360RSW05-WKB-CA09

Cisco 360 CCIE R&S Exercise Workbook Introduction

The Cisco 360 CCIE® R&S Exercise Workbook contains 20 challenging scenarios at the CCIE level that can be used for rigorous self-paced practice.

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 9 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 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" figure and the IPv4 and IPv6 IGP 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 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 9 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: Basic to Intermediate

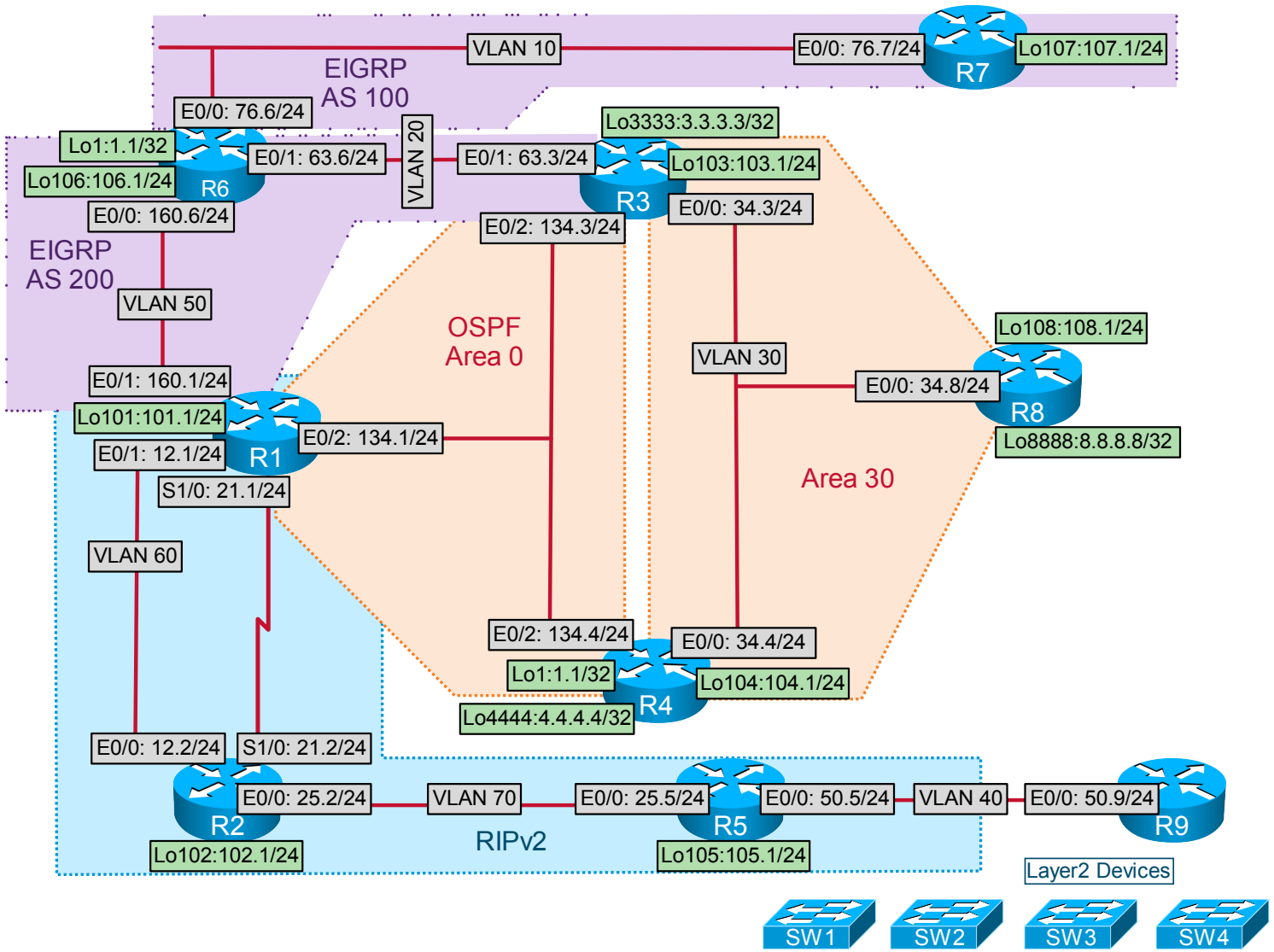
Restrictions and Goals

Note Read this section carefully.

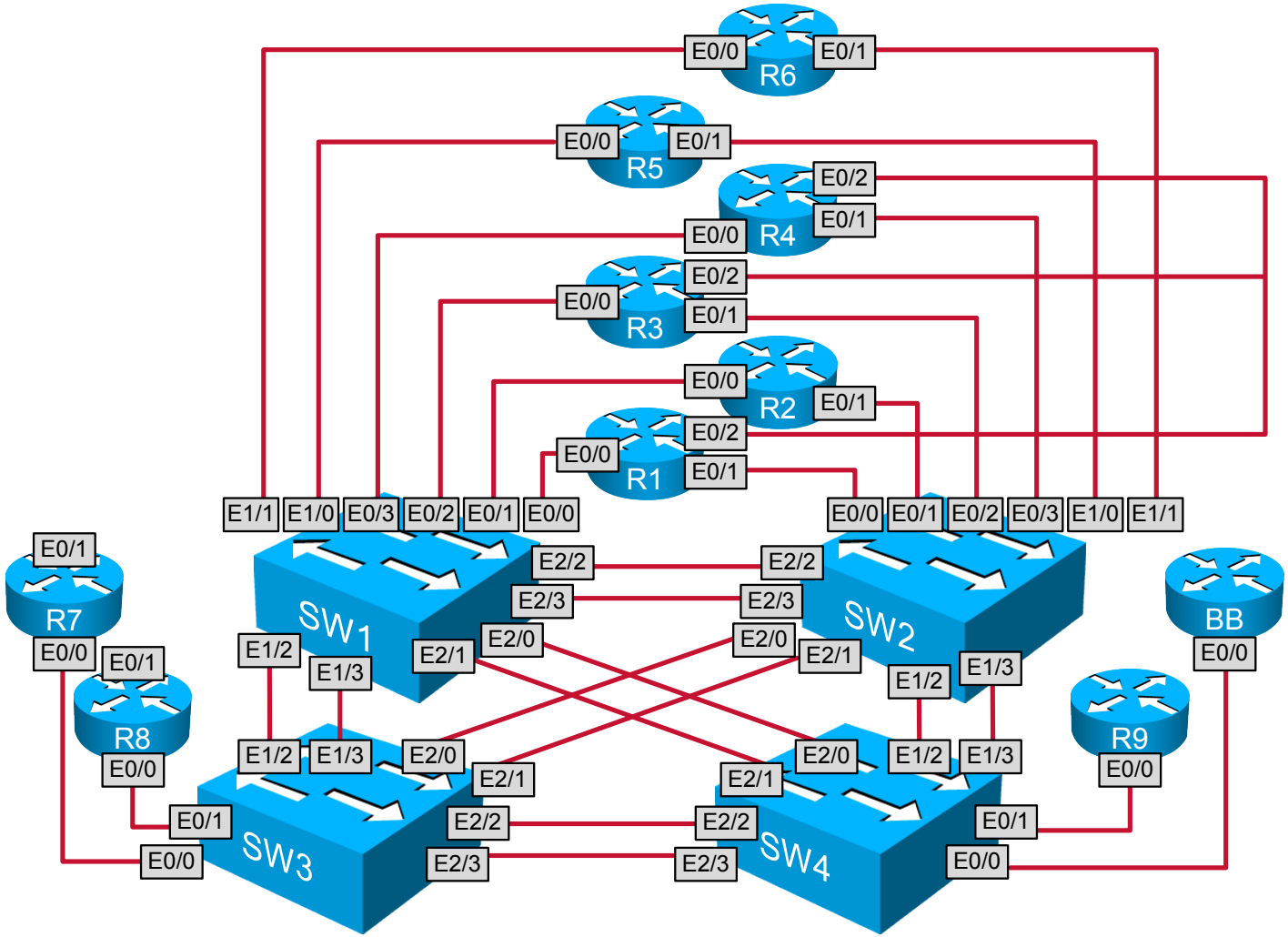
- To receive any credit for a subsection, you must fully complete the subsection as per requirements. You will *not* receive partial credit for partially completed subsections.
- IPv4 subnets displayed in the scenario diagram belong to network 148.49.0.0/16.
- *Points will be deducted from multiple sections for failing to assign correct IPv4 addresses.*
- Do not use any static routes.
- Advertise loopback interfaces with their original masks.
- Network 0.0.0.0/0 should not appear in any routing table (**show ip route**) except on R8.
- Do not use the **ip default-gateway** or **ip default-network** commands.
- Do not introduce any new IP addresses.
- All IP addresses involved in this scenario must be reachable, unless explicitly specified otherwise.
- Unless explicitly specified otherwise, addresses and networks that are advertised in the "Border Gateway Protocol" (BGP) section need to be reachable by all BGP routers but do not have to be reachable by interior gateway protocol (IGP)-only routers.
- Do not create new interfaces to fulfill IGP requirements, and do not create any summaries, unless the summary is required to meet explicitly stated scenario requirements.
- Do not introduce any new IPv4 or IPv6 addresses unless the instructions explicitly specify otherwise.
- Use only conventional routing algorithms, unless specified 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.

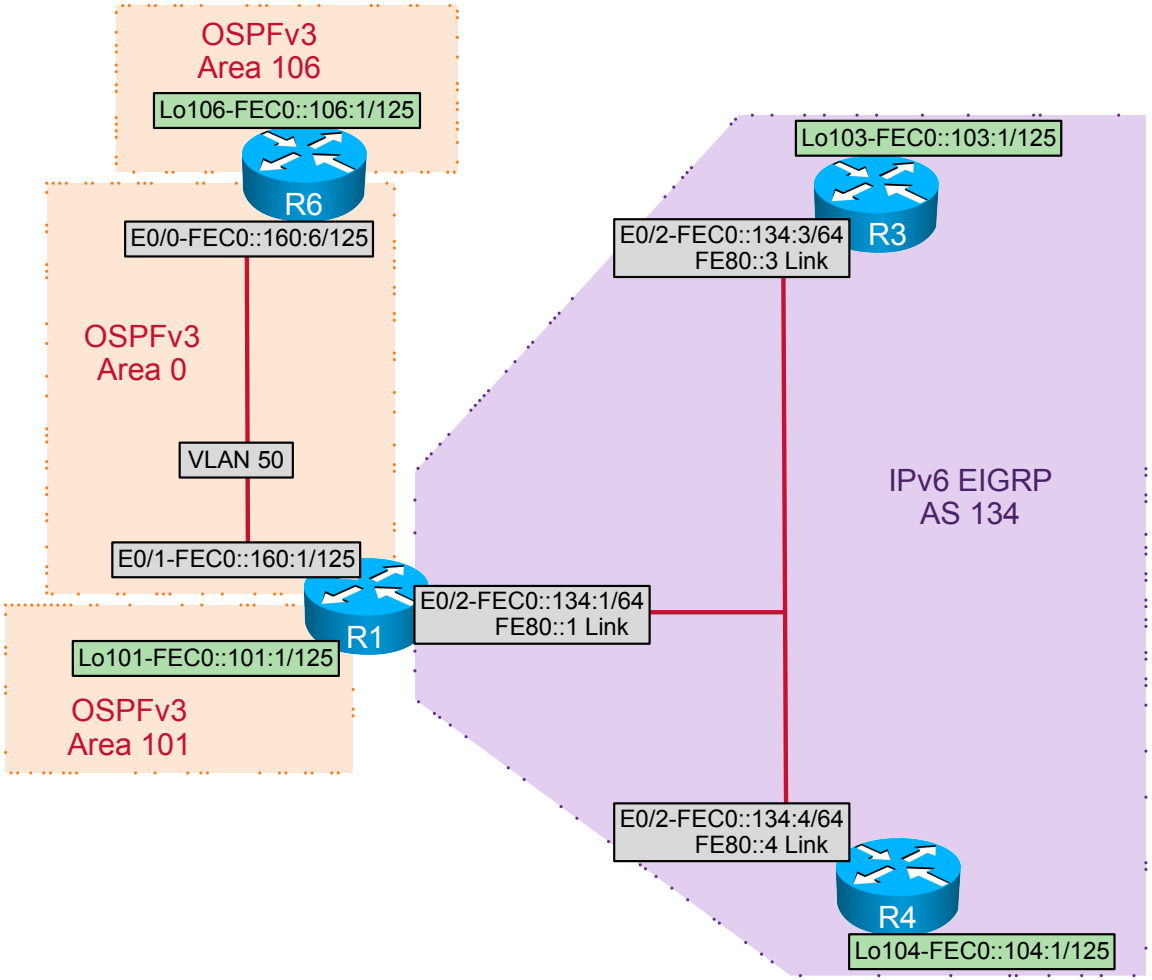
IPv4 IGP



Ethernet Switched Cabling Topology



IPv6 IGP



1. Switch Configuration Section (Total: 12 points)

1.1. Configure VLANs (Basic: 2 points)

- Create the VLANs referenced in the following table only on SW1:

VLAN Allocation

VLAN	VLAN Name
VLAN 10	DEVELOP
VLAN 20	PROD
VLAN 30	ENG
VLAN 40	TEST
VLAN 50	OFFICEA
VLAN 60	OFFICEB
VLAN 70	OFFICEC

- Configure the switch-to-router connections according to the "IPv4 IGP" diagram.
- For all trunks between a switch and a router, use dot1q encapsulation.

1.2. VTP Configuration (Basic: 2 points)

- All switches are in the TEST domain.
- Set VLAN Trunking Protocol (VTP) version 2 on all switches.
- No VLANs should be configured in the configuration mode on SW2, SW3, and SW4.

1.3. Control Switch-to-Switch Links (Basic: 2 points)

- Configure interfaces on active switch-to-switch links according to the following table, and verify that the ports indicated "administratively shutdown" remain in the shutdown state:

Switch-to-Switch Connections

Switch / Port		Switch / Port		Mode
SW1	1/2	SW3	1/2	administratively shutdown
	1/3		1/3	administratively shutdown
	2/0	SW4	2/0	Trunk 802.1Q
	2/1		2/1	Trunk 802.1Q
	2/2	SW2	2/2	Trunk 802.1Q
	2/3		2/3	Trunk 802.1Q
SW2	1/2	SW4	1/2	administratively shutdown
	1/3		1/3	administratively shutdown
	2/0	SW3	2/0	administratively shutdown
	2/1		2/1	administratively shutdown
SW3	2/2	SW4	2/2	Trunk 802.1Q
	2/3		2/3	Trunk 802.1Q

- Allow only necessary VLANs on all trunks.
- Use dot1q encapsulation for all trunks between two switches.

1.4. Tune Switch-to-Switch Links (Basic: 2 points)

- Configure a link between SW1 and SW2 combining both ports 2/2 and 2/3.

1.5. Tune STP (Basic: 2 points)

- Ensure that SW1 is the root bridge for VLAN 30.
- Ensure that SW2 is the root bridge for VLAN 20 and VLAN 40.
- Ensure that SW4 is the root bridge for VLAN 10.

1.6. Tune Forwarding Between SW1 and SW4 (Intermediate: 2 points)

- Configure forwarding on VLAN 10 to prefer the link between ports 2/1 of SW1 and SW4. If the link between ports 2/1 of SW1 and SW4 fails, forward traffic through the link between ports 2/0 of SW1 and SW4.

2. IPv4 OSPF Section (Total: 13 points)

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

2.1. Create OSPF Area 0 (Basic: 2 points)

- Configure Open Shortest Path First (OSPF) Area 0 between routers R1, R3, and R4 on the subnet 148.49.134.0/24.
- Do not use the default OSPF network type on the OSPF Area 0 Ethernet interfaces.
- Form the Area 0 adjacency without using the **neighbor** command.
- Advertise the Loopback1 interface on R4 in OSPF Area 0.

2.2. Create OSPF Area 30 (Basic: 2 points)

- Configure OSPF Area 30 between routers R3, R4, and R8 on the VLAN 30 subnet 148.49.34.0/24.
- Use the default OSPF network type to form the Area 30 adjacency.
- Router R3 must be elected as the designated router (DR).
- No backup designated router (BDR) must be elected on VLAN 30.
- R3 should use 148.49.255.3 as the OSPF router ID.

2.3. Tune OSPF Area 30 (Basic: 2 points)

- No external routing information is allowed into Area 30 from the backbone area.
- However, advertise the Loopback108 network on R8 as an OSPF external prefix.

2.4. Advertise More Loopback Interfaces (Basic: 2 points)

- Advertise Loopback interfaces 103 and 104 in OSPF Area 30.
- The Loopback101 network should be advertised as an external network of type 2 with a metric of 40.

2.5. Tune OSPF Route Type (Advanced: 3 points)

- The network of the Loopback108 interface must be listed in the routing tables of routers R3 and R4 as an N1 OSPF prefix.
- R1 must use the R4 router as the next hop to reach the network 148.49.108.0/24.

- Do not use any filtering technique to accomplish this task.

2.6. Verify Connectivity (Basic: 2 points)

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

3. IPv6 OSPF Section (Total: 4 points)

3.1. Configure Area 0 (Basic: 2 points)

- Configure OSPF IPv6 Area 0 on the link FEC0::160:0/125 between routers R1 and R6.

3.2. Advertise Loopbacks (Basic: 2 points)

- Place the Loopback networks FEC0::101:0/125 and FEC0::106:0/125 into OSPF IPv6 Areas 101 and 106, respectively, on routers R1 and R6.

4. IPv4 RIP Section (Total: 6 points)

4.1. Enable RIP (Basic: 2 points)

- Configure a Routing Information Protocol (RIP) routing information exchange between routers R1, R2, and R5.
- Updates should be sent only on VLAN 60, on the 148.49.21.0/24 subnet, and on VLAN 70.
- Ensure that all the interfaces participating in the RIP updates exchange send and receive RIP version 2 packets only. Do not use the interface configuration mode to accomplish this task.

4.2. Configure Preferred Path (Intermediate: 2 points)

- R1 and R2 must prefer the reachability to the RIP-learned prefixes via the Serial link.
- If the Serial link is down, the routers should prefer VLAN 60.

4.3. Link Between R5 and R9 (Basic: 2 points)

- No dynamic routing protocol should be configured on the VLAN 40 link between R5 and R9.
- Do not configure a gateway on R9.

5. IPv6 EIGRP Section (Total: 2 points)

5.1. Enable IPv6 EIGRP (Basic: 2 points)

- Configure IPv6 Enhanced Interior Gateway Routing Protocol (EIGRP) AS 134 on the link FEC0::134:0/125 between routers R1, R3, and R4.
- R3 and R4 should not form the IPv6 EIGRP AS 134 neighbor relationship.
- Include Loopbacks 103 and 104 in the IPv6 EIGRP AS 134 process.

6. IPv4 EIGRP Section (Total: 4 points)

6.1. Configure AS 200 (Basic: 2 points)

- Configure EIGRP AS 200 between routers R1, R3, and R6 on links 148.49.160.0/24 and 148.49.63.0/24.
- On R6, the interfaces Loopback106 and Loopback1 must be included in EIGRP AS 200.

6.2. Configure AS 100 (Basic: 2 points)

- Configure EIGRP AS 100 between R6 and R7.
- Advertise the Loopback107 interface into EIGRP AS 100 from R7.

7. IPv4 Route Redistribution Section (Total: 4 points)

7.1. Obtain Universal IPv4 Connectivity (Intermediate: 2 points)

- Perform a mutual redistribution of dynamic interior gateway protocols between:
  - RIP and OSPF on R1
  - RIP and EIGRP on R1
  - OSPF and EIGRP on R1 and R3
- Perform the **redistribute connected** command where required and not restricted by the scenario.
- EIGRP AS 200 speakers R1 and R3 should prefer R6 as a next hop for all EIGRP AS 100- and AS 200-originated prefixes.

7.2. Verify Connectivity (Intermediate: 2 points)

- Verify that all IPv4 IGP prefixes specified on the "IPv4 IGP" diagram can be reached from all devices. See the "Restrictions and Rules" section.
- R6 should prefer the Loopback108 network 148.49.108.0/24 of R8 via R3.
- Provide a redundant path for R8 to the rest of the network if the Ethernet0/1 and Ethernet0/2 interfaces of R3 become unavailable.

8. IPv6 Route Redistribution Section (Total: 2 points)

8.1. Obtain Partial Connectivity (Basic: 2 points)

- Perform mutual redistribution between IPv6 EIGRP and OSPFv3.
- Perform the **redistribute connected** command where required and not restricted by the scenario.

9. Border Gateway Protocol Section (Total: 7 points)

9.1. Configure Processes and Peers (Basic: 2 points)

- Configure BGP autonomous systems (AS) according to the following table:

BGP AS Assignment

Device	AS
R3, R4, R8	314
R6, R7	67

- Configure peering between
    - R3 and R6
    - R4 and R6, using Loopback interfaces 104 and 106

9.2. Advertise BGP Prefixes (Basic: 2 points)

- Advertise the networks associated with the following loopback interfaces into AS 314 with the ORIGIN attribute IGP:
    - Loopback3333
    - Loopback4444
    - Loopback8888

9.3. Tune IBGP Peering (Basic: 3 points)

- Do not form a full mesh of IBGP peer relationships within AS 314.

10. Quality of Service Section (Total: 3 points)

10.1. Discard Specific Traffic (Intermediate: 3 points)

- All HTTP traffic between routers R1 and R2 must be discarded without any further system processing.
- Apply your solution on both links between R1 and R2.
- Use the Modular QoS CLI (MQC) to accomplish this task.

11. System Administration Section (Total: 3 points)

11.1. Router Access (Advanced: 3 points)

- On R5, configure the username **admin** and the password **lab**.
- Configure system logging for both successful and failed login attempts.
- Provide a solution on R5 to slow down dictionary attacks that attempt to gain access to the username and access information:
    - Introduce a 3-second delay between successive login attempts.
    - If two login attempts to R5 fail within 15 seconds, R5 should not allow any login attempts for 10 seconds, except for attempts coming from 148.49.25.2.

12. Address Administration Section (Total: 6 points)

12.1. Configure Gateway Redundancy (Intermediate: 3 points)

- Two groups consisting of imaginary workstations are connected to VLAN 30.
- One Hot Standby Router Protocol (HSRP) group (GROUP1) is configured for the 148.49.34.1 gateway and the other HSRP group (GROUP2) is configured for 148.49.34.254.
- GROUP1 should use router R3 as a preferred gateway. If the Ethernet0/2 interface fails on R3, R4 must be preferred for the duration of the failure.
- GROUP2 should use router R4 as a preferred gateway. If the Ethernet0/2 interface fails on R4, R3 must be preferred for the duration of the failure.

12.2. Tune Telnet Sessions (Advanced: 3 points)

- The Telnet session from the Loopback108 interface of R8 to the Loopback106 interface of R6 should be listed on router R6 as originating from the IP address 148.49.108.180.
- This Telnet session must be established via R3.
- If the path via R3 becomes unavailable because the Ethernet0/1 and Ethernet0/2 interfaces on R3 have failed, the Telnet session should be established via R4.
- Extend your solution to the IP Finger protocol as well.

13. Multicast Section (Total: 10 points)

13.1. PIM Configuration (Basic: 2 points)

- Configure multicast routing between R1, R3, R4, R6, R7, and R8.
- Simulate the receivers of the multicast traffic destined to 225.23.23.23 using the loopback interfaces.

13.2. Configure Rendezvous Point (RP) (Intermediate: 2 points)

- Configure the Loopback1 interface on router R4 with the IP address 148.49.1.1/32.
- Configure the Loopback1 interface on router R6 with the IP address 148.49.1.1/32.
- Use these IP addresses for the RPs on R4 and R6 as well as mapping agents on the same routers.

13.3. Tune RP (Advanced: 2 points)

- Ensure that R4 and R6 accept join and prune messages only for RPs that are in their Auto-RP cache.

13.4. Tune Auto-RP Timer (Advanced: 2 points)

- All mapping agents should send RP announcements three times faster than the default.

13.5. Verify Multicast Connectivity (Intermediate: 2 points)

- Test your configuration by sourcing the multicast traffic from R7 and R8.

