360RSW05-WKB-TA09

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 Troubleshooting 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, 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 diagram.
- 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 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 Troubleshooting Section

Grading and Duration

- Troubleshooting lab duration: 2 hours
- Troubleshooting lab maximum score: 24 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

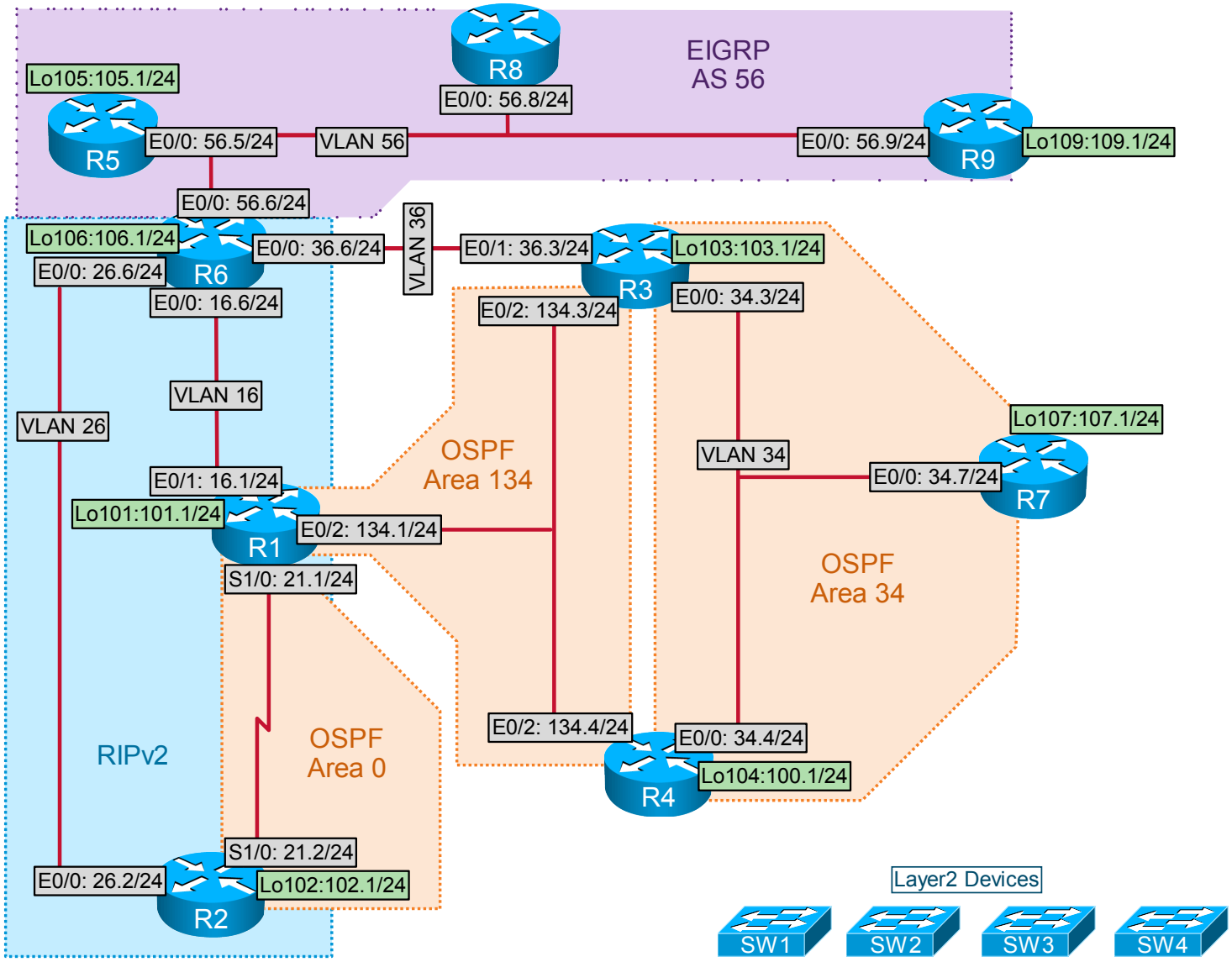
- Difficulty: Basic to Intermediate

Restrictions and Goals

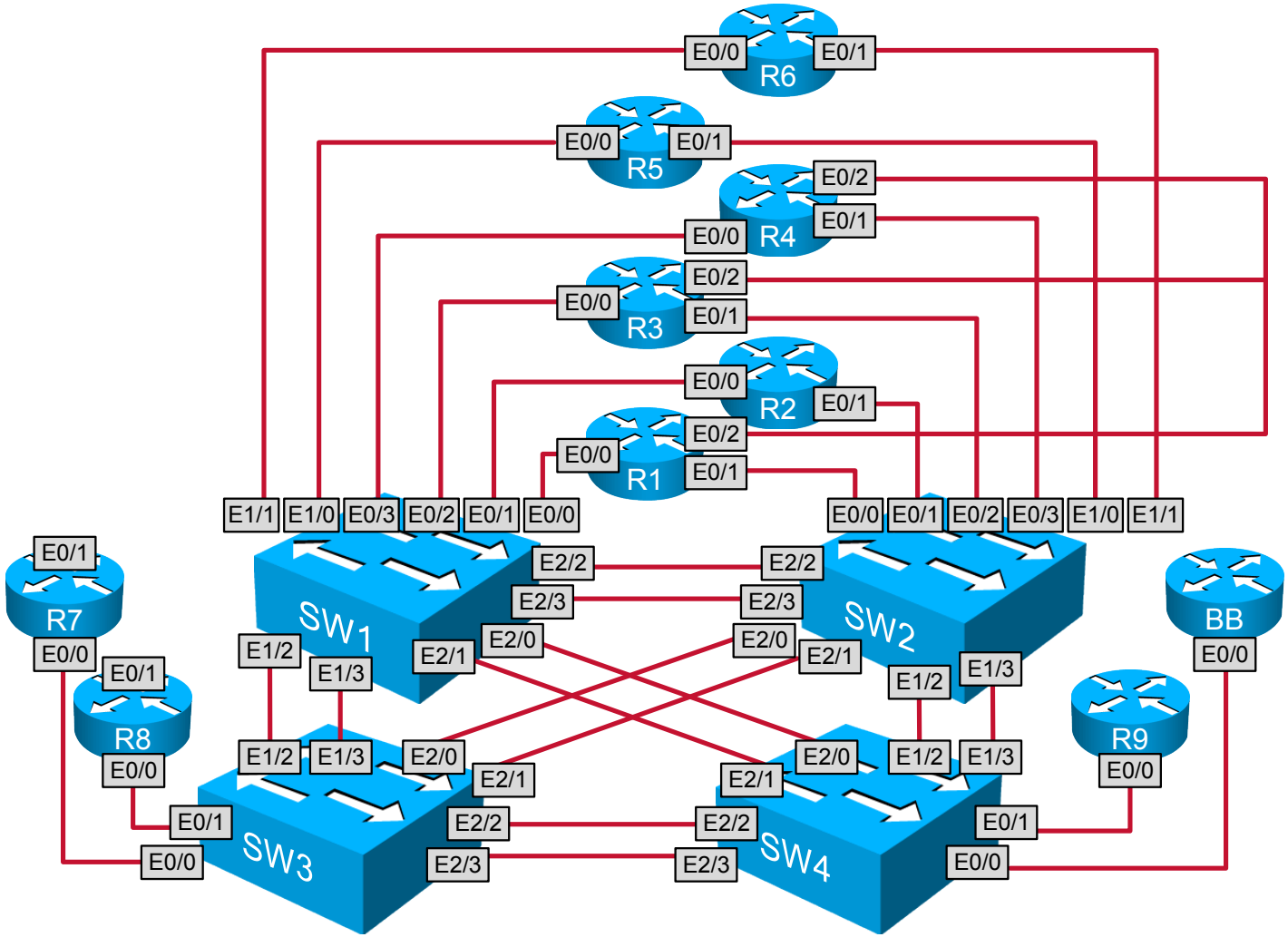
Note Read this section carefully.

- To receive credit for a subsection, you must fully complete the subsection per requirements. You will *not* receive partial credit for partially completed subsections.
- IPv4 subnets that are 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**).
- Do not use the **ip default-gateway** or **ip default-network** commands.
- Do not introduce any new IP addresses.
- 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.
- Use conventional routing algorithms only, unless the instructions specify otherwise.
- You may create new interfaces to fulfill IGP requirements, but do not summarize unless explicitly asked to do so.
- 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.

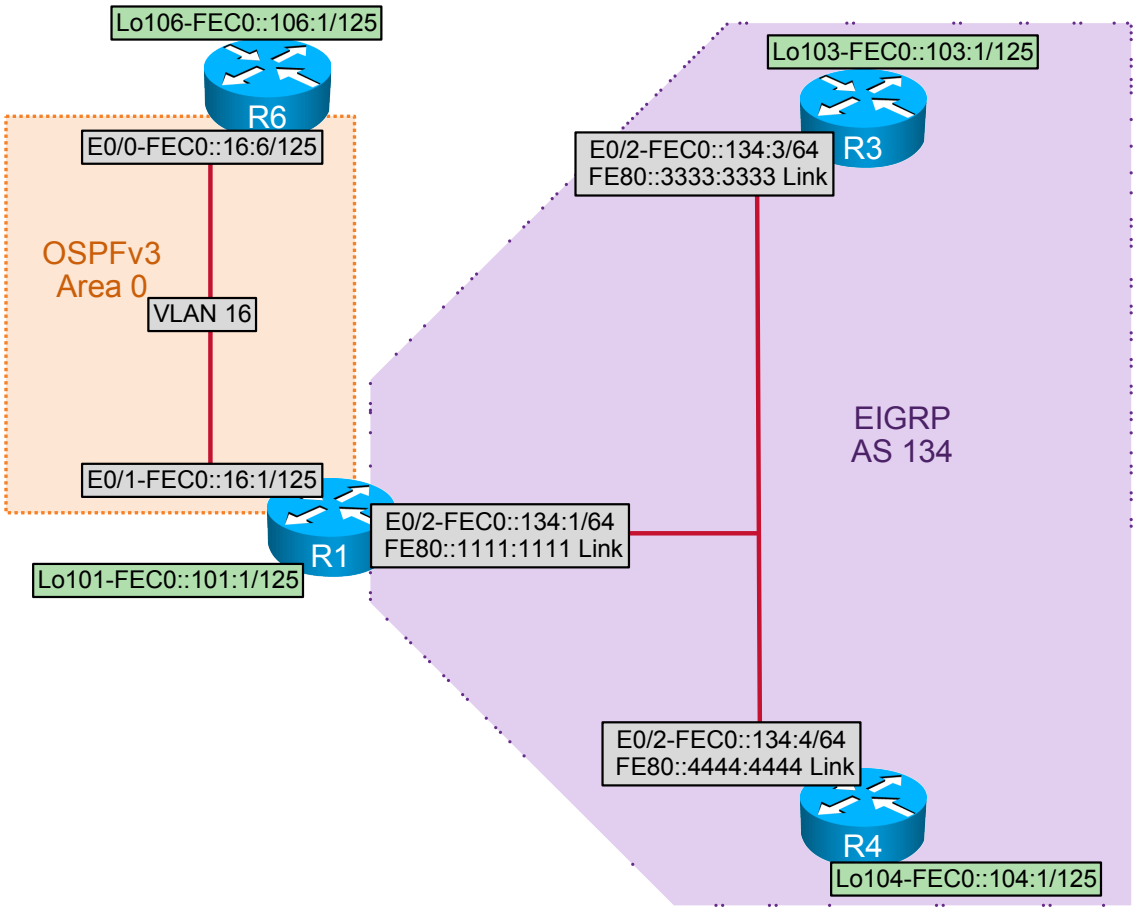
IPv4 IGP



Ethernet Switched Cabling Topology



IPv6 IGP



1. Switched Network Troubleshooting Section (Total: 3 points)

1.1. Troubleshooting Ticket

- Users reported that the switched network does not operate according to the requirements provided in the "Switched Network Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

1.2. Description of the Topology

- The switched Ethernet topology for this lab consists of five VLANs, as shown in the "IPv4 IGP" and "IPv6 IGP" diagrams. No additional VLANs may be configured or used.
- The trunk links connecting a switch and a router are encapsulated with dot1q. The trunk links between two switches are encapsulated with 802.1Q. All other links are access links.

1.3. Expected Behavior and Network Policies

- The Ethernet links shown in the "IPv4 IGP" and "IPv6 IGP" diagrams must support same-subnet reachability and the routing protocols shown.

1.4. Special Goals and Restrictions

- Allow only traffic in the required VLANs to cross trunk links.
- Do not create or use any additional Ethernet interfaces.
- All links that are administratively down must remain so.
- Using a standard protocol, Spanning Tree Protocol (STP) should not block any port between SW3 and SW4.
- All VLANs should have the same root switch SW4.
- If SW1, SW2, or SW3 reboot, they should rely on SW4 to rebuild their VLAN configurations.
- A local switch should send no broadcast traffic or unicast flooding across a trunk link, if the distant switch (or any switch behind) does not have a port configured in access mode for this VLAN. You can only use one command on one switch to perform this task.
- No IP address may be assigned to major interface E0/0 on R2.

2. IPv4 OSPF Troubleshooting Section (Total: 2 points)

2.1. Troubleshooting Ticket

- Users reported that the OSPF routing domain does not operate according to the requirements provided in the "IPv4 OSPF Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

2.2. Description of the Topology

- OSPF for IPv4 is divided into three areas, as shown in the "IPv4 IGP" diagram and listed below. Only these listed subnets should be internal to OSPF:

- Area 0 includes subnets 148.49.21.0/24 and 148.49.102.1/24.
- Area 134 includes subnet 148.49.134.0/24.
- Area 34 includes subnets 148.49.34.0/24, 148.49.103.0/24, and 148.49.100.0/24.

2.3. Expected Behavior and Network Policies

- OSPF must provide stable reachability between all internal subnets.
- In Area 0, the hello interval should be equal to 10 seconds and the dead interval should be equal to 40 seconds.
- Routers in Area 0 should elect a DR and BDR.
- The router ID of R1 should be 148.49.111.1.
- Subnet 148.49.107.1 should be redistributed into OSPF on R7.
- Subnet 148.49.26.0 should be redistributed into OSPF on R2 with a metric of 26.
- Area 34 should not have any DR.

2.4. Special Goals and Restrictions

- In Area 0, you may not use any of these commands: **ip ospf hello-interval**, **ip ospf dead-interval**, **ip ospf priority**, and **router-id**.
- The OSPF metric for subnet 148.49.26.0 should be the same on R1 and R7.
- The OSPF metric for subnet 148.49.107.0 should not be the same on R1 and R2.
- The **neighbor** command is not allowed in Area 34.
- The OSPF interface network type should not be changed in Area 134.
- Loopback networks must be advertised with their original masks.

3. IPv4 EIGRP Troubleshooting Section (Total: 2 points)

3.1. Troubleshooting Ticket

- Users reported that the EIGRP routing domain does not operate according to the requirements provided in the "IPv4 EIGRP Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

3.2. Description of the Topology

- As shown in the "IPv4 IGP" diagram, EIGRP AS 56 should operate:
  - On all interfaces located in VLAN 56
  - On Loopback105 of R5
  - On interface E0/0 of R6 located on VLAN 56
- No other networks are internal to EIGRP AS 56.

3.3. Expected Behavior and Network Policies

- Loopback106 should be advertised as an external route into EIGRP AS 56 with the following specifications:

- Tag 106
- Bandwidth 4,000,000 kb/s
- Delay 100,000 microseconds
- Reliability 255
- Loading 1
- MTU 1514

- Loopback109 should be advertised as an external route into EIGRP AS 56.

3.4. Special Goals and Restrictions

- No default routes may be advertised or used by EIGRP.
- EIGRP is not allowed to send any multicast frames on VLAN 56.

4. IPv4 RIP Troubleshooting Section (Total: 2 points)

4.1. Troubleshooting Ticket

- Users reported that the RIP routing domain does not operate according to the requirements provided in the "IPv4 RIP Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

4.2. Description of the Topology

- RIP operates between routers R1 and R6 and between R2 and R6, as shown in the "IPv4 IGP" diagram.

4.3. Expected Behavior and Network Policies

- RIP updates may be sent only on VLAN 16 and VLAN 26.
- Interfaces participating in the RIP updates may send only multicast updates.
- Interfaces participating in the RIP updates may not listen to unicast updates.

4.4. Special Goals and Restrictions

- Interface configuration commands are not all allowed to tune RIP configuration.

5. IPv4 Redistribution Troubleshooting Section (Total: 4 points)

5.1. Troubleshooting Ticket

- Users reported that the IPv4 IGP routing domain does not operate according to the requirements provided in the "IPv4 Redistribution Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

5.2. Description of the Topology

- OSPF and RIP are mutually redistributed on R1 and R2.
- EIGRP and RIP are mutually redistributed on R6.

- All devices should be able to reach all subnets.

5.3. Expected Behavior and Network Policies

- R2 should prefer R6 as the next hop for all traffic destined to VLAN 56.
- R6 should prefer R1 as the next hop for all traffic destined to all subnets advertised by R1, with the following exception:
  - R6 should prefer R2 as the next hop for all traffic destined to subnet 148.49.21.0/24.
  - No configuration may be done on R6 to obtain this policy.

5.4. Special Goals and Restrictions

- You may not use any additional commands such as **redistribute connected**.
- You may not configure any dynamic protocol on any additional interface from those indicated in the "IPv4 IGP" diagram.
- On R1 and R2, you may not create any additional route maps or access lists. You may modify the current access lists and route maps, but each access list may not have more than three statements.

6. Security Troubleshooting Section (Total: 3 points)

6.1. Troubleshooting Ticket

- Users reported that network security does not operate according to the requirements provided in the "Security Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

6.2. Description of the Topology

- To prevent MAC spoofing, make sure that only two MAC addresses are allowed on each interface E1/0 to E1/1 of SW2.
- In the future, administrators will enable PortFast on specific interfaces of SW1 and SW2.
- On SW1, if a bridge protocol data unit (BPDU) is received on such an interface, the interface should lose its PortFast feature.
- On SW2, if a BPDU is received on such an interface, the interface should be error-disabled.
- To mitigate STP manipulation and enforce root bridge placement in the network, make sure that interface E0/3 on SW2 becomes error-disabled if a better BPDU is received on this interface.

6.3. Expected Behavior and Network Policies

- The MAC addresses that are dynamically learned on SW2 E1/0 to E1/1 should be stored in the address table and added to the running configuration. Therefore, the interface will not need to dynamically relearn them when the switch restarts.

6.4. Special Goals and Restrictions

- On SW2 E1/0 to E1/1, if MAC spoofing is detected, the switch should shut down the interface.

7. IPv6 Troubleshooting Section (Total: 3 points)

7.1. Troubleshooting Ticket

- Users reported that the IPv6 network does not operate according to the requirements provided in the "IPv6 Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

7.2. Description of the Topology

- The IPv6 topology is shown in the "IPv6 IGP" diagram.
- All routable IPv6 prefixes start with hexadecimals FEC0.
- Link-local addresses are manually configured on the Ethernet0/2 links.
- IPv6 EIGRP AS 134 is configured as follows:
  - On interfaces with prefix FEC0::134:0/125 between R1, R3, and R4
  - On the Loopback103 and Loopback104 interfaces
- OSPFv3 is configured as follows:
  - Area 0 on prefixes FEC0::16:0/125 between routers R1 and R6.
  - Loopback network FEC0::101:0/125 should be redistributed into Area 0.
  - Loopback network FEC0::106:0/125 should be redistributed into Area 0.
- OSPFv3 and IPv6 EIGRP are mutually redistributed on R1.

7.3. Expected Behavior and Network Policies

- All routable IPv6 prefixes should be reachable from any other IPv6 interface.

7.4. Special Goals and Restrictions

- All networks must be advertised only with their original masks.

8. QoS Troubleshooting Section (Total: 3 points)

8.1. Troubleshooting Ticket

- Users reported that QoS does not operate according to the requirements provided in the "QoS Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

8.2. Description of the Topology

- Control Plane Policing (CoPP) should be configured with the average rate at 8000 b/s on R9.

8.3. Expected Behavior and Network Policies

- Traffic to be policed is any Telnet traffic, except:
- Telnet *source* IP address: Loopback103

- Telnet *destination* IP address: Loopback109

8.4. Special Goals and Restrictions

- Only the described traffic should be policed. All other types of traffic should not be affected.

9. IP Services Troubleshooting Section (Total: 2 points)

9.1. Troubleshooting Ticket

- Users reported that DHCP does not operate according to the requirements provided in the "IP Services Troubleshooting" section. R6 does not obtain the correct IP address from R2 on the interfaces connected to VLAN26.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

9.2. Description of the Topology

- R2 should act as the DHCP server for all Layer 3 devices that are connected to VLAN 26.

9.3. Expected Behavior and Network Policies

- R2 should announce R6 as the default gateway for workstations that are connected to VLAN 26.

9.4. Special Goals and Restrictions

- The workstation with the client name SPECIFIC should get the IP address 148.49.26.54.
- No configuration is allowed on R6.