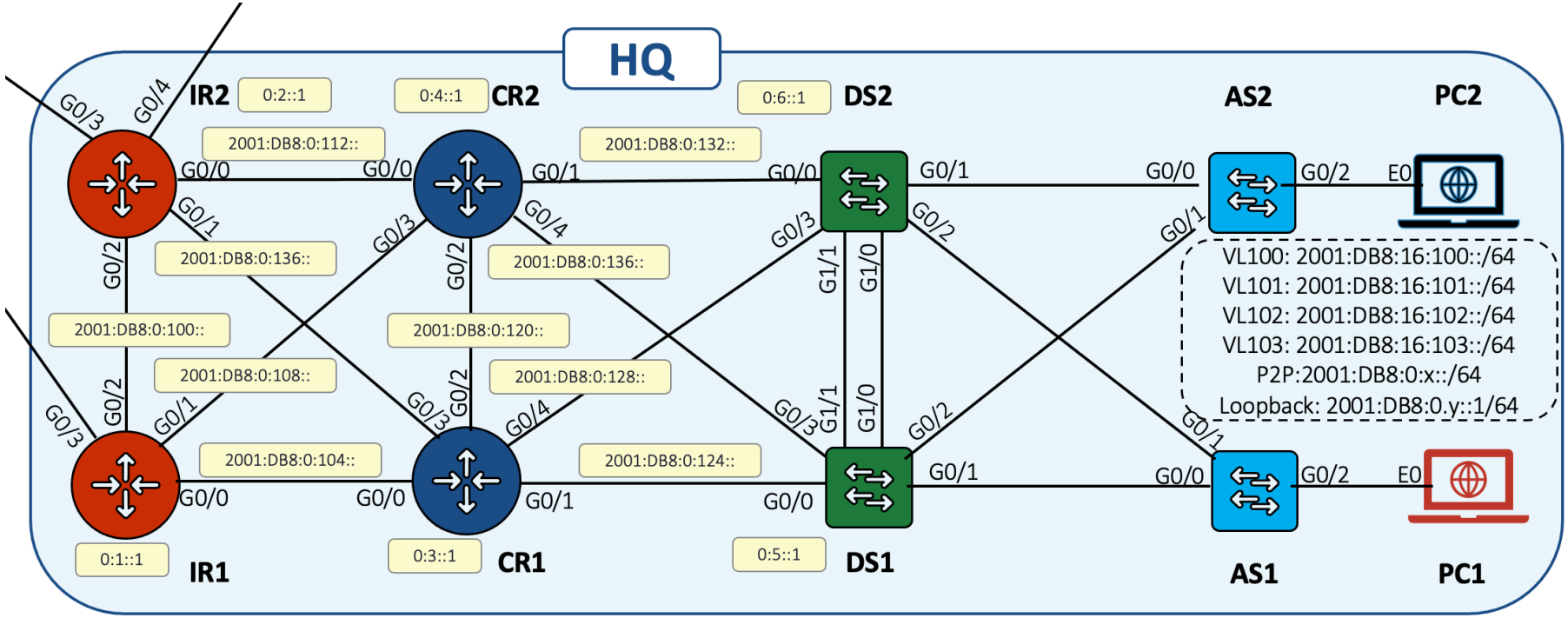
Topology

Physical Topology



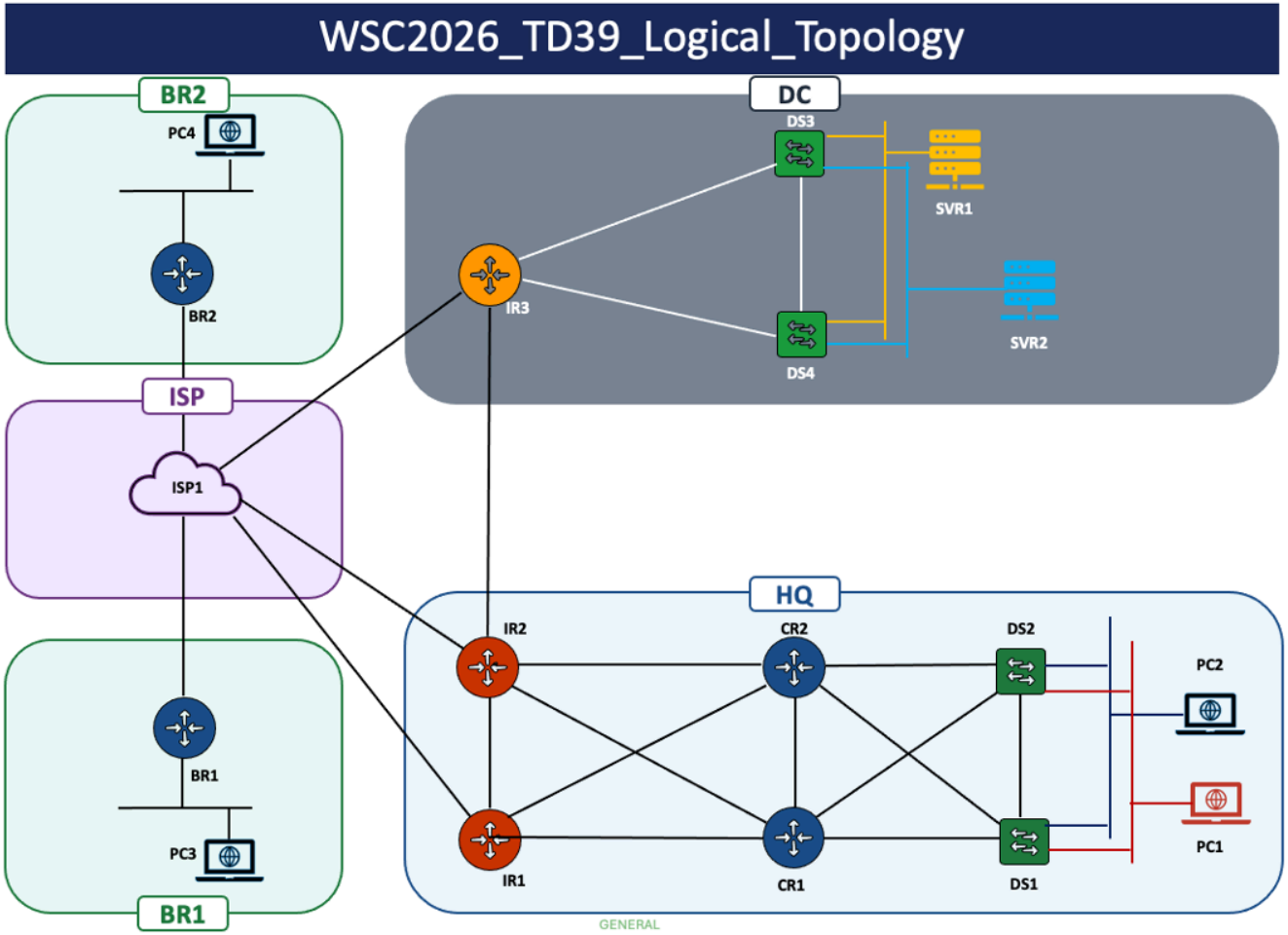
© WorldSkills International

HQ IPv6 Topology



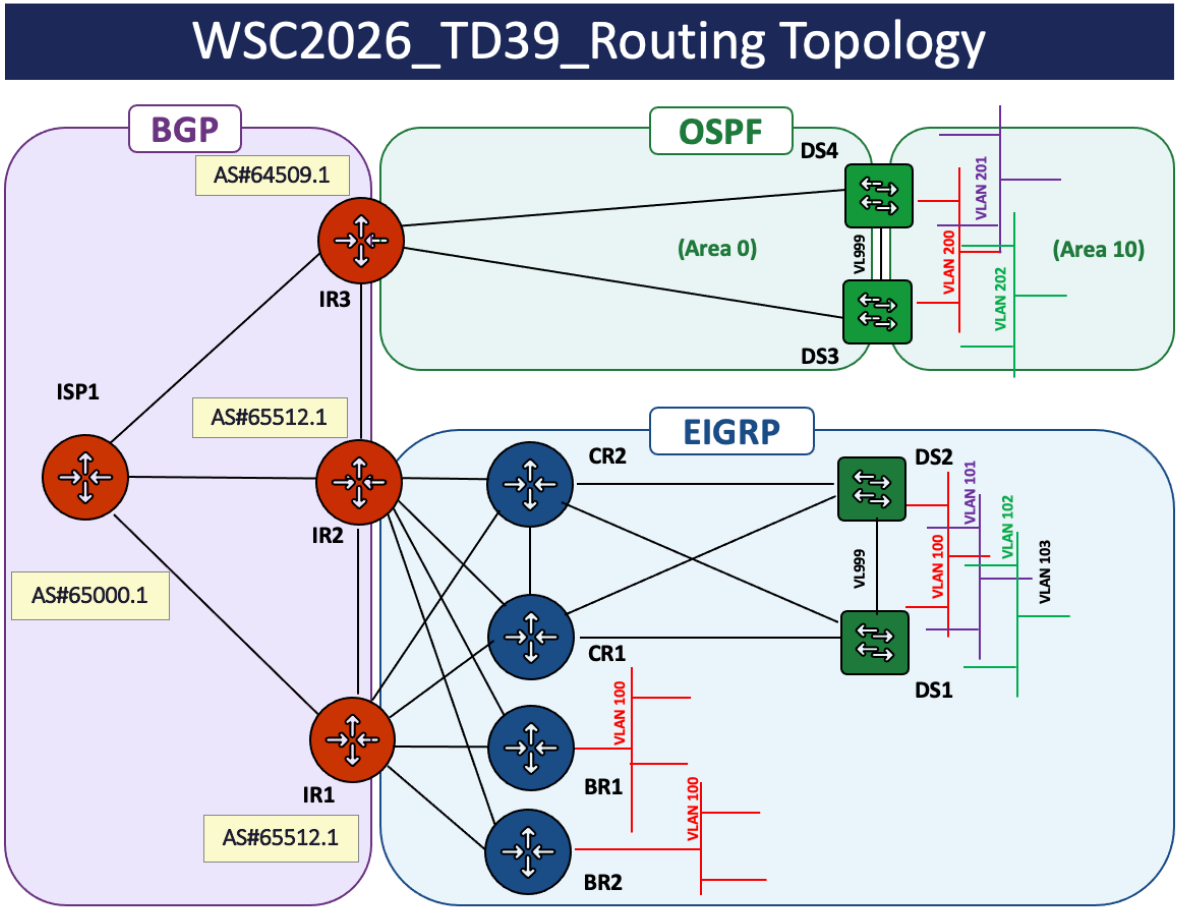
© WorldSkills International

Logical Topology



© WorldSkills International

Routing Topology



© WorldSkills International

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 (PC1, PC2, PC3, PC4) and Servers (SVR1 and SVR2) can be accessible with **admin\ Skill39@Shanghai** 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. Manually configured static routes are NOT allowed unless explicitly requested in this test project. Protocol generated discard routes crated automatically by OSFP/EIGRP summarization are premitted.

    (a) The only exception for manually configured static routes is when configuring BR1 and BR2 in Part 7: Security and VPN

11. Static routes including routes to Null0, must not be used to create, support or force routing outcomes for EIGRP, OSPF or BGP.

© WorldSkills International

Part 1: Basic Configuration

1. IPv4 addressing is already configured on all HQ and DC devices. However, **three interfaces** have incorrect IP configurations that must be corrected before proceeding.
2. In addition, configure the required IPv4 addresses on all interfaces for branch devices (BR1, BR2, AS3 and AS4) according to the addressing table provided.

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
ISP1	GigabitEthernet0/0	192.0.2.101/28	IR1
ISP1	GigabitEthernet0/1	192.0.2.201/28	IR2
ISP1	GigabitEthernet0/2	192.0.2.49/28	IR3
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
ISP1	Loopback8	8.8.8.8/32	N/A
IR1	GigabitEthernet0/0	172.16.0.105/30	CR1
IR1	GigabitEthernet0/1	172.16.0.109/30	CR2
IR1	GigabitEthernet0/2	172.16.0.101/30	IR2
IR1	GigabitEthernet0/3	192.0.2.102/28	ISP1
IR1	Loopback1	172.16.0.1/32	N/A
IR2	GigabitEthernet0/0	172.16.0.113/30	CR2
IR2	GigabitEthernet0/1	172.16.0.117/30	CR1
IR2	GigabitEthernet0/2	172.16.0.102/30	IR1
IR2	GigabitEthernet0/3	192.0.2.202/28	ISP1
IR2	GigabitEthernet0/4	203.0.113.2/28	IR3
IR2	Loopback1	172.16.0.2/32	N/A
IR3	GigabitEthernet0/0	172.31.0.101/30	DS3
IR3	GigabitEthernet0/1	172.31.0.105/30	DS4
IR3	GigabitEthernet0/2	203.0.113.1/28	IR2

© WorldSkills International

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
IR3	GigabitEthernet0/3	192.0.2.50/28	ISP1
IR3	Loopback1	172.31.0.10/28	N/A
CR1	GigabitEthernet0/0	172.16.0.106/30	IR1
CR1	GigabitEthernet0/1	172.16.0.125/30	DS1
CR1	GigabitEthernet0/2	172.16.0.121/30	CR2
CR1	GigabitEthernet0/3	172.16.0.118/30	IR2
CR1	GigabitEthernet0/4	172.16.0.129/30	DS2
CR1	Loopback1	172.16.0.3/32	N/A
CR2	GigabitEthernet0/0	172.16.0.114/30	IR2
CR2	GigabitEthernet0/1	172.16.0.133/30	DS2
CR2	GigabitEthernet0/2	172.16.0.122/30	CR1
CR2	GigabitEthernet0/3	172.16.0.110/30	IR1
CR2	GigabitEthernet0/4	172.16.0.137/30	DS1
CR2	Loopback1	172.16.0.4/32	N/A
DS1	GigabitEthernet0/0	172.16.0.126/30	CR1
DS1	GigabitEthernet0/3	172.16.0.138/30	CR2
DS1	Loopback1	172.16.0.5/32	N/A
DS1	Vlan100	172.16.100.2/24	N/A
DS1	Vlan101	172.16.101.2/24	N/A
DS1	Vlan102	172.16.102.2/24	N/A
DS1	Vlan103	172.16.103.2/24	N/A
DS1	Vlan999	172.16.0.141/30	DS2
DS2	GigabitEthernet0/0	172.16.0.134/30	CR2
DS2	GigabitEthernet0/3	172.16.0.130/30	CR1
DS2	Loopback1	172.16.0.6/32	N/A

© WorldSkills International

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
DS2	Vlan100	172.16.100.3/24	N/A
DS2	Vlan101	172.16.101.3/24	N/A
DS2	Vlan102	172.16.102.3/24	N/A
DS2	Vlan103	172.16.103.3/24	N/A
DS2	Vlan999	172.16.0.142/30	DS1
AS1	Vlan100	172.16.100.11/24	N/A
AS2	Vlan100	172.16.100.12/24	N/A
BR1	GigabitEthernet0/0	192.0.2.2/30	ISP1
BR1	GigabitEthernet0/1.100	172.21.100.1/24	N/A
BR1	GigabitEthernet0/1.101	172.21.101.1/24	N/A
BR1	GigabitEthernet0/1.102	172.21.102.1/24	N/A
BR1	GigabitEthernet0/1.103	172.21.103.1/24	N/A
BR1	Loopback1	172.16.0.11/32	N/A
BR1	Tunnel0	172.16.1.101/24	IR1/IR2
AS3	Vlan100	172.21.100.11/24	N/A
BR2	GigabitEthernet0/0	192.0.2.6/30	ISP1
BR2	GigabitEthernet0/1.100	172.22.100.1/24	N/A
BR2	GigabitEthernet0/1.101	172.22.101.1/24	N/A
BR2	GigabitEthernet0/1.102	172.22.102.1/24	N/A
BR2	GigabitEthernet0/1.103	172.22.103.1/24	N/A
BR2	Loopback1	172.16.0.12/32	N/A
BR2	Tunnel0	172.16.1.102/24	IR1/IR2
AS4	Vlan100	172.22.100.11/24	N/A
SVR1	Vlan201	203.0.113.100/27	Static
SVR2	Vlan200	203.0.113.75/27	Static

© WorldSkills International

DEVICE	INTERFACE	IPV4 ADDRESS	NEIGHBOR
PC1	Vlan103	172.16.103.200/24	DHCP
PC2	Vlan102	172.16.102.x/24	DHCP
PC3	Vlan101	172.21.101.x/24	DHCP
PC4	Vlan100	172.22.100.100/24	Static

3. All HQ devices already have IPv6 addresses configured, except DS1 and DS2. Configure the correct IPv6 addresses on the required interfaces of DS1 and DS2 according to the table below.

DEVICE	INTERFACE	IPV6 ADDRESS	NEIGHBOR
IR1	GigabitEthernet0/0	2001:DB8:0:104::1/64	CR1
IR1	GigabitEthernet0/1	2001:DB8:0:108::1/64	CR2
IR1	GigabitEthernet0/2	2001:DB8:0:100::1/64	IR2
IR1	Loopback1	2001:DB8:0:1::1/64	N/A
IR2	GigabitEthernet0/0	2001:DB8:0:112::1/64	CR2
IR2	GigabitEthernet0/1	2001:DB8:0:136::1/64	CR1
IR2	GigabitEthernet0/2	2001:DB8:0:100::2/64	IR1
IR2	Loopback1	2001:DB8:0:2::1/64	N/A
CR1	GigabitEthernet0/0	2001:DB8:0:104::2/64	IR1
CR1	GigabitEthernet0/1	2001:DB8:0:124::1/64	DS1
CR1	GigabitEthernet0/2	2001:DB8:0:120::1/64	CR2
CR1	GigabitEthernet0/3	2001:DB8:0:136::2/64	IR2
CR1	GigabitEthernet0/4	2001:DB8:0:128::1/64	DS2
CR1	Loopback1	2001:DB8:0:3::1/64	N/A
CR2	GigabitEthernet0/0	2001:DB8:0:112::2/64	IR2
CR2	GigabitEthernet0/1	2001:DB8:0:132::1/64	DS2
CR2	GigabitEthernet0/2	2001:DB8:0:120::2/64	CR1
CR2	GigabitEthernet0/3	2001:DB8:0:108::2/64	IR1

DEVICE	INTERFACE	IPV6 ADDRESS	NEIGHBOR
CR2	GigabitEthernet0/4	2001:DB8:0:136::1/64	DS1
CR2	Loopback1	2001:DB8:0:4::1/64	N/A
DS1	GigabitEthernet0/0	2001:DB8:0:124::2/64	CR1
DS1	GigabitEthernet0/3	2001:DB8:0:136::2/64	CR2
DS1	Loopback1	2001:DB8:0:5::1/64	N/A
DS1	Vlan100	2001:DB8:16:100::2/64	N/A
DS1	Vlan101	2001:DB8:16:101::2/64	N/A
DS1	Vlan102	2001:DB8:16:102::2/64	N/A
DS1	Vlan103	2001:DB8:16:103::2/64	N/A
DS1	Vlan999	2001:DB8:0:140::1/64	DS2
DS2	GigabitEthernet0/0	2001:DB8:0:132::2/64	CR2
DS2	GigabitEthernet0/3	2001:DB8:0:128::2/64	CR1
DS2	Loopback1	2001:DB8:0:6::1/64	N/A
DS2	Vlan100	2001:DB8:16:100::3/64	N/A
DS2	Vlan101	2001:DB8:16:101::3/64	N/A
DS2	Vlan102	2001:DB8:16:102::3/64	N/A
DS2	Vlan103	2001:DB8:16:103::3/64	N/A
DS2	Vlan999	2001:DB8:0:140::2/64	DS1

4. Configure all routers and switches in HQ, DC, BR1 and BR2 to use CST (UTC+8) as the timezone.
5. Each device must automatically update its hardware clock from the software clock whenever NTP synchronisation is maintained.
6. Configure domain name **wsc2026.net** for all devices in the topology.
7. Configure the enable password as **Skill39@Shanghai** on all routers and switches.
8. Create a local user account with the highest privilege:

- Username: **admin**
- Password: **Skill39@Shanghai**

Make sure all the passwords are configured using **Type 8** algorithm (see below).

IR1#sh run | in admin|enable

enable secret **8** 8d2iPEO59T7Pd49$LuWPYP49BXJl0rIlWUql4U4jgnLcQ9yQSUzzPDPbWIU

username admin privilege 15 secret **8** 8Shv/A1DTfQkU1v$.Hdpkdgnm2pXFMoKzHsLJS6JjbKK1R1f8mTTB2ROfSI

Part 2: L2 Services

1. Configure VTP domain "WSC2026" on DS1, DS2, DS3, DS4, AS1, AS2, AS3 and AS4. All switches to pass VTP advertisement through without acting on them.
2. Configure following VLANs across on switches in HQ, BR1 and BR2.

VLAN ID	VLAN NAME	DEVICES
100	MGMT	DS1, DS2, AS1, AS2, AS3, AS4
101	CCTV	DS1, DS2, AS1, AS2, AS3, AS4
102	WLAN	DS1, DS2, AS1, AS2, AS3, AS4
103	CORP	DS1, DS2, AS1, AS2, AS3, AS4
888	NATIVE	DS1, DS2, AS1, AS2, AS3, AS4
999	L3_P2P	DS1, DS2

3. Configure following VLANs across DS3 and DS4 in the Data Centre (DC)

VLAN ID	VLAN NAME	DEVICES
200	MGMT	DS3, DS4
201	SVR1	DS3, DS4
202	SVR2	DS3, DS4
999	L3_P2P	DS3, DS4

4. Configure STP to meet the requirements below:

   (a) Configure STP load balancing so DS1 is the root bridge for odd VLANs and DS2 for even VLANs. If one fails, the other must take over the root bridge role. Use the two lowest STP priority values to achieve this outcome.
   (b) In DC, 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) Configure all switches (DS1–DS4, AS1–AS4) to achieve the fastest possible STP convergence. Use an appropriate STP mode to meet this requirement.

5. Configure trunk ports between DS1/ DS2 (G 1/0-1) and AS1/AS2 (G0/1-2) using vlan 888 as native vlan.

   (a) Configure AS3 and AS4 G0/0 as trunk ports, keeping vlan 1 as the native vlan.
   (b) To prevent vlan hopping, ensure native vlan traffic is tagged between all HQ switches.

6. Configure port-channel 12 between DS1 and DS2 using G1/0 and G1/1. Use IEEE 802.3ad based aggregation protocol with both sides actively negotiating. If negotiation fails for any reason, let these ports fall back into standalone operation (independent mode)
7. Configure HSRP on DS1/DS2 for VLANs 100–103 and DS3/DS4 for VLANs 200-202 to meet the following requirements:

   (a) The HSRP virtual IP address must be the .1 address of each VLAN's /24 subnet. Use the VLAN number as the HSRP group number.
   (b) HSRP active roles must align with the STP root bridge assignment configured earlier:

   - DS1 must be HSRP active for odd-numbered VLANs where it is the STP root bridge
   - DS2 must be HSRP active for even-numbered VLANs where it is the STP root bridge
   - DS3 must be HSRP active for all VLANs (including any future VLANs), with DS4 assume the active role only if DS3 become unavailable.

   (c) Configure HSRP priority to ensure the correct active device is always preferred. When the active device recovers from a failure it must automatically reclaim the HSRP active role without manual intervention.

8. In HQ, configure IPv6 HSRP for VLAN 102 and VLAN 103 on DS1 and DS2 to meet the following requirements:

   (a) Use group number 1102 for VLAN 102 and group number 1103 for VLAN 103.
   (b) Configure a consistent link-local virtual IPv6 address for both VLAN 102 and VLAN 103 HSRP groups, ensuring end devices on both VLANs use the same virtual gateway address ending in ::FE80.
   (c) Follow the same Active/Standby rules used for IPv4 when configuring IPv6 (ie DS1 HSRP active for group 1103 and DS2 is HSRP active for group 1102).

9. Implement the following Spanning Tree Protocol (STP) mechanisms on the appropriate devices to prevent Layer 2 loops:

   (a) Configure DS1 and DS2 to ensure that AS1 and AS2 are prevented from becoming the root bridge under any circumstances.
   (b) Configure AS1 and AS2 so that any point-to-point link ports that stops receiving BPDUs is automatically placed into a loop-inconsistent blocking state.
   (c) On DS1 interface G1/2, suppress outbound BPDU transmission to simulate a BPDU failure.

10. Configure the switchports connected to SVR1 and SVR2 on DS3 and DS4 to establish server connectivity. The servers have been preconfigured with the static IP addresses 203.0.113.100/27 and 203.0.113.75/27.

Part 3: EIGRP

Configure EIGRP protocol in HQ (IR1, IR2, CR1, CR2, DS1 and DS2 devices) to achieve the following requirements. Note: You will be asked to configure EIGRP on BR1 and BR2 in Part 7: 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 "WSC2026" for this EIGRP configuration.
2. For IPv4, use autonomous system number 2026. Makesure loopback1 IP address becomes the EIGRP router-id.
3. Advertise all loopback and /30 P2P (point-to-point/) networks into EIGRP on IR1, IR2, CR1, CR2, DS1 and DS2. Advertise vlan 100-103 networks into EIGRP in DS1 and DS2.
4. By default, EIGRP should be disabled on all interfaces. Even if an interface IP range is included in a network statement, the interface must not send EIGRP hello messages or attempt to form EIGRP adjacencies unless explicitly enabled.
5. On all EIGRP-enabled interfaces at HQ, BR1, and BR2, limit EIGRP control plane traffic to a maximum of 10% of the configured interface bandwidth. Verify the setting is applied on all relevant interfaces.
6. Configure all EIGRP-enabled devices in HQ, BR1, and BR2 so that bandwidth is not used as a factor in the EIGRP metric calculation.
7. Configure DS1 and DS2 to advertise HQ vlan 100-103 subnets as efficiently as possible using a single advertisement instead of individual subnet entries.
8. Configure EIGRP authentication between IR1 and IR2 using the most secure method supported by the current EIGRP configuration. Use E?GRP as the authentication password.
9. Configure redundant internet gateways within the EIGRP domain using IR1 as the primary gateway and IR2 as the standby. EIGRP metrics must enforce path preference, and failover must occur automatically without manual intervention.
10. After configuring the routing for BR1 and BR2 (sec 3.7.1-3.7.3), ensure that summary routes (172.21.100.0/22 and 172.22.100.0/22) and loopback addresses (172.16.0.11 and 172.16.0.12) are available on HQ devices EIGRP routing table.
11. Configure EIGRP on IPv6 on HQ

    (a) Use same EIGRP instance WSC2026 configured for IPv4
    (b) Use autonomous system number 2026 for IPv6 as well
    (c) On DS1 and DS2, IPv6 EIGRP adjacencies should not established across vlan 100,101,102 or vlan 103.
    (d) Verify you can ping IR2 loopback 1 address (2001:DB8:0:2::1/64) from PC1.

Part 4: OSPF

Configure OSPF protocol in IR3, DS3 and DS4 devices in DC 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. DS3 and DS4, configure vlan 200-202 network in OSPF area 10.
3. OSPF hello messages should be only sent via /30 networks where devices are interconnected.
4. Configure all OSPF-enabled interfaces to operate as point-to-point links, ensuring no DR/BDR election occurs, and all loopback interfaces advertise their actual /28 subnet mask.
5. Configure IR3 to conditionally advertise a default route into OSPF only when a default route is being received from ISP1. The default route must appear as an OSPF External Type 2 (E2) route with a metric of 1000.
6. Configure OSPF summary routes on ABR (Area Border Routers) only 203.0.113.0/24 route being advertised.

Part 5: BGP

Configure the BGP protocol on IR1, IR2 and IR3 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, IR3, BR1 and BR2)

1. Configure eBGP sessions on IR1 and IR2 (both in AS 65512.1) and IR3 (in AS 64509.1) with the ISP router interfaces: G0/0 (192.0.2.101), G0/1 (192.0.2.201), and G0/2 (192.0.2.49). Note that ISP router already configured with following settings.

   (a) Keepalive interval 10s and Holddown time of 30s
   (b) Authentication password **Skill39@Shanghai**

2. Configure eBGP sessions between IR2 (AS 65512.1) and IR3 (AS 64509.1) using 203.0.113.0/28 IP addresses in each router and authentication password **Skill39@Shanghai**.
3. If a link failure occurs between IR2 and IR3, routers to drop the eBGP peer within one second interval.
4. Configure IR3 to advertise only 203.0.113.0/24, 172.31.0.0/28, 172.31.0.16/28 and 172.31.0.32/28 networks to the ISP and IR2. Prevent any other routes being accidently advertised to these eBGP peers.
5. Configure IR2 with an outbound BGP prefix filter towards IR3 that strictly permits only 172.16.0.0/16, 172.21.0.0/16, and 172.22.0.0/16, denying all other prefixes.
6. Configure iBGP between IR1 and IR2 to meet the following requirements.

   (a) Keepalive interval 10s and Holddown time of 30s
   (b) Authenticate each iBGP sessions with password **Skill39@Shanghai**
   (c) BGP peering to use loopback1 interface IP

7. Advertise 172.16.0.0/16, 172.21.0.0/16 and 172.22.0.0/16 routes into BGP on IR1 and IR2 using BGP and routing protocol mechanism.
   Static routes, including static routes to Null0, must not be used to create or support BGP advertisements. ISP1 should not receive any accidental routes from IR1 or IR2 other than above summary routes.
8. Configure BGP on IR1 and IR2 so that all inbound Internet traffic prefers IR1 as the primary path, and uses IR2 only if the primary path fails.

   Since ISP1 does not accept routes with AS-PATH prepending, use an alternative BGP attribute to achieve this behavior.

   You can run traceroute 172.16.0.1 from SVR1/SVR2 before and after your configuration to verify that traffic goes via IR1 after the change. During testing, shut down IR2 G0/4.

© WorldSkills International

9. Validate the resilience of the network by disabling the direct connection between IR2 and IR3.
   (a) Confirm that HQ & BR1/BR2 users on VLAN 103 (CORP) and VLAN 100 (MGMT) retain full connectivity to SVR1 via an alternate path.
   (b) Verify that you can ping SVR1 from PC1 (on CORP vlan) and PC4 (on MGMT vlan) when the direct connection between IR2 and IR3 fails.

Part 6: IP Services

You have been asked to configure following IP services.

1. Configure NAT on IR1 and IR2 to provide internet access exclusively for WLAN (VLAN 102) and CORP (VLAN 103)
   (a) Users across HQ, BR1 and BR2. MGMT and CCTV VLANs must not have internet access.
   (b) Translated addresses must reflect the exit point:
   (c) **Via IR1** -> 192.0.2.104 -192.0.2.110
   (d) **Via IR2** -> 192.0.2.193 -192.0.2.199
   (e) Use 8.8.8.8 to verify internet reachability after configuration.
2. When PC4 (172.22.100.100) access SVR1(203.0.113.100) during the direct connecrt failure scenario (Part 5 BGP, Dot Point 8) it is required to meet following conditions
   (a) PC4 traffic it should appear as 192.0.2.200 if traffic goes via IR2
   (b) PC4 traffic it should appear as 192.0.2.100 if traffic goes via IR1.
   (c) When PC4 traffic go to SVR2 (203.0.113.75) or any other server in DC it should not appear coming with these IPs.
3. IR1 and IR2 should get its time from ISP1 peering address (192.0.2.101 and 192.0.2.201). Ensure 192.0.2.201 is prefer over 192.0.2.101 as NTP server.
   (a) All other devices in HQ, DC, BR1 and BR2 should use IR1 (172.16.0.1) and IR2 (172.16.0.2) as their NTP servers.
   (b) Use loopback address for NTP communication with IR1 and IR2. (Except AS1 to AS4 where you can use SVI of vlan 100 IP)
   (c) Verify that each device's clock is synchronized with its respective NTP server after completing the lab configuration.
4. Configure DHCP services on DS1 and DS2 with the following scopes:
   (a) **VLAN 102**: IP range 172.16.102.101–172.16.102.254, GW 172.16.102.1
   (b) **VLAN 103**: IP range 172.16.103.101–172.16.103.254, GW 172.16.103.1
5. Configure the port connected to PC1 for VLAN 103 and the port connected to PC2 for VLAN 102.
   (a) Ensure both PCs receive IP addresses via DHCP from their respective VLANs.
6. Reserve the IP address 172.16.103.200 in the DHCP pool for PC1
   Configure DHCP services for VLAN 101 (CCTV) on HQ, BR1 and BR2 with the following scopes:
   (a) **HQ**: IP range 172.16.101.101–172.16.101.254, GW 172.16.101.1
   (b) **BR1**: IP range 172.21.101.101–172.21.101.254, GW 172.21.101.1
   (c) **BR2**: IP range 172.22.101.101–172.22.101.254, GW 172.22.101.1
7. Configure the port connected to PC3 on VLAN 101 and PC4 on vlan 100.
   (a) Verify CCTV VLAN connectivity and operation in Branch 1.

Part 7: Security and VPN

Multiple branch sites need to connect to the HQ network. To test the new connectivity, BR1 & BR2 have been required to configure as DMVPN spoke site with IR1 and IR2 routers in HQ.

1. Configure IR1 and IR2 as DMVPN Hub for branch sites connectivity. You are required to consider below when configuring IR1 and IR2.

   (a) Use network-id **2026**.
   (b) Tunnel interface 0 to use 172.16.1.1/24 and 172.16.1.2/24 IP addresses in IR1 and IR2 respectively.
   (c) Use string **WSC2026** to identify NHRP domain when establishing VPN connecivity.

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 172.16.1.101/24 IP address.
   (c) BR2 tunnel interface 0 to use 172.16.1.102/24 IP address.
   (d) BR1 and BR2 should establish dynamic tunnel between then when communicating each other.

3. Configure EIGRP on BR1, BR2, IR1 and IR2 to meet the following requirements.

   (a) BR1 and BR2 must each advertise a single summary route that encompasses all vlan 100-103 networks at their respective site.
   (b) IR1 and IR2 to must each adverise a single summary route that cover all HQ point-to-point links and loopback interface IP addresses.

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

   (a) Use most secure SSH version.
   (b) Use **admin/Skill39@Shanghai** credential.
   (c) Telnet should not be allowed.
   (d) Limit simultaneous sessions to 3 per SSH user

5. Limit only MGMT network (172.16.100.0/24, 172.21.100.0/24 and 172.22.100.0/24) hosts can SSH into IR1 and IR2.
6. Implement access control measures in HQ, BR1 and BR2 to secure the CCTV network, ensuring that:

   (a) Do not block DHCP/DNS/HSRP traffic by this ACL
   (b) CCTV devices are permitted to communicate only with SVR2 (203.0.113.75) in the DC, with access to all other DC servers denied.

© WorldSkills International