360RSW05-WKB-CA06

Cisco 360 CCIE R&S Exercise Workbook Introduction

The Cisco 360 CCIE® R&S Version 5 Exercise Workbook contains 20 challenging scenarios at the CCIE level that can be used for rigorous self-paced practice. The Exercise Workbook scenarios include both a troubleshooting section and a configuration section.

Each lab provides an extensive answer key, Mentor Guide support, and verification tables and is designed to maximize learning by providing practical experience. Also, self-paced learning resources such as the Cisco 360 CCIE R&S Reference Library and Cisco 360 CCIE R&S lessons supplement the Exercise Workbook scenarios.

Cisco 360 CCIE R&S Exercise Workbook Lab 6 Configuration Section

Table of Contents

Activity Objectives

When performing any Practice Lab, it is recommended that you formulate a test-taking strategy that includes the following activities. Some of these activities should be conducted in the actual lab:

- Download the latest copy of a Practice Lab, and then print it and read it carefully from beginning to end.
- Create a strategy for how to perform a Practice Lab.
- Draw diagrams if necessary.
- Create a checklist of general best practices to follow during the Practice Lab.
- Develop skill in finding issues in the lab so that you are able to uncover the hidden and complex internetworking issues.
- Carefully track your time so that you can develop good time-management techniques.
- Estimate the points that you have gained or lost to see where you are in your overall goal.

General Lab Instructions

Read the following instructions carefully. It is important to remember that if you misinterpret any directions, you could lose points. After you have read the "General Lab Instructions" section, read through the entire lab carefully and look for connections between the tasks. Pay close attention to the "Restrictions and Goals" section because the information may reduce the configuration options that are available to you.

- Your pod should be cabled according to the example in the "Ethernet Switched Cabling Topology" diagram and the IPv4 and IPv6 diagrams.
- Each router should have an initial IP configuration loaded.
- You should be able to access all devices on your learner virtual pod via Telnet.
- To begin, check the following base configuration for each router and switch:
  - Configure a hostname on each device.
  - If a DNS server is being used in your pod, disable the DNS lookups.
  - Familiarize yourself with any Cisco IOS Software shortcuts.
  - Remember that some Cisco IOS command parameters and regular expressions are case-sensitive.
- Verify the following information on each router and switch:
  - Determine the Cisco IOS Software versions that are being used for the routers and the virtual switches.
  - Verify that all the software on the routers and switches sees all physical interfaces.
- Review all the tasks in the scenario.

Difficulty Levels

Tasks are categorized as follows:

- **Basic:** These fundamental tasks are generally those tasks that are needed to provide the basic functions of the protocol or feature. You must complete these tasks to provide reachability and to move forward in the lab.
- **Intermediate:** These tasks include protocol features like routing optimization, route filtering, optimal path selection, load sharing, and summarization. Failure to complete these tasks will usually not affect later lab sections.
- **Advanced:** This category includes new Cisco IOS Software features and IP services, complex optimizations, and fine-tuning.

Scenarios are categorized as follows based on task classifications:

- Basic
- Basic to Intermediate
- Intermediate
- Intermediate to Advanced
- Advanced

Exercise Workbook Lab 6 Configuration Section

Grading and Duration

- Configuration lab duration: 6 hours
- Configuration lab maximum score: 76 points

Note You can assess your progress on the self-paced labs in this workbook by adding up the points that are assigned to sections and tasks. Consider taking the full Assessment Labs to assess your readiness level.

Difficulty Level

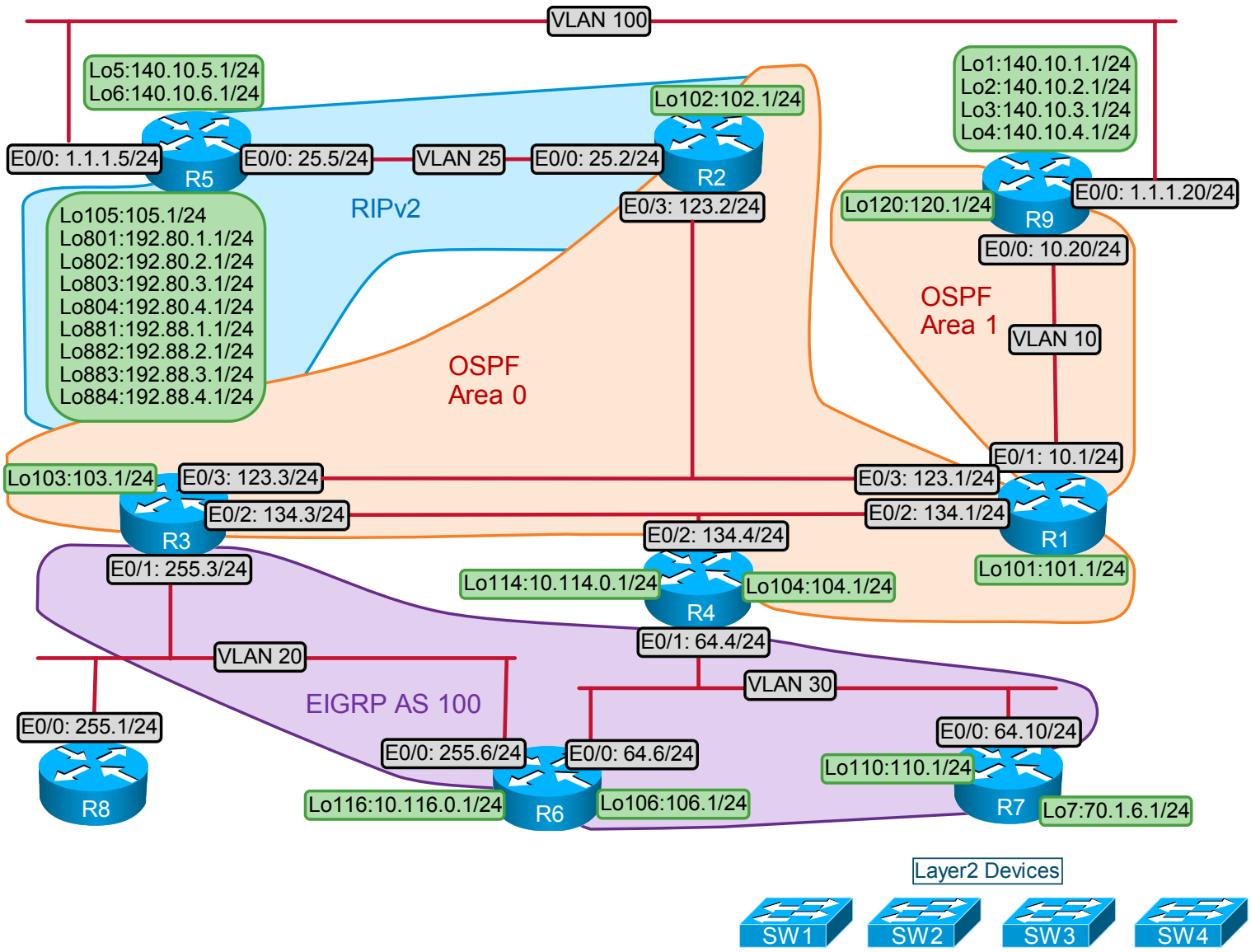
- Difficulty: Intermediate to Advanced

Restrictions and Goals

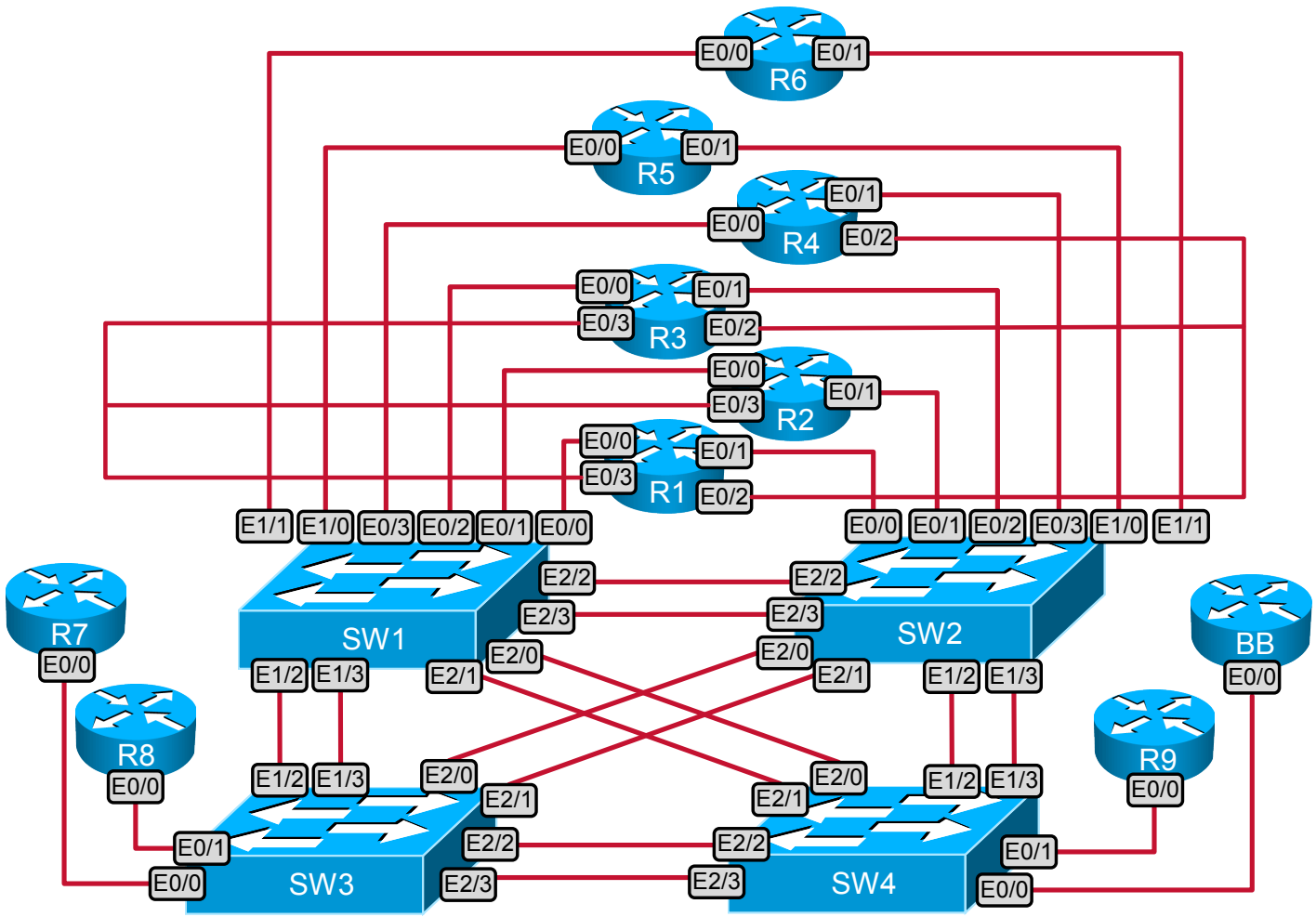
Note Read this section carefully.

- To receive credit for a subsection, you must fully complete the subsection per the requirements. You will *not* receive partial credit for partially completed subsections.
- IPv4 subnets that are displayed in the scenario diagram belong to network 170.18.0.0/16.
- *Points will be deducted from multiple sections for failing to assign correct IPv4 addresses.*
- Do not use any static routes.
- Advertise loopback interfaces with their original masks for IPv4 and IPv6 protocols.
- Do not use the **ip default-network** or **ip default-gateway** commands.
- All IP addresses that are involved in the same virtual routing and forwarding (VRF) instance must be reachable, unless an explicitly stated filtering requirement restricts reachability.
- Do not create new interfaces, and do not summarize prefixes unless the instructions explicitly specify it.
- Do not introduce any new IPv4 or IPv6 addresses, unless the instructions specifically require it.
- Use conventional routing algorithms only, unless the instructions specify otherwise.
- Do not modify the hostname, console, or vty configuration unless you are specifically asked to do so.
- Do not modify the initial interface or IP address numbering.

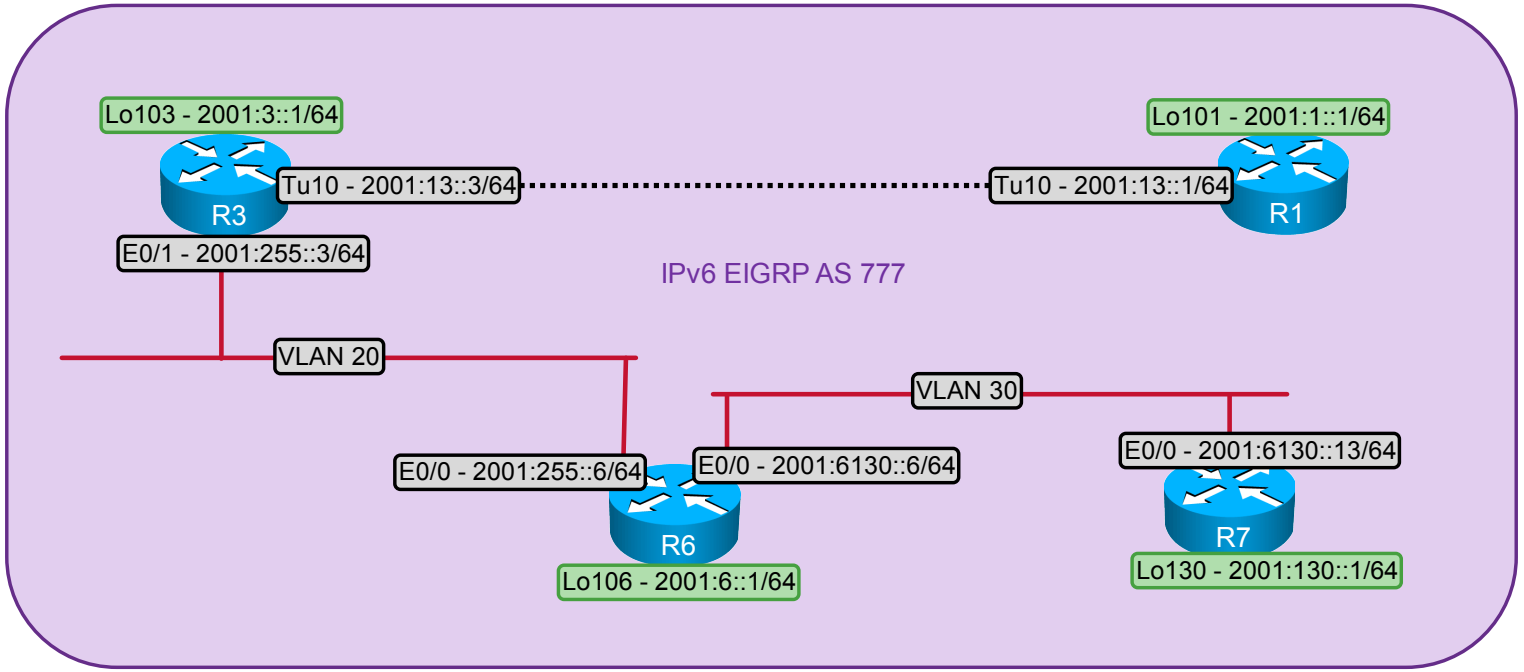
IPv4 IGP Diagram



Ethernet Switched Cabling Topology



IPv6 Topology Diagram



1. Switch Configuration Section (Total: 8 points)

1.1. Configure VLANs (Basic: 1 point)

- On SW1, SW2. SW3, and SW4, create the VLANs that are referenced in the following table:

VLANs

VLAN	VLAN Name
10	VLAN0010
20	VLAN0020
25	VLAN0025
30	VLAN0030
100	VLAN0100

1.2. Configure Switch-to-Router Connections (Basic: 2 points)

- Configure the following switch-to-router connections:

Switch-to-Router Connections

Switch	Router	VLAN
SW2	R1	VLAN 10
SW1	R2	VLAN 25
SW2	R3	VLAN 20
SW2	R4	VLAN 30
SW1	R5	VLANs 25,100
SW1	R6	VLANs 20,30
SW3	R7	VLAN 30
SW3	R8	VLAN 20
SW4	R9	VLANs 10,100

- Configure the switch ports as access VLAN ports whenever possible. Otherwise, use trunks.
- For switch-to-router trunking, use IEEE 802.1Q. Limit VLANs on the switch-to-router trunks to what is required in this scenario.
- Create the necessary Ethernet logical subinterfaces on the routers and assign the IP addresses that are specified in the diagram.

1.3. Configure VLAN Trunking Protocol (VTP) (Basic: 1 point)

- Do not use the VLAN configuration method that dynamically exchanges VLAN information over trunk links, but the trunk links should be able to forward the VLAN information.

1.4. Control Interswitch Links (Basic: 2 points)

- Verify that the ports that are listed in the following table have been administratively shut down (this is necessary) and make sure they remain in the shutdown state.

Switch Ports Shut Down

Switch	Port
SW1	1/3
	2/0
	2/1
SW2	1/3
	2/0
	2/1

Switch	Port
SW3	1/3
	2/0
	2/1
	2/2
	2/3
SW4	1/3
	2/0
	2/1
	2/2
	2/3

- Configure interfaces E2/2 and E2/3 connecting SW1 and SW2 as 802.1Q trunks.
- Configure interfaces E1/2 connecting SW1 and SW3 as an 802.1Q trunk.
- Configure interfaces E1/2 connecting SW2 and SW4 as an 802.1Q trunk.
- Only VLANs that need to carry traffic between the switches should be allowed on all trunk links.

1.5. Configure EtherChannel (Basic: 2 points)

- Make sure that you see the following output from the **show etherchannel summary** command on SW1 and SW2:

```
SW1#show etherchannel summary | begin Number
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
---
1      Po1(SU)         PAgP      Et2/2(P)    Et2/3(P)

SW1#
```

2. IPv4 OSPF Section (Total: 10 points)

Note	All OSPF routers must be configured with only one OSPF PID. *Points will be deducted from multiple sections for failing to assign one and only one OSPF PID on each specified router.* Use the IPv4 IGP diagram to help guide your configuration.

2.1. Create OSPF Areas (Basic: 2 points)

- Configure the network 170.18.123.0/24 between R1, R2, and R3 as OSPF Area 0.
- Configure the network 170.18.134.0/24 between R1, R3, and R4 as OSPF Area 0.
- Configure OSPF Area 1 on the subnet 170.18.10.0/24.

2.2. Advertise Networks into OSPF (Basic: 2 points)

- Advertise loopback subnets 170.18.101.1/24, 170.18.102.1/24, 170.18.103.1/24, and 170.18.104.1/24 in Area 0.
- Advertise the loopback subnet 170.18.120.1/24 in Area 1.

2.3. Establish OSPF Adjacencies (Intermediate: 2 points)

- Use an OSPF network type that elects a designated router, or DR, but does not require a neighbor statement for the subnet 170.18.123.0/24. Make sure that R3 is the DR and the other OSPF speakers are DROTHERs on subnet 170.18.123.0/24.
- Use an OSPF network type that elects a DR and requires neighbor statements for the subnet 170.18.134.0/24. Make sure that R4 is the DR and the other OSPF speakers are DROTHERs on subnet 170.18.134.0/24.

2.4. Tune OSPF (Intermediate: 3 points)

- Make sure that the loss of a neighbor relationship is detected twice as fast as the default for subnet 170.18.134.0/24.
- Make sure that OSPF sends the minimum information to R9.

2.5. Verify Connectivity (Basic: 1 point)

- Verify that all OSPF prefixes that are specified in this section can be reached from all devices in the OSPF domain.

3. IPv4 RIP Section (Total: 7 points)

3.1. Enable RIP (Basic: 1 point)

- Configure Routing Information Protocol version 2 (RIPv2) updates to exchange only over the VLAN25 connection between R2 and R5.

3.2. Advertise Networks into RIP (Basic: 2 points)

- Advertise the following loopback subnets into RIP from R5:
  - 192.80.1.0/24
  - 192.80.2.0/24
  - 192.80.3.0/24
  - 192.80.4.0/24
  - 192.88.1.0/24
  - 192.88.2.0/24
  - 192.88.3.0/24
  - 192.88.4.0/24

3.3. Control RIP Updates (Intermediate: 2 points)

- Allow only the following networks to be advertised to R2 using the minimum number of access list statements:
  - 192.80.2.0/24
  - 192.80.3.0/24
  - 192.88.2.0/24

- 192.88.3.0/24
- 170.18.105.0/24

3.4. Control RIP Routing (Intermediate: 2 points)

- Send the minimum required routing information from R2 to R5 to provide the connectivity to the subnets of 170.18.0.0.

4. IPv4 EIGRP Section (Total: 4 points)

4.1. Enable EIGRP (Basic: 2 points)

- Configure Enhanced Interior Gateway Routing Protocol (EIGRP) AS 100 on subnets 170.18.255.0/24 and 170.18.64.0/24 between R4, R3, R6, and R7.

4.2. Advertise Networks into EIGRP (Basic: 2 points)

- Advertise the loopback subnet 170.18.106.1/24 into EIGRP on R6.
- Advertise the loopback subnet 170.18.110.1/24 into EIGRP on R7.

5. Routing Stability Section (Total: 2 points)

5.1. Enhance Routing Stability (Intermediate: 2 points)

- Imagine that the Et0/1 interface on R4 is flapping, causing instability throughout the network. Now implement a feature on this interface that will isolate failures so that disturbances are not propagated.
- Configure the maximum configurable value for the half-life period and set the suppress threshold to 200 seconds, the reuse threshold value to 10 percent of the Cisco IOS default value, and the maximum suppress time to a value twice the value of the reuse threshold.
- Apply the configuration on R4.

6. Redistribution Section (Total: 7 points)

6.1. Obtain Universal Connectivity (Advanced: 2 points)

- Perform mutual redistribution between EIGRP AS 100 and OSPF on R3 and R4.
- Perform redistribution from RIP into OSPF on R2.
- Do not perform any other redistribution.

6.2. Verify Redistribution Filtering (Intermediate: 3 points)

- Ensure that only the following subnets are redistributed from EIGRP into OSPF; do not use filtering that is based on access or prefix lists:
  - 170.18.64.0/24
  - 170.18.106.0/24
  - 170.18.110.0/24
  - 170.18.255.0/24

6.3. Verify Connectivity (Advanced: 2 points)

- Verify that all IPv4 IGP prefixes that are specified in the IPv4 IGP diagram can be reached from all devices. See the "Restrictions and Goals" section for more information.

Note	VLAN 100 is used for BGP back-end connectivity only. Subnet 1.1.1.0/24 is not part of any IGP and does not have to be reachable via IGP.

7. BGP Section (Total: 12 points)

7.1. Configure Processes and Peers (Intermediate: 2 points)

- Configure BGP AS 100 on R1, R2, and R3.
- Configure BGP AS 10 on R4, R6, and R7.
- Configure BGP AS 1581 on R5.
- Configure BGP AS 1771 on R9.
- Configure BGP peer relationships between AS 10 and AS 100 using peers R3 and R6, and R1 and R4.
- Configure BGP peer relationships between AS 100 and AS 1581 using peers R2 and R5.
- Configure BGP peer relationships between AS 100 and AS 1771 using peers R1 and R9.
- Configure BGP peer relationships between AS 1581 and AS 1771 using peers R5 and R9 using VLAN 100.

7.2. Tune BGP Peering (Intermediate: 2 points)

- All Internal Border Gateway Protocol (IBGP) and External Border Gateway Protocol (EBGP) peering should be established using subnets that directly connect peering routers.

7.3. Advertise BGP Prefixes (Intermediate: 2 points)

- Advertise the following networks in AS 10 from R7:
  - 70.1.6.0/24
- Advertise the following networks in AS 1581 from R5:
  - 140.10.5.0/24
  - 140.10.6.0/24
  - 1.1.1.0/24
- Advertise the following networks in AS 1771 from R9:
  - 140.10.1.0/24
  - 140.10.2.0/24
  - 140.10.3.0/24
  - 140.10.4.0/24
  - 1.1.1.0/24

7.4. Configure AS 10 (Intermediate: 2 points)

- Do not peer R4 and R6 to meet the requirements of this section.
- Set R2 as a preferred exit point to networks 140.10.*.0/24 that have been originated by AS 1581 and AS 1771.

7.5. Enable BGP Route Filtering (Intermediate: 2 points)

- R1 should accept from R9 only prefixes originating in AS 1581 or AS 1771.

7.6. Control BGP Routing (Intermediate: 2 points)

- In AS 10, set the local preference value for all prefixes originating from AS 1771 and traversing AS 1581 to prefer R6 as a next hop.
- Set the local preference value for all prefixes originating from AS 1581 to prefer R4 as a next hop.
- Use local preference values 200 and 300 to accomplish this task.
- Do not use the AS path or the IP address prefix as match criteria to set the local preference value in AS 10.

8. MPLS Layer 3 VPNs Section (Total: 4 points)

8.1. Create a Customer VPN (Basic: 2 points)

- Configure VPN46 on R4 and R6 using the route distinguisher value 10:46. Include only the interfaces loopback 114 on R4 and loopback 116 on R6 in the VPN. Use the export route-target value 10:114 on R4 and the export route-target value 10:116 on R6.

8.2. Configure BGP to Support Site-to-Site Reachability (Intermediate: 2 points)

- Configure BGP peering between loopbacks 104 and 106. This peering must be used to exchange only VPNv4 addresses.
- Verify reachability between IP addresses 10.114.0.1 and 10.116.0.1.

9. Router Maintenance Section (Total: 8 points)

9.1. Enable Address Administration - Part 1 (Intermediate: 2 points)

- Configure R8 to act as a host with an IP address of 170.18.255.1/24.
- R8 should dynamically prefer R3 as a gateway and use R6 when R3 is not available. Do not use Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), or Gateway Loading Balancing Protocol (GLBP). Do not use any static configuration.

9.2. Enable Address Administration - Part 2 (Intermediate: 2 points)

- All packets originating from R8 should have the source IP address changed at the first-hop router, except for the packets that are destined to R3. The source IP address must be in the 170.18.255.0/24 range.

9.3. Manage Access to Routers (Intermediate: 2 points)

- Configure R7 so that it can be managed by a network management service that uses UDP port 161.
- Set read-only access using the string **RS-CCIE**. Set read-write access using the string **CCIE**.

9.4. Configure First-Hop Redundancy (Intermediate: 2 points)

- Configure HSRP between R4 and R6.
- Make R4 the preferred gateway.
- Switch to R6 if the Ethernet0/2 interface on R4 becomes inactive.
- The virtual gateway IP address is 170.18.64.1.

10. IPv6 Routing Section (Total: 6 points)

10.1. Establish R1-to-R3 IPv6 Connectivity and Assign IPv6 Addresses (Intermediate: 2 points)

- Create a logical link between R1 and R3 using IPv6 over IP encapsulation.
- Assign IPv6 addresses to router interfaces according to the following table:

IPv6 Address Assignment

Router	Link	IPv6 Routable Address
R1	Lo101	2001:1::1/64
	Logical Interface	2001:13::1/64
R3	Lo103	2001:3::1/64
	Et0/1 VLAN 20	2001:255::3/64
	Logical Interface	2001:13::3/64
R6	Lo106	2001:6::1/64
	Et0/0 VLAN 20	2001:255::6/64
	Et0/0 VLAN 30	2001:6130:6/64
R7	Lo130	2001:130::1/64
	Et0/0	2001:6130::13/64

10.2. Enable IPv6 EIGRP (Basic: 2 points)

- Place all of the above interfaces into IPv6 EIGRP AS 777. Make sure that all IPv6 routers can ping all IPv6 addresses.

10.3. Configure IPv6 Multicast (Intermediate: 2 points)

- Enable IPv6 multicast routing on R3 and R6
- Statically configure the IPv6 address 2001:3::1 as the rendezvous point, (RP).
- Join loopback 106 on R6 to the group address FF08:106::1.
- From R1, ping FF08:106::1 and verify a response from R6.

11. QoS Section (Total: 3 points)

11.1. Enable Traffic Management (Intermediate: 3 points)

- Restrict the Test TCP, or TTCP, utility traffic from R9 that is destined for 170.18.11.1 port 5001 to 1000000 b/s on R1. Allow burst traffic up to 512,000 bytes.
- Traffic that exceeds the above-specified condition is dropped.
- See the diagram for IP addressing. Do not use the MQC approach to accomplish this task.

12. Multicast Section (Total: 5 points)

12.1. Configure PIM (Intermediate: 3 points)

- Enable multicast routing between R1, R2, and R3 on subnet 170.18.123.0/24.
- Use a multicast routing protocol that uses any unicast routing protocol for source address determination and is based on a shared tree.
- Use the 224.0.1.39 PIM dense group for this configuration. Make R1 the root of the shared tree using the loopback 101 interface. Accomplish this task by configuring only R1.

12.2. Configure Internet Group Management Protocol (IGMP) (Intermediate: 1 point)

- Configure routers R1, R2, and R3 to join the multicast group 229.10.10.10. Associate this multicast group with a loopback interface on each router.

12.3. Verify Multicast Connectivity (Advanced: 1 point)

- Ping the multicast group 229.10.10.10 from R4 to all other multicast routers.